ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ
МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ (УНИВЕРСИТЕТ) МИНИСТЕРСТВА
ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

На правах рукописи

Титов Андрей Александрович

РАСКРЫТИЕ И РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ОТНОШЕНИИ И С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ (РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ)

Специальность 5.1.4. Уголовно-правовые науки

Диссертация на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук,
профессор
Васюков Виталий Федорович

Москва – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3

ГЛАВА I. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ОТНОШЕНИИ И С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ 24

§ 1. Криптовалютная среда как источник криминалистически значимой информации 24

§ 2. Механизм следообразования преступной деятельности в элементах инфраструктуры криптовалюты 67

§ 3. Типичные способы преступлений, совершаемых в отношении и с использованием криптовалюты 98

ГЛАВА II. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ АСПЕКТЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ОТНОШЕНИИ И С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ 146

§ 1. Особенности проведения оперативно-розыскных мероприятий при раскрытии преступлений, совершаемых в отношении и с использованием криптовалюты 146

§ 2. Тактика проведения следственных действий на первоначальном этапе расследования преступлений, совершаемых в отношении и с использованием криптовалюты 172

§ 3. Тактика проведения последующих следственных действий при расследовании преступлений, совершаемых в отношении и с использованием криптовалюты 193

ЗАКЛЮЧЕНИЕ 225

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 229

Приложение 271

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена тем, что глобальная цифровизация экономики и, в частности, финансового сектора, обусловливает фундаментальные изменения в архитектуре финансовых потоков и механизмах их регулирования. Расширение спектра финансовых инструментов, доступных благодаря новым технологиям, сопровождается как оптимизацией транзакционных издержек и повышением эффективности рыночных процессов, так и возникновением принципиально новых угроз, связанных с потенциальным злоупотреблением достижениями технологического прогресса в преступных целях.

В этой связи разработка и внедрение комплексных стратегий, направленных на обеспечение финансовой безопасности и поддержание стабильности финансовой системы, основанных на результатах углубленного научного анализа, становятся императивом.

Необходимость оперативной адаптации к новым вызовам, связанным с трансграничными финансовыми операциями и распространением криптовалют, требует разработки инновационных подходов к выявлению и пресечению всего спектра преступлений, где были использованы подобные виртуальные активы.

При этом криптовалюты становятся не только предметом преступных действий, но и инструментом, позволяющим трансграничным организованным преступным сообществам (синдикатам) реализовывать многоуровневые схемы легализации преступных доходов, оборота наркотических средств и психотропных веществ, совершения коррупционных действий, финансирования терроризма и различного рода хищений. Нарастают угрозы применения критовалют в целях перемещения незаконных финансовых потоков, включая неконтролируемый вывод капитала за рубеж[1]. Сложившаяся ситуация ставит

[1] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. – Paris, France. 2021 // URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (дата обращения: 30.03.2025).

перед правоохранительными органами и регуляторами новые беспрецедентные задачи, требующие не только модернизации существующих методов анализа финансовых потоков, но и разработки принципиально новых стратегий, учитывающих децентрализованную и псевдоанонимную природу криптовалютных транзакций.

Согласно статистическим данным аналитической компании Chainalysis, в 2024 г. наблюдался значительный рост объёмов хищений криптовалютных активов. По сравнению с предыдущим годом общий объём украденных средств увеличился на 21,07%, достигнув отметки в 2,2 миллиарда долларов США. Параллельно с этим ростом наблюдалось увеличение количества отдельных инцидентов, связанных с несанкционированным доступом и хищением криптовалюты, которые выросли с 282 случаев, зафиксированных в 2023 г., до 303 случаев в 2024 г. Представленные данные свидетельствуют о существенном росте криминальной активности в сфере криптовалют и, как следствие, о необходимости усиления мер по обеспечению безопасности и защите цифровых активов[2].

При этом за последние годы наблюдается существенный рост объемов денежных средств граждан Российской Федерации, вкладываемых в криптовалюты. По экспертным оценкам ими открыто более 12 миллионов криптовалютных кошельков, а объем средств на кошельках составляет порядка 2 трлн. рублей. Кроме того, по экспертным данным Российская Федерация занимает третье место в мире по объему мировых майнинговых мощностей[3].

Значительно усугубляет ситуацию отсутствие единого международного правового поля и несовершенство контроля за оборотом цифровых активов, в результате чего создается обширное поле для злоупотреблений. В этих условиях крайне важен детальный анализ рисков, связанных с новыми

---

[2] $2.2 Billion Stolen from Crypto Platforms in 2024, but Hacked Volumes Stagnate Toward Year-End as DPRK Slows Activity Post-July // Chainalysis. – URL: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/ (дата обращения: 22.01.2025).

[3] Концепция законодательного регламентирования механизмов организации оборота цифровых валют // https://sozd.duma.gov.ru/bill/127303-8 (дата обращения: 22.01.2025).

финансовыми технологиями, и разработка методов, способных эффективно противостоять возникающим угрозам и обеспечить безопасность физических и юридических лиц.

В свою очередь криптовалютная система демонстрирует уникальное сочетание характеристик: с одной стороны, она потенциально усиливает привлекательность цифровых активов для совершения противоправных деяний, с другой - формирует потребность в дополнении существующих методик раскрытия и расследования за счет разработки новых алгоритмов, учитывающих специфику следообразования в децентрализованной цифровой инфраструктуре. Указанные объективные обстоятельства и определяют актуальность настоящего исследования, обусловливают его научную и прикладную потребность.

Степень разработанности темы исследования. Основой для исследования стали фундаментальные труды А.И. Бастрыкина[4], Д.В. Бахтеева[5], Р.С. Белкина[6], А.А. Бессонова[7], В.Ф. Васюкова[8], В.Б. Вехова[9], Б.Я. Гаврилова[10], А.Ю. Головина[11], К.К. Горяинова[12], А.В. Гриненко[13], В.В. Дорошкова[14],

---

[4] *Бастрыкин, А.И.* Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий / А. И. Бастрыкин // Вестник Российской правовой академии. – 2022. – № 4. – С. 88-94.

[5] *Бахтеев, Д.В.* Векторы цифрового развития криминалистики / Д. В. Бахтеев // Технологии XXI века в юриспруденции : Материалы Шестой всероссийской научно-практической конференции, Екатеринбург, 24 мая 2024 года. – Екатеринбург, 2024. – С. 13-17.

[6] *Белкин, Р.С.* Курс криминалистики. В 3 т. Т. 3: Криминалистические средства, приемы и рекомендации. – М.: Юристь, 1997. - 480 с.

[7] *Бессонов, А.А.* Проблемные вопросы установления признаков организованной группы по преступлениям, совершенным с использованием информационно-телекоммуникационных технологий / А. А. Бессонов // Журнал российского права. – 2024. – Т. 28, № 1. – С. 108-119.

[8] *Васюков, В.Ф.* К вопросу о сущности следов преступлений, совершаемых в сфере информационно-коммуникационных технологий / В. Ф. Васюков // Право и образование. – 2016. – № 8. – С. 112-118.

[9] *Вехов, В.Б.* Отдельные аспекты следственного осмотра некоторых электронных устройств / В. Б. Вехов, А. Б. Смушкин // Вестник Саратовской государственной юридической академии. – 2024. – № 4(159). – С. 230-236.

[10] *Гаврилов, Б.Я.* К вопросу о совершенствовании уголовной политики противодействия преступности в условиях информатизации общества: искусственный интеллект в уголовном судопроизводстве / Б. Я. Гаврилов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2025. – № 1 (69). – С. 262-265.

[11] *Головин, А.Ю.* Задачи криминалистики в сфере противодействия криптопреступности / А. Ю. Головин, Е. В. Головина // Санкт-Петербургский международный криминалистический

С.И. Захарцева[15], С.В. Зуева[16], И.Н. Кондрата[17], А.Л. Осипенко[18], А.С. Подшибякина[19], Е.Р. Россинской[20], Е.А. Русскевича[21], А.Ю. Шумилова[22], Е.Е. Центрова[23], Н.П. Яблокова[24] и других авторов.

форум : Материалы международной научно-практической конференции, Санкт-Петербург, 10–11 июня 2024 г. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2024. – С. 119-126.

[12] *Горяинов К.К.* Некоторые вопросы оперативно-розыскной практики в борьбе с коррупционными проявлениями в США и Великобритании / К.К. Горяинов // Современное состояние и актуальные проблемы противодействия коррупции в органах и учреждениях УИС. Сборник материалов круглого стола. 2019. – С. 55-60.

[13] *Гриненко, А. В.* Взаимодействие уголовно-процессуальной и криминалистической наук: труды профессора Р.С. Белкина и современность / А. В. Гриненко // Вестник криминалистики. – 2022. – № 3(83). – С. 11-14.

[14] *Дорошков, В.В.* Уголовно-правовая политика Российского государства в современную эпоху / В. В. Дорошков // Мировой судья. – 2024. – № 5. – С. 2-8.

[15] *Захарцев, С. И.* Кибермафия как угроза нормальному человеческому существованию: рецензия-размышление по поводу монографии «Мировые тенденции и международное противодействие» / С.И. Захарцев, В.П. Сальников // Юрист-Правоведъ. – 2022. – № 3 (102). – С. 215–220.

[16] *Зуев, С.В*. IT-следователь в цифровой среде уголовного судопроизводства / С.В. Зуев А.И. Зазулин // Правопорядок: история, теория, практика. – 2024. – № 2 (41). – С. 48-54.

[17] *Кондрат И.Н.* Особенности предупреждения преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий / И.И. Иванов, И.Н. Кондрат // Мировой судья. – 2024. – № 12. – С. 2–9.

[18] *Осипенко, А.Л.* Информационное воздействие на криминальную среду в условиях цифровизации / А. Л. Осипенко // Вестник Краснодарского университета МВД России. – 2024. – № 4(66). – С. 6-14.

[19] *Подшибякин, А.С.* Современная криминалистика и ее развитие / А. С. Подшибякин // Криминалистика и судебно-экспертная деятельность в условиях современности : Материалы Международной научно-практической конференции: в 2-х томах, Краснодарский университет МВД России, 26 апреля 2013 г. / Том I. – Краснодарский университет МВД России, 2013. – С. 3-15.

[20] *Россинская, Е.Р.* Система теории цифровизации судебно-экспертной деятельности / Е. Р. Россинская // Теория и практика судебной экспертизы. – 2024. – Т. 19, № 3. – С. 20-32.

[21] Р*усскевич, Е.А.* Преступления, связанные с обращением криптовалют: особенности квалификации / Е.А. Русскевич, И.И. Малыгин // Право. Журнал Высшей школы экономики. – 2021. – № 3. – С. 106–125.

[22] *Шумилов, А. Ю.* Совершенствование законодательного регулирования оперативно-розыскной деятельности таможенных органов / А. Ю. Шумилов // Регулирование внешнеэкономической деятельности и эволюция таможенной политики России : Тезисы докладов международной научно-практической конференции (22-23 октября 1996 г.): в 2 частях, Москва, 22–23 октября 1996 г. / Российская таможенная академия; председатель редколлегии Н.М. Блинов. Том Часть 2. – Москва: Российская таможенная академия, 1996. – С. 34-37.

[23] *Центров, Е. Е.* Теоретико-практический анализ соотношения понятий криминалистическая характеристика и классификация преступлений / Е. Е. Центров // Санкт-Петербургский международный криминалистический форум: Материалы международной научно-практической конференции, Санкт-Петербург, 10–11 июня 2024 г. – Санкт-Петербург: Санкт-

В научных трудах В.А. Ализаде[25], А.Г. Волеводза[26], Э.Л. Сидоренко[27] и О.Н. Тисен[28] детально анализируются отдельные вопросы противодействия

Петербургский университет Министерства внутренних дел Российской Федерации, 2024. – С. 537-542.

[24] *Яблоков, Н. П.* К вопросу о криминалистическом мышлении / Н.П. Яблоков // Правовые проблемы укрепления российской государственности. – Томск, 2012. – С. 156-159.

[25] *Ализаде, В. А.* Неприменение ст. 174.1 Уголовного кодекса РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов / В. А. Ализаде, А. Г. Волеводз // Наркоконтроль. – 2018. – № 1. – С. 5-13; *Ализаде, В. А.* Судебная практика применения ст. 174¹ УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты / В. А. Ализаде, А. Г. Волеводз // Наркоконтроль. – 2017. – № 4. – С. 8-14.

[26] *Волеводз, А. Г.* Криптовалюта и цифровые финансовые активы как предмет и способ преступного посягательства / А. Г. Волеводз // Цифровое право: Учебник. – Москва: ООО Издательский дом «Юрлитинформ», 2024. – С. 589-599; *Волеводз, А. Г.* К вопросу об учете потребностей противодействия отмыванию денег и финансированию терроризма при формировании правовых основ оборота криптовалюты в Российской Федерации / А. Г. Волеводз // Правовое поле современной экономики. – 2016. – № 3. – С. 135-145; *Волеводз, А. Г.* Международное сотрудничество в сфере уголовного судопроизводства по делам о преступлениях, совершенных с использованием криптовалюты: постановка проблемы / А. Г. Волеводз // Современное уголовно-процессуальное право - уроки истории и проблемы дальнейшего реформирования: Сборник материалов Международной научно-практической конференции. К 300-летию российской полиции, Орёл, 18–19 октября 2018 г. / Под редакцией Е.Б. Гришина. – Орёл, 2018. – С. 66-75; *Волеводз, А. Г.* Особенности криптовалюты в системе денежных инструментов как определяющие факторы правовой регламентации ее оборота / А. Г. Волеводз, В. А. Кутырин // Электронная валюта в свете современных правовых и экономических вызовов: сборник материалов Международной научно-практической конференции, Москва, 2 июня 2016 г. – Москва: Издательство «Юрлитинформ», 2016. – С. 292-308; *Волеводз, А. Г.* Оценка криптовалюты как предмета преступления, предусмотренного ст. 174.1 УК РФ / А. Г. Волеводз // Уголовное право: стратегия развития в XXI веке: Материалы XV Международной научно-практической конференции, Москва, 25–26 января 2018 г. – Москва: РГ-Пресс, 2018. – С. 597-603.

[27] *Сидоренко, Э. Л.* Криминологические риски оборота криптовалюты и проблемы ее правовой идентификации / Э. Л. Сидоренко // Библиотека криминалиста. Научный журнал. – 2016. – № 3(26). – С. 148-154; *Сидоренко, Э. Л.* Криптовалюта как новый юридический феномен // Общество и право. – 2016. – № 3 (57). – С. 193-197; *Сидоренко, Э. Л.* Криптопреступность как новое криминологическое явление / Э. Л. Сидоренко // Общество и право. – 2018. – № 2(64). – С. 15-21; *Сидоренко, Э. Л.* Легализация преступных доходов с использованием DeFi: типовые схемы и индикаторы риска / Э. Л. Сидоренко // Russian Journal of Economics and Law. – 2023. – Т. 17, № 4. – С. 822-836; *Сидоренко, Э. Л.* Криптовалюта и будущее цифровых финансов / Э. Л. Сидоренко. – Москва : МГИМО МИД России, 2023. – 36 с.

[28] *Тисен, О. Н.* Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют / О. Н. Тисен // Уголовное право. – 2024. – № 3(163). – С. 69-80; *Тисен, О. Н.* Установление владельцев криптокошельков, обнаружение и изъятие приватных ключей при расследовании уголовных дел / О. Н. Тисен // Уголовный процесс. – 2024. – № 1(229). – С. 78-83; *Тисен, О. Н.* Противодействие финансированию терроризма и диверсий, совершаемых с использованием

криптопреступлениям. Особое внимание уделяется проблемам формирования и оптимизации нормативной базы, необходимой для эффективного обнаружения угроз, исходящих от преступных формирований, и пресечения механизмов легализации преступных доходов, полученных с использованием криптовалют.

Авторским коллективом Санкт-Петербургской академии Следственного комитета Российской Федерации в 2022 г. была подготовлена монография, посвященная особенностям расследования преступлений, совершаемых с использованием цифровой валюты[29]. В этом же году была опубликована монография И.Б.Тутынина и О.В. Химичевой, в которой отражаются аспекты, связанные с применением мер уголовно-процессуального принуждения при расследовании преступлений, совершенных с использованием криптовалюты[30].

Отдельного внимания заслуживает исследование, проведенное в 2022-2024 г.г. на кафедре уголовного права, уголовного процесса и криминалистики МГИМО МИД России, которое было посвящено вопросам противодействия криптовалютным преступлениям в зарубежных странах. В результате исследования определены основные проблемные векторы не только в урегулировании указанной деятельности в отдельных юрисдикциях, но и в контексте использования механизмов отслеживания зарубежными правоохранительными органами цифровых следов в блокчейн-сети[31].

Не умаляя значения перечисленных работ для формирования научного базиса в выстраивании доктрины противодействия криптопреступности, отметим, что в них на комплексной основе не рассматриваются именно

криптовалют: Серия: Библиотека криминалиста / О. Н. Тисен. – Москва : Издательский дом «Юрлитинформ», 2025. – 248 с.

[29] Особенности расследования преступлений, совершаемых с использованием цифровой валюты: монография / под ред. Е. В. Емельяновой и О.С. Бутенко. – СПб: Санкт-Петербургская академия СК России, 2022. – 250 с.

[30] *Тутынин, И. Б.* Применение мер уголовно-процессуального принуждения при расследовании преступлений, совершенных с использованием криптовалюты / И. Б. Тутынин, О. В. Химичева. – Москва : Издательство «Юрлитинформ», 2022. – 144 с.

[31] Противодействие криптовалютным преступлениям в зарубежных странах / В. Ф. Васюков, А. Г. Волеводз, К. К. Клевцов [и др.]. – Москва : ООО Издательский дом «Юрлитинформ», 2025. – 504 с.

криминаличтические аспекты раскрытия и расследования преступлений с учетом как российского, так и зарубежного опыта.

Между тем теоретические аспекты и правоприменительные проблемы раскрытия и расследования преступлений, связанных с информационными технологиями, в различной степени затрагивались в исследованиях: В.А. Мещерякова «Основы методики расследования преступлений в сфере компьютерной информации» (2001)[32]; А.А. Шаевича «Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений» (2007)[33]; Ю.В. Гаврилина «Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы» (2010)[34]; М.А. Бабаковой «Проблемы розыска при расследовании преступлений в сфере высоких технологий» (2010)[35]; Е.И. Мазурова «Методика расследования хищений, совершенных с использованием интернет-технологий» (2017)[36]; В.В. Коломинова «Расследование мошенничества в сфере компьютерной информации (научно-теоретическая основа и прикладные аспекты первоначального этапа)» (2017)[37]; Г.З. Гаспаряна «Расследование хищений денежных средств, совершенных с использованием информационных

---

[32] *Мещеряков, В.А.* Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. … д-ра юрид. наук. – Воронеж, 2001. – 39 с.

[33] *Шаевич, А.А.* Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений : дис. … канд. юрид. наук / Шаевич Антон Александрович. – Иркутск, 2007. – 195 с.

[34] *Гаврилин, Ю.В.* Расследование преступлений, посягающих на информационную безопасность в сфере экономики : теоретические, организационно-тактические и методические основы : автореф. дис. … д-ра юрид. наук / Гаврилин Юрий Викторович. – Москва, 2010. – 55 с.

[35] *Бабакова, М.А.* Проблемы розыска при расследовании преступлений в сфере высоких технологий : дис. … канд. юрид. наук / Бабакова Мария Алексеевна. – Саратов, 2010. – 268 с.

[36] *Мазуров, И. Е*. Методика расследования хищений, совершенных с использованием интернет - технологий : автореф. дис. … канд. юрид. наук / Мазуров Игорь Евгеньевич. – Ростов-на-Дону, 2017. – 24 с.

[37] *Коломинов, В.В.* Расследование мошенничества в сфере компьютерной информации : научно-теоретическая основа и прикладные аспекты первоначального этапа : автореф. дис. … канд. юрид. наук / Коломинов Вячеслав Валентинович. – Краснодар, 2017. – 25 с.

банковских технологий» (2021)[38]; Н.И. Старостенко «Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий» (2023)[39]. Между тем криптовалюты в данных исследованиях либо вообще не исследовались, либо изучались как разновидность информационных технологий, используемых в реализации преступного умысла.

Следует особо отметить, что криминальное применение криптовалют уже становилось объектом диссертационных исследований М.М. Долгиевой «Теоретические основания уголовной политики в сфере оборота криптовалюты» (2023)[40] и В.А. Перова «Квалификация преступлений, совершаемых с использованием криптовалюты» (2023)[41]. Однако указанные авторы уделили свое внимание уголовно-правовым аспектам противодействия преступлениям, связанным с криптовалютами.

Признавая значимость перечисленных исследований как отправной точки для настоящей работы, следует подчеркнуть, что вопросы, касающиеся исключительно раскрытия и расследования преступлений, совершаемых в отношении и с использованием криптовалюты, с учетом рассмотрения иностранного опыта, не являлись предметом самостоятельного изучения. В связи с этим настоящее исследование представляется актуальным и своевременным, а его результаты позволят внести вклад в решение значимой научной и прикладной задачи.

Цель исследования – разработка с учетом иностранного опыта частной методики раскрытия и расследования преступлений, совершаемых в отношении

---

[38] *Гаспарян, Г.З.* Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : автореф. дис. … канд. юрид. наук / Гаспарян Гурген Зорикович. – Москва, 2020. – 30 с.

[39] *Старостенко, Н.И.* Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий : дис. … канд. юрид. наук / Старостенко Нина Игоревна. – Краснодар, 2023. – 230 с.

[40] *Долгиева, М.М.* Теоретические основания уголовной политики в сфере оборота криптовалюты: дис. … д-ра юрид. наук / Долгиева Мадина Муссаевна. – Москва, 2023. – 474 с.

[41] *Перов, В.А.* Квалификация преступлений, совершаемых с использованием криптовалюты : автореф. дис. … канд. юрид. наук / Перов Валерий Александрович. – Москва, 2023. – 25 с.

и с использованием криптовалюты как комплекса научно обоснованных предложений и тактических рекомендаций, направленных на повышение эффективности противодействия рассматриваемым деяниям.

Достижение цели предполагает постановку и решение следующих **задач**:

- определить и систематизировать криминалистически значимую информацию, содержащуюся в криптовалютной среде;
- исследовать механизм следообразования преступной деятельности в различных элементах инфраструктуры криптовалюты;
- классифицировать и описать типичные способы совершения преступлений в отношении и с использованием криптовалюты;
- раскрыть особенности проведения оперативно-розыскных мероприятий, направленных на раскрытие преступлений, совершаемых в отношении и с использованием криптовалюты;
- определить специфику проведения первоначальных следственных действий при расследовании преступлений, связанных с криптовалютой;
- раскрыть особенности проведения последующих следственных действий при расследовании рассматриваемых преступлений.

Объектом исследования являются общественные отношения, возникающие в процессе совершения преступлений, связанных с криптовалютой, а также деятельность, осуществляемая в ходе раскрытия и расследования таких преступлений.

Предметом исследования выступают закономерности механизма преступлений, совершаемых в отношении и с использованием криптовалюты, и основанные на познании данных закономерностей, а также особенности их раскрытия и расследования.

Научная новизна работы обусловлена тем, что оно представляет собой первое комплексное исследование, посвященное криминалистическим аспектам раскрытия и расследования преступлений, совершаемых в отношении и с использованием криптовалюты, с учетом как российского, так и зарубежного опыта. Разработаны предложения по совершенствованию криминалистических

механизмов, направленных на повышение эффективности работы с цифровыми следами в блокчейн-среде.

Теоретическая значимость исследования заключается в том, что сформулированные в нем выводы и положения о понятии, криминалистических особенностях криптовалютной среды и методических основах ее использования могут найти применение в дальнейших научных исследованиях по проблемам криминалистической техники, криминалистической тактики, методики расследования отдельных видов преступлений, а также в области криминалистической методики расследования преступлений, совершаемых в отношении и с использованием криптовалют.

Практическая значимость результатов исследования заключается в том, что научно обоснованные рекомендации, изложенные в работе, могут способствовать оптимизации практической деятельности по расследованию и профилактике преступлений, совершаемых в отношении криптовалюты и с их использованием. В частности, результаты исследования могут найти применение в правоохранительной деятельности, а именно в работе органов предварительного расследования и органов прокуратуры. Наконец, предлагаемые результаты исследования могут быть интегрированы в образовательный процесс организаций юридического и технического профиля для повышения качества обучения по дисциплине «Криминалистика» и специализированным курсам, связанным с противодействием преступности в условиях цифровизации.

Методология и методы исследования. В работе применялись общенаучные методы, в частности диалектический материализм, с помощью которого представилось возможным применить фундаментальные категории и принципы права в контексте исследуемой темы. Особая роль была отведена системному методу, оперирование которым позволило сформулировать целостный правовой механизм раскрытия и расследования преступлений, совершаемых в отношении и с использованием криптовалюты. Методы анализа и синтеза открыли возможность получить реальные сведения относительно

законодательного регулирования деятельности органов дознания, органов предварительного следствия и прокуратуры в контексте борьбы с указанными общественно опасными деяниями.

Вместе с тем были задействованы и специальные методы, в особенности юридические. К ним стоит отнести формально-юридический метод, благодаря которому автору удалось сконструировать понятие и определить правовую природу криптовалюты и иных смежных категорий. Посредством метода интерпретаций представилось возможным выяснить действительный смысл норм, применяемых в досудебном производстве по уголовным делам о преступлениях, совершенных в отношении и с использованием криптовалюты. Использование сравнительно-правового метода позволило соотнести нормы зарубежного и отечественного права в сфере противодействия преступлениям, где фигурировала криптовалюта. Автор также использовал социологические методы, состоящие из наблюдения, анализа письменных источников, анкетирования, интервьюирования по проблемам, обозначенным в настоящем исследовании.

Нормативно-правовую основу исследования составляют положения международных договоров Российской Федерации, Конституции Российской Федерации, Уголовного кодекса Российской Федерации, Уголовно-процессуального кодекса Российской Федерации, иных федеральных законов, а также подзаконных нормативных правовых актов. Кроме того, использовалось законодательство отдельных иностранных государств в части, касающейся регулирования криптовалют.

Информационную основу исследования составили ранее действовавшие законодательные акты, действующие нормативные акты иных государств, решения Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, разъяснения Пленума Верховного Суда Российской Федерации, рекомендации ФАТФ и др.

Эмпирическая база диссертационного исследования включает в себя: официальные статистические данные с 2020 по 2024 гг., содержащие

показатели деятельности правоохранительных органов Российской Федерации, связанные с раскрытием и расследованием преступлений, совершенных с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации; сведения, полученные в результате изучения материалов 327 уголовных дел, где фигурировала криптовалюта; результаты анкетирования и опроса 274 практических сотрудников, из которых 153 сотрудника следственных подразделений МВД России, 46 следователей Следственного комитета Российской Федерации в различных субъектах Российской Федерации (Москва, Санкт-Петербург, Республика Башкортостан, Саратовская область, Краснодарский край, Свердловская область, Хабаровский край, Омская область, Саха (Якутия), Республика Коми, Республика Мордовия и др.), а также 75 сотрудников, уполномоченных осуществлять оперативно-розыскную деятельность.

Также изучен опыт противодействия криптопреступлениям Интерполом, Европолом, ФАТФ, УНП ООН, а также правоохранительными органами таких стран, как Австралийский Союз, Аргентинская Республика, Государство Япония, Итальянская Республика, Канадская Федерация, Китайская Народная Республика, Королевство Нидерландов, Объединённые Арабские Эмираты, Португальская Республика, Республика Беларусь, Республика Индия, Республика Индонезия, Республика Казахстан, Республика Корея, Республика Косово, Малайзия, Республика Сингапур, Соединённые Штаты Америки, Турецкая Республика, Федеративная Республика Бразилия, Федеративная Республика Германия, Французская Республика, Чешская Республика, Швейцарская Конфедерация.

Научная новизна диссертационного исследования заключается в разработке комплексного подхода к криминалистическим аспектам раскрытия и расследования преступлений, совершаемых в отношении и с использованием криптовалюты, с интеграцией российского и зарубежного опыта. В работе предложена частная методика расследования, основанная на анализе следообразования в блокчейн-среде, учитывающая её децентрализованную

архитектуру, псевдоанонимность участников и трансграничный характер транзакций.

Также в результате исследования были систематизированы криминалистически значимые данные, формируемые в криптовалютной инфраструктуре; установлены закономерности взаимодействия цифровых следов в блокчейне с данными социальных ресурсов и операционных систем, обеспечивающие реконструкцию полной картины преступной деятельности; разработаны адаптированные модели оперативно-розыскных мероприятий.

Научную новизну диссертационного исследования подтверждают **основные положения, выносимые на защиту:**

1. Криптовалютная среда обладает уникальным криминалистическим потенциалом как источник структурированных данных, позволяющих смоделировать механизм преступной деятельности. Это обусловлено её свойствами: децентрализацией, неизменностью транзакций, прозрачностью блокчейна и псевдоанонимностью участников. Указанные характеристики формируют устойчивые цифровые следы, которые при корректной интерпретации становятся основой для установления причинно-следственных связей, идентификации субъектов и доказывания их причастности к противоправным деяниям.

2. Ценность криминалистически значимой информации в криптовалютной среде определяется её способностью минимизировать неопределённость в процессе расследования, однако её эффективное использование требует адаптации традиционных методов к специфике криптотехнологий. Актуальность, точность, полнота и эргономичность данных выступают ключевыми критериями, а их анализ должен опираться на принципы критического мышления, междисциплинарный подход и интеграцию современных инструментов, таких как графовая аналитика и алгоритмы машинного обучения.

3. Технология «блокчейн», являясь фундаментом криптовалютной инфраструктуры, формирует новый тип следообразования, требующий

разработки специализированной криминалистической методики. Несмотря на устойчивость и публичность данных в распределённом реестре, их интерпретация осложняется псевдоанонимностью, использованием миксеров и приватных монет, а также трансграничным характером транзакций. Это обусловливает необходимость создания стандартизированных протоколов работы с цифровыми следами, включая их фиксацию, верификацию и интеграцию в доказательственную базу.

4. Цифровые следы, формируемые в блокчейн-среде, обладают уникальными характеристиками, обусловленными технологическими особенностями распределённых реестров. Их ключевые свойства – неизменяемость, прозрачность и структурированность – делают их ценным источником криминалистически значимой информации. Каждая транзакция, включая метаданные (временны*е* метки, хеши, комиссии), создаёт устойчивый «цифровой отпечаток», позволяющий реконструировать цепочки перемещения активов. Однако псевдоанонимность участников и использование инструментов маскировки следов (миксеры, приватные криптовалюты) усложняют прямую идентификацию субъектов, требуя применения специализированных методов анализа, таких как: графовый анализ транзакций для выявления связей между кошельками; кластеризация адресов на основе шаблонов активности; корреляция данных из внешних источников.

5. Разделение криптопреступлений на две категории – посягательства на криптовалюты и их использование в противоправных целях – определяет дифференциацию тактических приемов, используемых при расследовании. В первом случае приоритетным является ретроспективный анализ транзакций в публичных реестрах блокчейна с целью установления цепочек перемещения активов, тогда как во втором акцент переносится на выявление инфраструктурных элементов, что требует применения превентивных оперативно-тактических моделей. Изучение международного опыта показывает, что симуляция элементов криптовалютной инфраструктуры позволяет с высокой точностью документировать деятельность организованных

преступных групп, однако результативность подобных операций напрямую зависит от технологической достоверности и учета субкультурных особенностей криминальной среды.

6. Существенным фактором повышения эффективности раскрытия и расследования преступлений, совершаемых в отношении и с использованием криптовалюты, является углубленный анализ и систематизация закономерностей между следами, оставленными в сети блокчейн, и данными, генерируемыми и распространяемыми на различных электронных социальных ресурсах. Комплексный подход к изучению цифровых следов, в свою очередь, позволяет не только выявить прямые связи между участниками преступной деятельности, но и установить латентные, косвенные взаимосвязи, раскрывающие полную картину преступления и способствующие установлению всех причастных лиц.

7. Тактические особенности проведения допроса жертв криптопреступлений обусловлены необходимостью детализации каналов коммуникации со злоумышленниками, включая мессенджеры, социальные сети и специализированные инвестиционные платформы. При этом ключевое значение приобретает фиксация технических параметров транзакций, таких как типы криптовалют, адреса кошельков и данные криптобирж. Установление методов манипуляции, включая обещания высокой доходности и психологическое давление, требует применения психологических подходов к изучению поведения жертв, а приобщение скриншотов переписок и выписок транзакций может существенно усилить значение опроса в поисковых мероприятиях. Дифференциация подхода, основанная на классификации криптопреступлений, актуализирует фокусировку на обстоятельствах хищения при посягательствах на криптоактивы и установлении связей транзакций с противоправной деятельностью при их использовании в качестве инструмента, что отражает дуализм оперативно-розыскной тактики в условиях технологической сложности.

8. Специфика оперативно-розыскного мероприятия «Наведение справок» заключается в комплексном анализе публичных данных блокчейна, включая историю транзакций и баланс кошельков, а использование инструментов для визуализации связей и поиска в открытых источниках позволяет выявлять корреляции между псевдонимами и реальными фигурантами. В свою очередь мониторинг сети Даркнет и специализированных форумов, направленный на идентификацию нелегальных сервисов, требует применения методов сетевого анализа, а направление запросов в криптобиржи и интернет-провайдеры подчеркивает важность межведомственного взаимодействия. Комбинация изучения открытых источников с данными блокчейн-аналитики формирует методологическую основу для реконструкции цепочек транзакций и выявления инфраструктуры преступных схем.

9. Тактика допроса при расследовании криптопреступлений базируется на интеграции специальных знаний в области блокчейн-технологий, криптографических алгоритмов и архитектуры криптобирж, адаптированных к специфике трансграничности и технологической опосредованности противоправных деяний. Стратегически значимым элементом выступает предварительное изучение технической компетенции подозреваемого, что позволяет сформулировать вопросы с использованием узкоспециализированной терминологии для нейтрализации попыток манипуляции в показаниях. Особое значение имеет установление алгоритмов функционирования вредоносного программного обеспечения, методов преодоления систем кибербезопасности и масштаба серийности правонарушений, подкрепленное визуализацией технических элементов (графы транзакций, схемы эксплуатации уязвимостей).

10. Эффективность проведения обыска напрямую коррелирует с привлечением специалистов в области блокчейн-аналитики и тактическим арсеналом по нейтрализации противодействия, в том числе с помощью блокировки интернет-соединения для исключения риска удалённого уничтожения информации, структурного анализа помещения на предмет скрытых хранилищ, а также с применением рефлексивных методов,

направленных на прогнозирование поведенческих реакций субъектов, вовлечённых в противоправную деятельность.

11. Иностранный опыт раскрытия и расследования преступлений свидетельствует о том, что эффективное противодействие криптопреступности требует интеграции инновационных оперативно-тактических моделей, основанных на создании контролируемых цифровых платформ, имитирующих функционал криминальной инфраструктуры. Ключевым условием успеха выступает синтез блокчейн-аналитики с традиционными оперативными методами, позволяющими реконструировать сетевые взаимодействия преступных групп и устанавливать их иерархию. Технологическая достоверность таких платформ достигается за счет воспроизведения востребованных в криминальной среде инструментов, учета региональных особенностей и социокультурных норм, а также применения гибридных моделей, сочетающих контролируемые системы с участием содействующих лиц.

Степень достоверности и апробация результатов исследования.

Настоящая работа выполнена на кафедре уголовного права, уголовного процесса и криминалистики Московского государственного института международных отношений (университет) Министерства иностранных дел Российской Федерации.

Основные положения и выводы диссертационного исследования нашли отражение в 12 научных статьях автора,

6 из которых опубликованы в научных журналах, рекомендованных ВАК Минобрнауки России:

1. Титов, А.А. Некоторые вопросы обнаружения и исследования компьютерной информации при раскрытии и расследовании преступлений / А.А. Титов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2022. – № 3 (37). – С. 39-48. – DOI 10.17150/2411-6122.2022.3.39-48.

2. Титов, А.А. Понятие, признаки и правовая природа цифровых финансовых активов: уголовно-правовой аспект / А. А. Титов // Пролог: журнал о праве. – 2022. – № 4 (36). – С. 105-113. – DOI 10.21639/2313-6715.2022.4.10.

3. Титов, А.А. Процессуальные и тактические проблемы изъятия электронных носителей и копирования информации при расследовании преступлений с использованием криптовалюты / А. А. Титов, В. Ф. Васюков // Российский следователь. – 2023. – № 2. – С. 23-27. – DOI 10.18572/1812-3783-2023-2-23-27.

4. Титов, А.А. Отдельные особенности рассмотрения сообщений (заявлений) о преступлениях, совершенных с использованием криптовалют / А.А. Титов // Вестник Академии Следственного комитета Российской Федерации. – 2023. – № 2. – С. 121-128. – DOI 10.54217/2588-0136.2023.36.2.015.

5. Титов, А.А. Отдельные аспекты выявления и раскрытия криптомошенничеств в Индии / А.А. Титов // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 3 (98). – С. 279-283.

6. Титов, А.А. Использование криптовалют в преступных целях: методы выявления и противодействия / А.А. Титов // Современное общество и право. – 2024. – № 4. – С. 138-146.

7 – в иных научных изданиях:

7. Титов, А.А. К вопросу о методах получения компьютерной информации при расследовании преступлений, совершаемых с использованием цифровых финансовых активов / А.А. Титов // Современное уголовно-процессуальное право - уроки истории и проблемы дальнейшего реформирования: Сборник материалов международной научно-практической конференции, посвященной 100-летию принятия УПК РСФСР 1922 г., 20-летию действия УПК РФ. В 2-х частях, Орел, 06–07 октября 2022 года. – Орел: Орловский юридический институт Министерства внутренних дел Российской Федерации имени В.В. Лукьянова, 2022. – С. 121-126.

8. Титов, А.А. Некоторые аспекты проведения осмотра при расследовании преступлений, связанных с информационными технологиями / А.А. Титов // Актуальные проблемы уголовно-процессуального права, криминалистики и оперативно-розыскной деятельности : сборник статей, Орел, 28 октября 2022 года. – Орёл: Орловский юридический институт Министерства внутренних дел Российской Федерации имени В.В. Лукьянова, 2022. – С. 91-94.

9. Титов, А.А. Цифровые финансовые инструменты как средства совершения преступлений: постановка проблемы / А.А. Титов // Научные труды Российской таможенной академии. Вып. 1: По материалам Международной научно-практической конференции «Шумиловские чтения – 2022», 25 ноября 2022 г. / отв. за вып. Д.А. Бражников. – М.: РИО Российской таможенной академии, 2022. – С. 222 – 226.

10. Титов, А.А. Отдельные вопросы использования криптовалюты в доказывании по уголовному делу (по законодательству Республики Беларусь) / А.А. Титов // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности. Сборник научных статей по материалам международной научно-практической конференции. Академия управления МВД России. – М., 2023. – С. 155-159.

11. Титов, А.А. К вопросу о механизме легализации (отмывания) денежных средств с использованием криптовалюты / А.А. Титов // Современное уголовно-процессуальное право - уроки истории и проблемы дальнейшего реформирования. Сборник материалов Международной научно-практической конференции. К 30-летию принятия Конституции РФ. В 2-х частях. Редколлегия: К.В. Муравьев [и др.]. – Орел, 2023. – С. 180-185.

12. Титов, А.А. О некоторых вопросах выявления и расследования преступлений, связанных с криптовалютами / А.А. Титов // Актуальные проблемы криминалистики и судебной экспертизы: сборник статей международной научно-практической конференции. – Иркутск: ФГКОУ ВО ВСИ МВД России, 2024. – С. 66-70.

13. Противодействие криптовалютным преступлениям в зарубежных странах : учеб. пос. / В.Ф. Васюков, А.Г. Волеводз, К.К. Клевцов, Э.Л. Сидоренко, А.А. Титов, А.Д. Цыплакова / под ред. докт. юрид. наук., проф. А.Г. Волеводза. – Москва: Юрлитинформ, 2025. – 504 с.

Результаты проведенного исследования изложены автором на всероссийских и международных конференциях, в том числе:

1) Международной научно-практической конференции «Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования» (Орел, Орловский юридический институт МВД России имени В.В. Лукьянова, 6–7 октября 2022 г.);

2) Международной научно-практической конференции «Шумиловские чтения – 2022» (Москва, Российская таможенная академия, 25 ноября 2022 г.);

3) Всероссийской научно-практической конференции «Советская и российская криминалистика: традиции и перспективы» (Москва, Московская академия Следственного комитета Российской Федерации, 2 февраля 2023 г.);

4) Международной научно-практической конференции «Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности» (Москва, Академия управления МВД России, 26 мая 2023 г.);

5) Международной научно-практической конференции «Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования» (Орел, Орловский юридический институт МВД России имени В.В. Лукьянова, 12–13 октября 2023 г.);

6) Международной научно-практической конференции «Актуальные проблемы криминалистики и судебной экспертизы», посвященной 105-летию Экспертно-криминалистической службы МВД России (Иркутск, Восточно-Сибирский институт МВД России, 6–7 июня 2024 г.);

7) Всероссийской научно-практической конференции «Актуальные вопросы производства предварительного следствия в современных условиях

совершенствования уголовно-процессуального законодательства» (Москва, Московский университет МВД России имени В.Я. Кикотя, 10 апреля 2025 г.);

8) I Всероссийских академических слушаний законов и законопроектов в сфере цифровой безопасности (Москва, Московский государственный институт международных отношений (Университет) МИД России, 11 апреля 2025 г.);

9) XIII Международной научно-практической конференции «Теория и практика расследования преступлений» (Краснодар, Краснодарский университет МВД России, 17 апреля 2025 г.);

10) II Всероссийских академических слушаний законов и законопроектов в сфере цифровой безопасности (Москва, Московский государственный институт международных отношений (Университет) МИД России, 13 мая 2025 г.).

Достоверность и объективность сделанных выводов обеспечены использованием соответствующей научно-теоретической и нормативной правовой основы, а также эмпирических данных, полученных в процессе подготовки настоящей работы.

Структура и объем исследования обусловлены его целью и задачами. Работа состоит из введения, двух глав, включающих в себя шесть параграфов, заключения, списка использованных источников и приложения.

ГЛАВА I. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ОТНОШЕНИИ И С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

§ 1. Криптовалютная среда как источник криминалистически значимой информации

Деятельность, состоящая в раскрытии и расследовании преступлений, неразрывно сопровождается поиском и последующим использованием криминалистически значимой информации. Это обусловлено тем, что информация представляет собой фундаментальную категорию, определяющую процессы познания, принятия решений и коммуникации.

Информация определяется как абстрактное понятие, представляющее собой структурированные данные, несущие потенциальную смысловую нагрузку. Происходя от латинского «informare», означающего «придавать форму», информация требует материального носителя для своего проявления и передачи[42]. Однако её фундаментальная ценность заключается не в физической форме представления, а в организованной структуре данных, позволяющей извлекать знания и делать умозаключения.

Содержание информации, являясь её семантической составляющей, отражает смысл, передаваемый сообщением[43]. В контексте следственной работы содержание информации играет определяющую роль в формировании картины преступления, установлении мотивов и идентификации лиц, причастных к совершению противоправных действий. Интерпретация следов, показаний свидетелей, результатов оперативно-розыскных мероприятий и судебных экспертиз – всё это сводится к извлечению содержания информации, скрытого за

---

[42] *Чернавский, Д. С.* Синергетика и информация. Динамическая теория информации. – М.: УРСС. ЛЕНАНД. 2017. - 304 с.

[43] *Ладов, В. А.* О понятии информации в контексте современных исследований по проблемам семантики и искусственного интеллекта / В. А. Ладов // Вестник Томского государственного университета. Философия. Социология. Политология. – 2013. – № 4 (24). – С. 26-32.

символами, знаками и сигналами. При этом эффективность извлечения информации напрямую зависит от компетенции следователя, его способности учитывать контекст, понимать специализированные термины и логически связывать разрозненные данные.

В этой связи нельзя не отметить справедливость суждения профессора А.С. Подшибякина о том, что криминалистика должна осваивать специфические закономерности возникновения следов преступления посредством внедрения в том числе технологических новшеств и достижений науки, а также расширения междисциплинарных связей с другими областями знаний[44].

Структурный анализ содержания информации выступает в качестве мощного инструмента, ориентированного на формализацию и автоматизацию процесса выявления скрытых взаимосвязей, логических противоречий и нетипичных закономерностей в больших объёмах данных. Например, изучение переписки подозреваемых с использованием методов обработки естественного языка может выявить закономерности, указывающие на их причастность к преступной деятельности. Такой подход не только способствует выявлению прямых признаков противоправного деяния, но и позволяет установить косвенные связи, мотивы и намерения, критически важные для понимания общей картины и построения доказательственной базы[45].

В своем исследовании отдельные зарубежные криминалисты отмечают, что обеспечение объективности расследования требует от следователя применения принципов критической оценки информации[46]. Подобное

---

[44] *Подшибякин, А. С.* Современная криминалистика и ее развитие / А. С. Подшибякин // Криминалистика и судебно-экспертная деятельность в условиях современности : Материалы Международной научно-практической конференции: в 2-х томах, Краснодарский университет МВД России, 26 апреля 2013 г. / Том I. – Краснодарский университет МВД России, 2013. – С. 3-15.

[45] *Черданцев, А. Ю.* Практические проблемы получения, анализа и последующей правильной интерпретации полученной цифровой криминалистически значимой информации / А. Ю. Черданцев // Эксперт-криминалист. – 2022. – № 4. – С. 26-29.

[46] *Conti, M.* Blockchain-Based Distributed and Secure Digital Forensic Investigation Systems / M. Conti, G. Kumar, C. Lal, R. Saha // Blockchains. Advances in Information Security. – Cham : Springer, 2024. – Vol. 105. – DOI: https://doi.org/10.1007/978-3-031-32146-7_11 (дата обращения: 14.03.2025).

утверждение обосновывает проведение всесторонней проверки поступающих данных, включающую в себя сравнительный анализ информации из независимых источников, а также применение специализированных криминалистических методов, направленных на выявление и нейтрализацию факторов, искажающих истинную картину произошедшего[47].

Информационный подход к следственной деятельности предполагает оценку каждого источника информации с точки зрения его способности уменьшать неопределённость в понимании обстоятельств преступления. Так, обнаружение редкого или уникального следа на месте преступления имеет существенно большую ценность для следствия, чем констатация фактов, согласующихся с уже имеющейся информацией, поскольку влечёт за собой существенное сужение круга возможных версий.

Довольно уместно в рассматриваемом ключе привести суждение бразильского криминалиста Л.Ф. Гомеса, который подчеркивает, что «…эффективность правоохранительной деятельности, в частности разведывательных, оперативных и экспертных мероприятий, напрямую зависит от степени интеграции, систематизации и аналитической обработки поступающей информации. Разрозненные и несистематизированные данные не могут служить надежной основой для принятия обоснованных решений, а, следовательно, требуют комплексного подхода к их сбору, анализу и интерпретации»[48].

Соглашаясь с мнением ученого, позволим себе предположить, что ценность информации, представляющая собой ее полезность для конкретного следователя при решении конкретной задачи, является весьма субъективным, но при этом критически важным параметром. В свою очередь ценность

---

[47] *Wang, M.* Lightweight and manageable digital evidence preservation system on Bitcoin / M. Wang, Q. Wu, B. Qin [и др.] // Journal of Computer Science and Technology. – 2018. – Vol. 33. – P. 568–586. – DOI: 10.1007/s11390-018-1841-4.

[48] *Gomes, L.F.* Direito penal estratégico / L.F. Gomes, R. Cervini. – 4. ed. – São Paulo : Revista dos Tribunais, 2008. – 656 p.

информации в следственной работе определяется ее способностью приблизить раскрытие преступления, установить виновных и обеспечить справедливость[49].

Актуальность, точность, полнота, доступность и формат представления информации – всё это факторы, влияющие на её ценность. Следуя логике, раскрытой профессором А.Ф. Лубиным в своей работе, становится очевидным, что несвоевременность, недостоверность или неадекватная форма представления информации нивелируют ее практическую значимость и могут негативно сказаться на эффективности расследования, провоцируя ложные умозаключения и замедляя процесс установления истины[50].

Эргономичность информации применительно к следственной работе подразумевает оптимизацию затрат на сбор, обработку и анализ информации с целью получения максимальной пользы. В теории принятия решений ценность информации определяется как разница между ожидаемым результатом (например, раскрытием преступления) при наличии информации и ожидаемым результатом при ее отсутствии[51]. Оценка ценности информации требует учёта не только потенциальных выгод, но и рисков, связанных с её неправильным использованием или недостоверностью. Следователь должен обладать навыками критического мышления, уметь оценивать надёжность источников информации и учитывать возможные предубеждения и мотивы лиц, ее предоставляющих. В свою очередь согласимся с мнением С.А. Машкова о том, что современные информационные реалии обусловливают необходимость криминалистического осмысления и широкого практического применения исследовательских

---

[49] *Nakayama, H.* Criminal Psychology in Japan / H. Nakayama. – Tokyo : University of Tokyo Press, 2015.

[50] *Лубин, А. Ф.* О версионном анализе исходной информации при расследовании преступлений / А. Ф. Лубин // Казанские уголовно-процессуальные и криминалистические чтения : Материалы Международной научно-практической конференции. В 2-х частях, Казань, 28 апреля 2022 г. / Редколлегия: Ю.Н. Кулешов (отв. ред.) [и др.]. Том Часть 1. – Казань: Общество с ограниченной ответственностью "ЮрЭксПрактик", 2022. – С. 173-182.

[51] *Шуклин, А. Е.* Особенности принятия информационных и тактических решений в сложных следственных ситуациях : диссертация на соискание ученой степени кандидата юридических наук / Шуклин Александр Евгеньевич. – Екатеринбург, 2012. – 211 с.

возможностей цифровых технологий в целях раскрытия и расследования преступлений[52].

Научные методы определения ценности информации, такие как статистический анализ, моделирование и экспертные оценки, могут быть использованы для принятия обоснованных решений о приоритетности различных направлений расследования и выборе оптимальных стратегий. Например, оценка вероятности успеха различных версий, основанная на статистических данных о раскрываемости аналогичных преступлений и экспертных оценках криминалистов, позволяет следователю более эффективно распределять ресурсы. В данном контексте профессор Н.П. Яблоков уместно упоминает о том, что следователю важно извлекать из среды не столько исчерпывающе полную информацию, сколько значимую в соответствующем контексте[53].

Как верно подмечает О.А. Васильева, инновационные преобразования современного общества, обусловленные развитием информационных технологий, появлением новых видов и носителей информации, а также интенсификацией информационных процессов, оказывают существенное влияние на следственную деятельность, кардинально усложняя ее[54]. Но существующие методы и инструменты, ориентированные на работу с информацией в традиционных формах, оказываются неэффективными в условиях цифровой среды, характеризующейся огромными объемами данных, высокой скоростью их распространения и возможностью сокрытия или искажения. В связи с этим возникает необходимость решения задач, основанных на использовании современных информационных технологий и специальных криминалистических знаний.

---

[52] *Машков, С. А.* «Большие данные» и криминалистика: возможности и перспективы / С. А. Машков // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 2(44). – С. 78-86.

[53] *Яблоков, Н. П.* К вопросу о криминалистическом мышлении / Н.П. Яблоков // Правовые проблемы укрепления российской государственности. - Томск, 2012. С. 156-159.

[54] *Васильева О. А.* Организационно-тактические основы проверки криминалистически значимой информации при расследовании преступлений: дис. … канд. юрид. наук. - Калининград, 2022. - 199 с.

Между тем эффективность предварительного расследования преступлений определяется не только способностью следователей получать информацию, имеющую значение для уголовного дела, но и их умением эффективно, в полном объеме проверять, оценивать и использовать ее при принятии процессуальных решений. Как подчеркнул профессор Р.С. Белкин, «…по сути весь процесс расследования представляет собой последовательность взаимосвязанных этапов анализа имеющейся информации, выбора адекватных этой информации приёмов и средств работы с доказательствами и их практического применения»[55].

Солидаризируясь с точкой зрения ученого, отметим необходимость четкой дифференциации упомянутых этапов. Представляется, что на *первом этапе* происходит критическое осмысление всей совокупности данных, доступных следователю на текущий момент расследования. Подобное осмысление включает в себя не только формальное изучение документов и показаний, но и выявление противоречий, нестыковок, а также установление связей между разрозненными фактами.

Необходимо подчеркнуть, что анализ информации должен осуществляться непрерывно, по мере поступления новых данных, что позволяет корректировать расследование и своевременно выявлять перспективные направления. Современные криминалистические методики делают акцент на применении методов аналитической разведки, позволяющих извлекать максимальную пользу из больших объёмов данных и выявлять скрытые закономерности[56].

Во время *второго этапа* на основе анализа имеющейся информации следователь определяет, какие оперативно-розыскные мероприятия и следственные действия необходимо провести для получения дополнительных доказательств и проверки имеющихся версий. Выбор приёмов и средств должен

---

[55] *Белкин Р.С.* Курс криминалистики. В 3 т. Т. 3: Криминалистические средства, приемы и рекомендации. – М.: Юристь, 1997. – С. 430.

[56] *Kim, J. H.* A Study on the Application of Digital Forensic Investigation for Cryptocurrency Crime / J. H. Kim, C. S. Park // Journal of Digital Forensics, Security and Law. – 2019. – Vol. 14, No. 2. – P. 45-62.

быть обусловлен спецификой расследуемого преступления, особенностями личности преступника, а также тактическими соображениями.

В современных условиях этот этап предполагает активное использование достижений науки и техники, в частности методов цифрового поиска, компьютерной экспертизы и других инновационных средств. Важным аспектом является соблюдение законности и этических норм при применении выбранных приёмов и методов.

Третий этап представляет собой непосредственное проведение оперативно-розыскных мероприятий и следственных действий, направленных на обнаружение, фиксацию и изъятие следов преступления. Важно обеспечить надлежащее процессуальное оформление полученных результатов, чтобы впоследствии их можно было использовать в суде. Также на этом этапе особое значение приобретает профессионализм следователя, его умение эффективно взаимодействовать с экспертами, специалистами и другими участниками процесса.

Важно понимать, что выделенные этапы не являются изолированными. Результаты каждого этапа влияют на последующие этапы, образуя замкнутый цикл. Например, результаты анализа информации определяют выбор методов и средств работы с доказательствами, а результаты применения этих методов и средств, в свою очередь, предоставляют новую информацию, которая требует анализа, и т. д. Эффективность предварительного расследования напрямую зависит от качества реализации каждого этапа и от налаженного взаимодействия между ними. Недостаточное внимание к анализу информации может привести к выбору неадекватных методов и средств, что, в свою очередь, негативно скажется на результатах расследования[57]. И наоборот, некачественное проведение следственных действий и оперативно-розыскных мероприятий

[57] *Гаврилов, Б. Я.* К вопросу о совершенствовании уголовной политики противодействия преступности в условиях информатизации общества: искусственный интеллект в уголовном судопроизводстве / Б. Я. Гаврилов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2025. – № 1 (69). – С. 262-265.

может привести к потере ценной информации и затруднить дальнейшую деятельность.

Видится, что предложенная Р.С. Белкиным этапность отражает динамичный и многогранный характер процесса расследования, подчёркивая важность постоянного анализа, адаптации и использования современных достижений науки и техники для достижения успеха в борьбе с преступностью[58].

Особое значение подобные суждения имеют в условиях стремительной технологической эволюции и появления новых форм преступной деятельности, когда традиционные методы расследования все чаще оказываются неэффективными, что требует применения принципиально иных подходов. Особенно остро эта проблема проявляется в случаях, когда преступления совершаются с использованием современных информационных технологий, где злоумышленниками активно применяются механизмы цифровой анонимизации для сокрытия следов своей деятельности.

В связи с этим возрастает роль криминалистически значимой информации, которая может быть получена в процессе тщательного изучения технологической инфраструктуры, используемой правонарушителями при совершении преступлений. В одной из своих работ профессор Ли Ван (Национальный университет Цинхуа, Пекин), подчеркивает следующее: «Преступность всегда адаптируется к новым условиям. В цифровую эпоху преступники используют технологию как оружие, маскируя свои действия и расширяя свои возможности. Информация, которую мы можем извлечь из технологической инфраструктуры, используемой этими преступниками, становится не просто инструментом расследования, а скорее компасом, который помогает нам ориентироваться в этом новом и сложном мире преступности»[59].

Именно детальный анализ аспектов подобного характера деятельности подозреваемых, используемого ими аппаратного и программного обеспечения,

---

[58] *Белкин Р.С.* Указ соч. С. 430.

[59] *Li, W.* Digital Forensics and Cybercrime in China / W. Li, Y. Zhang // Proceedings of the International Conference on Cybercrime and Digital Forensics. – Beijing : Tsinghua University Press, 2020. – P. 123-135.

иных элементов инфраструктуры может предоставить следователю незаменимые для доказывания сведения. Соответственно совершенствование средств и методов выявления, фиксации и анализа криминалистически значимой информации, извлекаемой из технологической инфраструктуры преступной деятельности, является одним из приоритетных направлений развития современной криминалистики.

В научных трудах отечественных ученых – В.Ф. Васюкова[60], А.Г. Волеводза[61], Ю.В. Гаврилина[62], А.В. Гриненко[63], Э.И. Дамирчиева[64], М.М. Долгиевой[65], С.И. Захарцева[66], И.Н. Кондрата[67], А.Н. Колычевой[68],

---

[60] *Васюков, В. Ф.* Преступления, совершаемые с использованием цифровых технологий: понятие и виды / В. Ф. Васюков, А. Г. Волеводз // Цифровое право : Учебник. – Москва : ООО Издательский дом "Юрлитинформ", 2024. – С. 525-540.

[61] *Волеводз, А. Г.* Международное сотрудничество в сфере уголовного судопроизводства по делам о преступлениях, совершенных с использованием криптовалюты: постановка проблемы / А. Г. Волеводз // Современное уголовно-процессуальное право - уроки истории и проблемы дальнейшего реформирования : Сборник материалов Международной научно-практической конференции. К 300-летию российской полиции, Орёл, 18–19 октября 2018 г. / Под редакцией Е.Б. Гришина. – Орёл, 2018. – С. 66-75.

[62] *Гаврилин, Ю. В.* Развитие методов цифровой криминалистики: пределы допустимости / Ю. В. Гаврилин // Уголовный процесс и криминалистика: теория, практика, дидактика : Сборник материалов VII Всероссийской научно-практической конференции, Рязань, 16 декабря 2021 г. – Рязань: Академия права и управления Федеральной службы исполнения наказаний, 2022. – С. 69-75.

[63] *Grinenko, A.* Comparative Legal Analysis of the Use of Electronic Format of Criminal Cases and the Procedure under the Code of Criminal Procedure of the Russian Federation / D. Ivanov, A. Grinenko, P. Fadeev [et al.] // Jurnal Cita Hukum. – 2024. – Vol. 12, No. 2. – P. 309-320. – DOI 10.15408/jch.v12i2.39691. – EDN OSCXUU.

[64] *Дамирчиев, Э. И.* Международный и зарубежный опыт криминализации противоправных деяний, связанных с использованием информационно- коммуникационных технологий / Э. И. Дамирчиев // Мировой судья. – 2024. – № 7. – С. 9-14.

[65] *Долгиева, М. М.* Теоретические основания уголовной политики в сфере оборота криптовалюты: дис. … д-ра юрид. наук / Долгиева Мадина Муссаевна. – Москва, 2023. – 474 с.

[66] *Захарцев, С. И.* Кибермафия как угроза нормальному человеческому существованию: рецензия-размышление по поводу монографии «Мировые тенденции и международное противодействие» / С.И. Захарцев, В.П. Сальников // Юрист-Правоведъ. – 2022. – № 3 (102). – С. 215–220.

[67] *Иванов, И. И.* Особенности предупреждения преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий / И.И. Иванов, И.Н. Кондрат // Мировой судья. – 2024. – № 12. – С. 2–9.

[68] *Колычева, А. Н.* Расследование преступлений с использованием компьютерной информации из сети Интернет : учебное пособие / А. Н. Колычева, В. Ф. Васюков. – Москва : Общество с ограниченной ответственностью "Проспект", 2025. – 200 с.

Э.Л. Сидоренко[69], О.Н. Тисен[70] – подробно исследуется проблематика цифровой трансформации преступности, а также рассматривают вопросы адекватности и эффективности мер, направленных на противодействие этой деятельности.

Однако, признавая перспективность данного направления, необходимо констатировать наличие определённых проблем, связанных с феноменальным ростом популярности новых финансовых инструментов. Несмотря на очевидный потенциал, заложенный в их развитии, следует с должным вниманием отметить существующую угрозу, обусловленную их стремительным распространением.

Как представляется, это оказывает существенное влияние на глобальные экономические процессы, а также на экономическую ситуацию в Российской Федерации, что привлекает пристальное внимание не только участников легитимного финансового сектора[71], но и представителей криминального мира, стремящихся использовать новые возможности в противоправных целях.

Указанное требует проведения углубленного изучения рисков и разработки эффективных мер по противодействию злоупотреблениям, направленных на поддержание стабильности и безопасности финансовой системы в целом и обеспечение прав и законных интересов граждан в частности. В связи с этим приоритетное значение приобретает углубленное исследование технологических основ, лежащих в основе цифровых активов, в частности криптовалют.

В криминологической литературе для обозначения преступлений, связанных с оборотом криптовалюты, предложен собирательный термин «криптопреступность», а также представлены его научные дефиниции. Не ставя перед собой задачу рассмотрения всех существующих определений, отметим позицию Э.Л. Сидоренко, согласно которой криптопреступность представляет

---

[69] *Сидоренко, Э. Л.* Криптовалюта как новый юридический феномен // Общество и право. - 2016. - № 3 (57). - С. 193-197.

[70] *Тисен, О. Н.* Противодействие финансированию терроризма и диверсий, совершаемых с использованием криптовалют : Серия: Библиотека криминалиста / О. Н. Тисен. – Москва : Издательский дом «Юрлитинформ», 2025. – 248 с.

[71] К началу 2025 года глобальная капитализация рынка криптовалют составила 3,19 трлн евро // https://coinmarketcap.com/?ysclid=m8alhxewyt731798258 (дата обращения: 14.03.2025).

собой «совокупность общественно опасных деяний, совершаемых в отношении либо с использованием продуктов блокчейн-технологий (криптовалюты, токенов) за определенный период на определенной территории»[72].

В свою очередь, исследуя этот вопрос в уголовно-правовой плоскости, М.М. Долгиева пришла к выводу о том, что под криптопреступлениями следует понимать «общественно опасные, виновные и наказуемые деяния, в которых криптовалюта выступает в качестве предмета или средства совершения преступления, нарушающие установленный порядок экономической, финансовой и информационной деятельности»[73].

Таким образом, представленные дефиниции свидетельствуют о едином понимании масштаба криптопреступности, охватывающей широкий спектр общественно опасных деяний, совершаемых как в отношении криптоактивов, так и с их использованием. Оба подхода подчеркивают, что криптопреступность, будучи феноменом, тесно связанным с технологией блокчейн, посягает на установленный правопорядок в экономической, финансовой и информационной сферах.

В целом соглашаясь с предложенными подходами к определению криптопреступности, необходимо отметить, что криминалистика рассматривает преступления как объект научного познания несколько иначе. Как известно, при криминалистическом изучении преступлений, в том числе их отдельных групп и видов, основное внимание уделяется закономерностям, проявляющимся в системе связей и отношений между структурными элементами преступной деятельности[74].

Криптопреступность как сложный социально-правовой феномен характеризуется вариативностью структуры и механизмов, обусловленных

---

[72] *Сидоренко, Э. Л.* Криптопреступность как новое криминологическое явление / Э. Л. Сидоренко // Общество и право. – 2018. – № 2(64). – С. 15-21.

[73] *Долгиева, М. М.* Теоретические основания уголовной политики в сфере оборота криптовалюты: дис. … д-ра юрид. наук / Долгиева Мадина Муссаевна. – Москва, 2023. – 474 с.

[74] *Коновалов, С. И.* Теоретико-методологические основы криминалистики (Современное состояние и проблемы развития): дис. … д-ра юрид. наук / Коновалов Станислав Иванович. – Волгоград, 2001. – 269 с.

многообразием форм использования криптовалют в преступной деятельности. Транснациональные схемы и организованные преступления, где криптовалюта выступает как предмет или инструмент противоправных действий, демонстрируют наиболее сложные алгоритмы реализации, что требует отдельного криминалистического осмысления. При этом редукция криптопреступности исключительно к категории киберпреступлений методологически некорректна, так как её специфика выходит за рамки классических преступлений в сфере компьютерной информации.

Кроме того, как верно подчеркивается А.Ю. Головиным и Е.В. Головиной, «…помимо специфики способов, применяемых на стадиях подготовки, совершения и сокрытия криптопреступлений, существенными криминалистическими особенностями обладают субъекты совершения таких деяний, личность жертв и их вовлеченность в процессы производства и обращения криптовалюты или различную преступную деятельность, связанную с криптовалютой, а также место, время и обстановка совершения таких деяний»[75].

В этой связи ключевое значение приобретает технологическая инфраструктура криптовалют, центральным элементом которой выступает «блокчейн». Согласно положениям стандарта ISO 22739, принятому Международной организацией по стандартизации[76], «блокчейн» представляет собой «распределённый реестр, формируемый последовательным добавлением блоков с использованием криптографической технологии и подтверждённый консенсусом»[77]. В своей работе зарубежный исследователь Т.Х. Рауд, стремясь к большей ясности, предлагает следующую иллюстрацию: «Для наглядности

---

[75] *Головин, А. Ю.* Задачи криминалистики в сфере противодействия криптопреступности / А. Ю. Головин, Е. В. Головина // Санкт-Петербургский международный криминалистический форум : Материалы международной научно-практической конференции, Санкт-Петербург, 10–11 июня 2024 г. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2024. – С. 119-126.

[76] В переводе с англ. – International Standard Organization; сокр. – ISO.

[77] International Organization for Standardization. Blockchain and Distributed Ledger Technologies-Vocabulary. – 2020. – URL: https://www.iso.org/obp/ui/en/#iso:std:iso:22739:ed-1:v1:en (дата обращения: 05.08.2024).

структуру блокчейна можно представить в виде паутины. Повреждение одного элемента не приводит к разрушению всей системы, поскольку децентрализованная архитектура позволяет обновлять и восстанавливать данные из множества источников, обеспечивая устойчивость и надёжность сети в целом»[78].

Таким образом, можно сделать вывод о том, что блокчейн выступает в качестве первичного источника криминалистически значимой информации, отражающей все операции, когда-либо совершённые с использованием конкретной криптовалюты. В свою очередь эффективное использование этой информации в целях раскрытия и расследования преступлений требует разработки специализированных методов ее выявления, фиксации, анализа и интерпретации, что, в свою очередь, обусловливает необходимость дальнейших исследований в области криминалистического обеспечения расследования преступлений рассматриваемого вида[79].

С учетом обозначенной актуальности вопроса следует акцентировать внимание на том, что впервые протокол, подобный блокчейну, был предложен американским криптографом Д. Чаумом в его диссертации 1982 г. под названием «Компьютерные системы, созданные, поддерживаемые и пользующиеся доверием взаимно подозрительных групп»[80]. Хотя в работе не была приведена полная реализация идеи сети блокчейна, она содержала многие ключевые аспекты, которые легли в основу дальнейших исследований математиков Д. Байера, С. Хабера и В. Сторнетта, описавших в 1991 г. криптографически

---

[78] *Raud, T.H.* Combating money laundering using cryptocurrencies: a comparative analytical study / T. H. A. Raud // Journal of the Center for Rule of Law and Anti-Corruption. – 2024. – № 1. – DOI: https://doi.org/10.70139/rolacc.2024.1.7.

[79] *El-Kadi, R. M.* Criminal Counteraction to Encrypted Digital Currencies and Artificial Intelligence Crimes: An Analytical Study in Egyptian and Comparative Legislation / R. M. El-Kadi // Journal of Shariah and Law. – 2022. – No. 89, Article 6. – URL: https://scholarworks.uaeu.ac.ae/sharia_and_law/vol2022/iss89/6 (дата обращеиня: 05.04.2025).

[80] *Jones, M.* Book Review: Tracers in the dark: The global hunt for the crime lords of cryptocurrency / M. Jones // International Journal of Cybersecurity Intelligence & Cybercrime. – 2024. – Vol. 7. – No. 1. – DOI: https://doi.org/10.52306/2578-3289.1161 (дата обращения: 05.04.2025).

защищённую цепочку блоков. Авторы тем самым создали систему, в которой временны́е метки документов нельзя было бы подделать[81].

В 1996 г. Д. Джексон и Б.К. Дауни создали электронную валюту «e-Gold», которая позволяла необратимо передавать право собственности на золото между пользователями веб-сайта[82]. Хотя намерения создателей были благими, очень скоро веб-сайт начал использоваться для легализации денежных средств, а также хищения личных данных. По этой причине многие учетные записи пользователей были заблокированы, а обмен «золотой» валютой остановлен[83].

В последующем, год спустя, А. Бэк представил концепцию системы «доказательства выполнения работы» (с англ. – «proof-of-work») под названием «Hashcash». Изначально разработанная для борьбы со спамом в электронной почте и предотвращения кибератак, система Hashcash по сути решила фундаментальную проблему, препятствовавшую развитию проектов виртуальных валют: обеспечение невозможности бесконечного копирования цифровых файлов и, как следствие, контроль над объёмом виртуальных денег в обращении. В частности, механизм «доказательства выполнения работы» позволил ограничить эмиссию криптовалюты, поскольку для её производства требовались значительные временны́е и энергетические ресурсы, затрачиваемые на решение сложных вычислительных задач. По утверждению С.К. Оранбурга

---

[81] *Bayer, D.* Improving the Efficiency and Reliability of Digital Time-Stamping / Dave Bayer, Stuart Haber, W. Scott Stornetta. – 1992. – Vol. 2. – P. 329-334.

[82] Под «веб-сайтом» по тексту нами понимается сайт сети Интернет, то есть совокупность программ для компьютерных устройств и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством сети Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать такие сайты. Страница сайта в сети Интернет (далее также – интернет-страница) – часть сайта, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети Интернет. См.: Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // Бюллетень Верховного Суда Российской Федерации. 2023. № 3. С. 3-8.

[83] Известный также как «Белая книга» (с англ. – «White Paper»).

была установлена прямая связь между стоимостью производства криптовалюты и затрачиваемой на это энергией[84].

В 1998 г. В. Дай, инженер-программист, предложил анонимную и распределенную систему электронных платежей под названием B-money[85]. Первоначально проект предусматривал создание реестра, который любой участник должен был обновлять для каждой выполненной транзакции. Для обеспечения конфиденциальности этот реестр должен был быть представлен открытыми ключами, которые указывали только сумму транзакции, а не личность пользователя, соответствующую самому ключу[86]. Кроме того, реестр не должен был контролироваться центральным органом. Однако возникла проблема так называемых «двойных расходов»: пользователь мог бы дважды отправить один и тот же B-money разным людям. По этой причине В. Дай разделил участников системы на «обычных пользователей» и «серверы» и только последним поручил задачу хранения копии реестров.

Таким образом, обычные пользователи могли бы выполнить проверку транзакции со случайной частью сервера и, в случае ошибки, отклонить ее. Однако идея B-money не была воплощена в жизнь, проект «остался на бумаге»[87]. В течение почти десяти лет идея распределённого реестра оставалась в стадии стагнации.

Сатоши Накамото 31 октября 2008 г. представил интернет-сообществу революционную концепцию, опубликовав документ «Биткоин: одноранговая электронная денежная система»[88]. Опираясь на предыдущие исследования в этой

---

[84] *Oranburg, S. C.* Cryptocurrency Regulation / S. C. Oranburg // A History of Financial Technology and Regulation: From American Incorporation to Cryptocurrency and Crowdfunding. – Cambridge: Cambridge University Press, 2022. – P. 129-152.

[85] *Sharad Mangrulkar, R.* Bitcoin / R. Sharad Mangrulkar, P. Vijay Chavan // Blockchain Essentials. – Berkeley, CA : Apress, 2024. – DOI: 10.1007/978-1-4842-9975-3_3 (дата обращения: 05.04.2025).

[86] *Böhme, R.* Bitcoin: Economics, technology, and governance / R. Böhme, N. Christin, B. Edelman, T. Moore // Journal of Economic Perspectives. – 2015. – Vol. 29, No. 2. – P. 213–238.

[87] *Zhang, S. T.* Bitcoin History and Purpose / S. T. Zhang // The Potential and Limitations of Bitcoin and Ethereum. – Cham : Palgrave Macmillan, 2024. – DOI: 10.1007/978-3-031-56783-4_1.

[88] В переводе с англ. – «Bitcoin: A Peer-to-Peer Electronic Cash System». https://bitcoin.org/bitcoin.pdf (дата обращения: 14.03.2025).

области, Накамото изложил принцип работы «блокчейна», заложив фундамент для нового этапа развития системы хранения и передачи «ценностей». В основе концепции был определен децентрализованный протокол «равный к равному» (от англ. – «peer-to-peer»), обеспечивающий генерацию криптографических единиц и верификацию транзакций посредством распределённого реестра, функционирующего как криптографически защищённая «главная книга»[89].

В начале своего пути проект Сатоши Накамото не вызвал особого интереса, а немногочисленные отзывы были преимущественно критическими. Однако, несмотря на имевшийся скепсис, американский программист Хэл Финни поддержал идею, после чего был реализован алгоритм Бикоина. Позднее Сатоши Накамото создал первый блок блокчейна («генезис-блок»), сгенерировав первые 50 единиц. Через несколько дней им была совершена первая транзакция – было отправлено 10 Биткоинов Хэлу Финни. Тем самым заявленная концепция была реализована на практике, а «алгоритм продемонстрировал свою жизнеспособность»[90].

Получив общественное признание, Биткоин[91] стал обозначаться как цифровая валюта, которая приобрела название с учетом принципа своего функционирования на основе криптографических методов[92]. В итоге стал популяризироваться термин «криптовалюта» (с англ. – «cryptocurrency»), в последующем обозначающий валютную единицу, использующую в своем обращении криптографические методы.

Именно по этой причине в настоящем исследовании мы используем указанный термин исключительно в единственном числе – «криптовалюта», так

---

[89] Следует отметить разнообразие аллегорий и метафор, которые отдельные авторы используют для объяснения принципов работы блокчейна – «библиотека», «кирпичный дом», «бухгалтерская книга», «счет в ресторане» и пр.

[90] *Ly, K. M.* Coining Bitcoin's 'legal-bits': Examining the regulatory framework for Bitcoin and virtual currencies / K. M. Ly // Harvard Journal of Law and Technology. – 2014. – Vol. 27, No. 2. – P. 587–608.

[91] Биткоин (от англ. Bitcoin, от bit – бит, определенная часть информации, и coin - монета).

[92] *Basynya, E. A.* Bitcoin Transaction Analysis System / E. A. Basynya, N. Karapetyants, M. Karapetyants // Program and Computer Software. – 2024. – Vol. 50 (Suppl. 2). – P. 104–112. – DOI: 10.1134/S0361768824700488.

как объектом правового регулирования исследования выступает не тот или иной конкретный токен, но именно феномен в его собирательном, родовом значении.

Рассмотрение криптовалюты как единого, целостного явления позволяет выявлять и систематизировать общие модели преступного поведения, которые, по своей сути, смежны к конкретной технологической реализации. Нельзя не учитывать и тот факт, что в общественном и профессиональном сознании данное понятие укоренилось именно в своей обобщающей, собирательной ипостаси. Оперирование термином в единственном числе отражает сложившуюся следственную практику и способствует смысловой цельности научного и профессионального дискурса, обеспечивая ясность и однозначность формулировок.

Появление и развитие криптовалюты как нового универсального финансового инструмента закономерно повлекло за собой создание специализированных бирж. Эти платформы были необходимы для торговли, обмена и хранения цифровых активов. Между тем их операционная модель, зачастую основанная на ограниченных ресурсах и недостаточной информационной безопасности, создавала благоприятную среду для незаконного получения доступа к программному обеспечению и первых преступлений, совершенных в отношении криптовалют[93].

Отсутствие понимания основателями бирж потенциальных угроз «взломов» приводило к серьезным ошибкам, которыми впоследствии и пользовались злоумышленники. Одним из примеров использования уязвимостей в программном коде стал инцидент с криптобиржей Bitfloor, в ходе которого незашифрованное хранение конфиденциальных данных пользователей привело к хищению значительного объёма криптовалюты. Подобные случаи стали закономерными, но при этом не получали широкой общественной огласки.

---

[93] *Zheng, B.* Identifying the vulnerabilities of Bitcoin anonymous mechanism based on address clustering / B. Zheng, L. Zhu, M. Shen [и др.] // Science China Information Sciences. – 2020. – Vol. 63, 132101. – DOI: 10.1007/s11432-019-9900-9.

Однако банкротство японской криптобиржи Mt.Gox в феврале 2014 г., некогда лидера рынка, через которую в 2013 г. проходило до 70% всех транзакций с криптовалютой, стало громким событием в криптовалютной индустрии. Биржа объявила о неплатёжеспособности, заявив о потере около 850 000 биткоинов, принадлежавших её клиентам. Среди причин, озвученных представителями Mt.Gox, была названа эксплуатация так называемой «гибкости транзакций»[94] в блокчейне Биткоина. Подобная особенность позволяла изменять идентификаторы транзакций, чем в итоге и воспользовались злоумышленники, инициируя повторные отправки криптовалюты. Инцидент с Mt.Gox не только выявил потенциальные уязвимости, связанные с гибкостью транзакций в протоколе Биткоин, но и определил значимость государственного контроля в этой сфере[95].

На ранних этапах развития криптовалютных технологий также наблюдались случаи их использования в противозаконной деятельности. В частности, функционирование онлайн-платформы «Шелковый путь» (с англ. – «Silk road»), обеспечивавшей международную торговлю наркотиками, стало одним из первых масштабных примеров использования криптовалют в преступных целях. Упоминания о подобных фактах в официальных документах правоохранительных органов сигнализировали о возможном возникновении проблем, связанных с использованием цифровых активов в незаконных финансовых операциях, что стало важным фактором для дальнейшего изучения и регулирования этой сферы[96].

---

[94] Гибкость транзакций – это свойство Биткоина, позволяющее изменять идентификатор транзакции (TXID) без изменения ее сути: отправитель, получатель и сумма остаются прежними. Это стало возможным благодаря определенным частям транзакции, которые можно было изменить, не аннулируя ее подпись.

[95] *Mezquita, Y.* Cryptocurrencies, systematic literature review on their current context and challenges / Y. Mezquita, M. Plaza-Hernández, M. Abbasi, J. Prieto // International Congress on Blockchain and Applications. – 2023. – Vol. 595. – P. 162-172.

[96] Только по официальным оценкам общий доход от продаж через этот магазин составил порядка 1,2 млрд долл., более 80 млн долл. было выручено в качестве комиссионных за услуги. Расследование по делу «Шёлковый путь» проводилось в течение двух лет при взаимодействии правоохранительных органов США, Исландии и Франции. Фактически, первые «звоночки» грядущей проблемы стали заметны уже в начале работы платформы в сети Даркнет. Именно

Можно сделать вывод, что «Шёлковый путь» представляет собой хрестоматийный пример использования архитектуры криптовалюты в качестве главного инструмента незаконной торговли. Используя маршрутизацию трафика через сеть Tor[97], платформа обеспечивала эффективное сокрытие IP-адресов пользователей. При этом сеть Даркнет (с англ. – Darknet), представляя собой сеть, функционирующую поверх сети Интернет, создавала благоприятную среду для сокрытия подпольного рынка, функционирующего вне контроля со стороны каких-либо государственных органов. Причем использование Биткоина в качестве единственного платёжного средства значительно усиливало анонимность транзакций.

Псевдонимный характер биткоин-адресов в сочетании с отсутствием централизованного органа управления облегчал сокрытие личности участников незаконных операций. Кроме того, использование динамически генерируемых адресов для каждой транзакции эффективно затрудняло отслеживание финансовых потоков, связанных с незаконной деятельностью. Ограниченность информации, доступной для анализа многочисленных транзакций, которые приходилось сопоставлять вручную, представляла серьезную проблему для сотрудников правоохранительных органов.

Иными словами, технологии, призванные обеспечить конфиденциальность и децентрализацию, непреднамеренно послужили инструментом для сокрытия преступных операций, значительно усложнив противодействие финансовым преступлениям в зарождающейся криптоиндустрии. Это связано с тем, что архитектура криптовалюты стала уникальной в своем роде технологией, с

тогда в официальных документах стали упоминаться случаи использования криптовалюты в преступных целях. Что стало тревожным предзнаменованием более масштабного применения нового финансового инструмента. Abate, C. Online-Durchsuchung, Quellen-Telekommunikationsüberwachung und die Tücke im Detail: Einfluss rechtlicher und technischer Entwicklungen auf verdeckte Online-Ermittlungen zur Gewährleistung der Inneren Sicherheit / C. Abate // Datenschutz und Datensicherheit. – 2011. – Heft 2. – S. 122–125.

[97] Tor (сокр. от англ. – The Onion Router, буквально «луковый маршрутизатор») – программное обеспечение с открытым исходным кодом, использующее систему прокси-серверов, которая позволяет устанавливать анонимное сетевое соединение, защищённое от контроля со стороны правоохранительных органов.

которой ранее не приходилось соприкасаться оперативным работникам и следователям. Созданные специализированные подразделения (отделы, группы, команды) по выявлению преступлений в сети Даркнет[98] задачу по отслеживанию цепочки цифровых следов в сети блокчейн решить не смогли[99].

Действительно, до этого момента все вопросы отслеживания транзита денежных средств с помощью банковских организаций тем или иным образом касались установления лиц, обналичивших и (или) разместивших на счетах в банках наличные деньги.

Даже если при этом использовались посредники («дропы», «мулы», «смурфы»), не имеющие непосредственного отношения к преступным формированиям, существовала возможность их физического и цифрового контроля, благодаря чему становилось возможным оперативными методами установить лиц, незаконно обоьгигатившихся, или участвующих в процессах функционирования преступных организаций[100]. То есть механизмы выявления и документирования противоправной деятельности со стороны правоохранительных органов были выработаны, и в зависимости от юрисдикции

---

[98] Даркнет (англ. DarkNet, также известен как «Скрытая сеть», «Тёмный интернет», «Тёмная сеть», «Теневая сеть», «Тёмный веб») – скрытая сеть, не индексируемая поисковыми системами, которая представляет собой систему не связанных между собой виртуальных туннелей, предоставляющих передачу данных в зашифрованном виде. Даркнет отличается от других распределённых одноранговых сетей, так как файлообмен происходит анонимно (поскольку IP-адреса недоступны публично).

[99] Например, еще в 2018 г. Европол сформировал собственную специализированную команду для работы в Даркнете. Соединенные Штаты Америки, в свою очередь, создали Объединенную оперативную группу по борьбе с опиоидами в Даркнете, известную как J-Code (с англ. – Joint Criminal Opioid Darknet Enforcement Team). В Индии в рамках стратегии безопасности, принятой в 2020 г., была создана специализированная команда в составе Национальной организации технических исследований в целях противодействия преступности в Даркнете.

[100] *Akartuna, E. A.* A Holistic Network Analysis of the Money Laundering Threat Landscape: Assessing Criminal Typologies, Resilience and Implications for Disruption / E. A. Akartuna, S. D. Johnson, A. Thornton // Journal of Quantitative Criminology. – 2024. – DOI: 10.1007/s10940-024-09594-3 (дата обращения: 05.04.2025).

и имеющихся у них на вооружении средств и методов они с той либо иной степенью эффективности успешно использовались[101].

Для обеспечения конспирации преступные организации были вынуждены направлять значительные ресурсы на перемещение финансовых активов, поскольку полная анонимность была недостижима даже при использовании альтернативных способов передачи денег. Так, в системе «Хавала» лицо, отправляющее денежные средства, должно было лично или через посредника связаться с «хаваладаром», который, в свою очередь, взаимодействовал с коллегой в другой стране[102]. При использовании в преступной деятельности предоплаченных банковских карт, которые перемещались через границу с применением мер маскировки, пополнение счетов осуществлялось посредством определенных банковских операций, поддающихся оперативному отслеживанию на международном уровне[103].

Перемещение через границу с помощью «стада мулов» – группы людей, часто используемых для перевозки небольших сумм наличности, при надлежащем оперативном сыске также довольно быстро выявлялось благодаря применению комплекса оперативно-розыскных и следственных методов[104].

Между тем создание криптовалют значительно упростило процессы вывода денежных потоков «из-под крыла» национальных юрисдикций. Система виртуальных активов, по яркому выражению отдельных зарубежных

---

[101] *Calafos, M. W.* Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency / M. W. Calafos, G. Dimitoglou // Principles and Practice of Blockchains / ed. K. Daimi [и др.]. – Cham : Springer, 2023. – DOI: 10.1007/978-3-031-10507-4_12 (дата обращения: 05.04.2025).

[102] *Система «Хавала»* (или «Хаваладар» – человек, занимающийся «хавалой») – это неформальная система денежных переводов, которая существует вне традиционных банковских каналов. Она уходит корнями в древние торговые сети и до сих пор используется в различных частях света, особенно в странах Ближнего Востока, Африки и Азии.

[103] Guidance for a Risk-Based Approach for Money or Value Transfer Services // FATF. – Paris. - 2016. – URL: www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html

[104] *Wang, H. M.* Cryptocurrency is new vogue: a reflection on money laundering prevention / H. M. Wang, M. L. Hsieh // Security Journal. – 2024. – Vol. 37. – P. 25–46.

криминалистов, «стали ключом к «ящику Пандоры», в котором хранилось множество злодеяний, требующих своего финансирования»[105].

В работе Е.А. Русскевича и И.И. Малыгина справедливо отмечается, что «для правоохранительных органов криптовалюты ознаменовали принципиально новый этап в борьбе с преступностью. С одной стороны, криптовалюты стали активно использоваться в гражданском обороте законопослушными гражданами и хозяйствующими субъектами, в том числе как инструмент хранения капитала, что поставило задачу их надлежащей правовой защиты. С другой – децентрализованный характер и анонимность криптовалют изменили механизм совершения многих традиционных преступлений, раскрытие и расследование которых стало чрезвычайно трудноразрешимой задачей» [106].

Преимущества использования криптовалюты в преступной деятельности вскоре оценили транснациональные организованные преступные сообщества, которые создали развернутую криптовалютную сеть для легализации преступных доходов с помощью технологии блокчейн. Масштаб проблемы был настолько очевидным, что отдельные преступные схемы стали пристально изучаться международными правоохранительными организациями[107].

В частности, Группа разработки финансовых мер борьбы с отмыванием денег[108] в 2014 г. опубликовала обзорный отчет, в котором указала на необходимость для стран и финансовых институтов выявлять и оценивать риски легализации преступных доходов и финансирования терроризма, возникающие в связи с развитием и использованием виртуальных активов[109]. В глоссарии

---

[105] Agarwal, U. Blockchain and crypto forensics: Investigating crypto frauds / U. Agarwal, V. Rishiwal, S. Tanwar, M. Yadav // International Journal of Network Management. – 2023. – Vol. 34. – DOI: https://doi.org/10.1002/nem.2255

[106] *Русскевич, Е.А.* Преступления, связанные с обращением криптовалют: особенности квалификации / Е.А. Русскевич, И.И. Малыгин // Право. Журнал Высшей школы экономики. – 2021. – № 3. – С. 106–125.

[107] *Khan, S.* Network forensics: review, taxonomy, and open challenges / S. Khan, A. Gani, A.W.A. Wahab [и др.] // Journal of Network and Computer Applications. – 2016. – Vol. 66. – P. 214–235.

[108] Financial Action Task Force, FATF, далее – ФАТФ.

[109] Virtual Currencies: Key Definitions and Potential AML/CFT Risks [Электронный ресурс] : [доклад]. – June 2014. – [S. l.]: FATF, [2014]. – URL: https://www.fatf-gafi.org/content/dam/fatf-

документа определяется, что «криптовалюта – это основанная на математических принципах децентрализованная конвертируемая валюта, которая защищена с помощью криптографических методов, то есть использует криптографию для создания распределённой, децентрализованной и защищённой информационной экономики»[110].

Таким образом, ФАТФ не только обратил внимание на вопросы контроля виртуальных активов, но и дал понятие «криптовалюты» как разновидности цифровой валюты. Уже на тот момент было понятно, что традиционные методы получения криминалистически значимой информации перестали быть актуальными в условиях проведения оперативно-розыскных (разведывательных) мероприятий при выявлении преступлений, связанных с цифровыми активами[111].

Специалисты в области кибербезопасности осознали необходимость адаптации существующих криминалистических подходов к новым реалиям цифровой среды, в частности, к особенностям обращения криптовалют[112]. Сложность выявления и пресечения преступлений, связанных с использованием виртуальных активов, обусловило активный поиск новых инструментов и методов, способных эффективно противодействовать этому типу угроз[113].

Учитывая потребности практики, в научном сообществе стали активно проводиться исследования, связанные с созданием специализированных программных продуктов и аналитических платформ в целях отслеживания транзакций в блокчейне, идентификации участников операций, а также выявления признаков подозрительной активности пользователей. Например, в

---

gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (дата обращения: 27.10.2024).

[110] Там же.

[111] *Васюков, В. Ф.* Понятие и виды криптовалют / В. Ф. Васюков, А. А. Титов // Противодействие криптовалютным преступлениям в зарубежных странах. – Москва : ООО Издательский дом "Юрлитинформ", 2025. – С. 43-65.

[112] *Сидоренко, Э. Л.* Криминологические риски оборота криптовалюты и проблемы ее правовой идентификации / Э. Л. Сидоренко // Библиотека криминалиста. Научный журнал. – 2016. – № 3(26). – С. 148-154.

[113] *Hou, Y.* A survey on digital forensics in Internet of Things / Y. Hou, J. Li, J. Yu, W. Shi // IEEE Internet of Things Journal. – 2020. – Vol. 7, No. 1. – P. 1-15.

2014 г. компания Chainalysis[114] презентует одну из первых коммерческих аналитических платформ «Reactor» с внедренной «базой данных атрибуции»[115], с помощью которой устанавливались закономерности криптовалютного оборота с визуализацией аналитических данных в виде фигурных графов. На тот момент этот инструмент был уникальным и пользовался большим спросом у правоохранительных органов, несмотря на его высокую стоимость[116].

По утверждению знатока в области исследования криптовалют Н. Фурно «…визуализация графов транзакций в Chainalysis Reactor была лишь второстепенным преимуществом. Его истинная ценность заключалась в динамичной, постоянно обновляемой базе данных атрибуций, которая служила основой для идентификации различных цифровых объектов в криптопространстве»[117].

Довольно уместно в этом случае утверждать, что появился эффективный криминалистический инструмент, позволяющий выявлять информацию, представляющую значение для раскрытия и расследования «криптовалютных инцидентов»[118]. Но вскоре в иностранной оперативной и следственной практике стали использоваться и альтернативные инструменты – Elliptic, CipherTrace,

---

[114] Основателями стали Д. Левин и М. Гронагер, которые стали реализовывать идею после резонанса вокруг многомиллиардного хищения с криптовалютной биржи Mt. Gox. // https://www.chainalysis.com/wp-content/uploads/2023/05/chainalysis-2022-soc3-final-report.pdf (дата обращения: 05.04.2025).

[115] База данных атрибуции (attribution database) — это специализированная база данных, которая хранит и систематизирует информацию о владельцах, контролирующих конкретные адреса в блокчейне. В контексте анализа криптовалютных транзакций атрибуция — это процесс связывания криптографических адресов с реальными субъектами, такими как физические лица, организации, сервисы или даже отдельные программы.

[116] В каждом отдельном случае сотрудники, уполномоченные проводить расследование преступлений, связанных с криптовалютами, получали разрешение у руководства на оплату услуги из бюджета правоохранительного органа (США, Канада, Великобритания и др.). Позднее отдельные компании стали предоставлять возможности по использованию своим программным обеспечением за абонентскую оплату.

[117] *Furneaux, N.* There's No Such Thing as Crypto Crime: An Investigative Handbook / N. Furneaux // URL: https://Theres-Such-Thing-Crypto-Crime/dp/1394164823#

[118] Так, например, благодаря полученной информации от Chainalysis, отдел уголовных расследований Налогового управления США изъял 50 676 биткоинов (3,36 млрд долл.) у Д. Чжуна, признавшего себя виновным в хищении биткоинов в сентябре 2012 г. // Chainalysis in Action: Department of Justice Announces Second-Largest Ever Crypto Seizure // https://www.chainalysis.com/blog/james-zhong-silk-road-hack-seizure/ (дата обращения: 14.03.2025).

которые, хотя и имели схожие с Chainalysis Reactor функции, однако здесь применялись несколько иные методологические подходы[119].

Причем выбор конкретного криминалистического инструментария для анализа блокчейн-транзакций определялся прежде всего двумя основополагающими факторами: во-первых, предпочтениями, методиками и опытом, которыми руководствовались сотрудники правоохранительных органов в своей оперативной деятельности; во-вторых, глубиной охвата и уровнем точности базы данных, формируемой выбранным программным обеспечением. В своем исследовании Дж. Шарфман констатирует, что «подобная вариативность позволила подбирать наиболее оптимальный продукт для исследования блокчейна»[120].

Применение подобных инструментов стало важнейшей частью раскрытия преступлений, связанных с криптовалютой. В этом контексте показателен пример проведения успешной международной тактической операции «Bayonet», в ходе которой на территории Королевства Нидерландов была прекращена деятельность двух крупнейших интернет-магазинов, реализующих наркотики с использованием криптовалют. Причем согласно заранее разработанной оперативной комбинации сначала была прекращена деятельность одного магазина – «AlphaBay», который насчитывал более 200 тысяч пользователей и 40 тысяч продавцов. Деятельность же второго магазина – «Hansa» – была остановлена только спустя месяц. Это было осуществлено для того, чтобы установить причастность к преступной деятельности в том числе пользователей «AlphaBay», которые были вынуждены после закрытия платформы обращаться к сервисам «Hansa». Тактическая комбинация сработала, так как сразу после

---

[119] Также стали популярны такие аналитические программы, как CipherTrace (США) (приобретена Mastercard), Coinfirm (Польша), Scorechain (Люксембург), Merkly (США), Nansen (Сингапур), TRM Labs (США), Bware Labs (Румыния) и др.

[120] *Scharfman, J.* Introduction to Cryptocurrency and Digital Asset Fraud and Crime / J. Scharfman // The Cryptocurrency and Digital Asset Fraud Casebook. – Cham : Palgrave Macmillan, 2023. – DOI: 10.1007/978-3-031-23679-2_1 (дата обращения: 05.04.2025).

начала операции стало наблюдаться восьмикратное увеличение пользователей оставшегося магазина[121].

С учетом того что серверы Hansa были расположены в юрисдикции Нидерландов, национальные оперативные службы при участии сотрудников из семи стран санкционировали физический и технический захват магазина и установили негласное оперативно-техническое наблюдение за продолжающейся деятельностью уже под своим контролем. Соответственно финансовые связи между клиентами и менеджерами незаконной торговли могли быть установлены только посредством аналитических инструментов блокчейна. В течение месяца были установлены все транзакции «оптовых» и «розничных» продавцов[122].

В условиях быстрого развития цифровых технологий и активного использования криптовалют в финансовой системе, их регулирование становится важным вопросом для обеспечения национальной безопасности[123]. В этой связи улучшение криминалистических методов для раскрытия и расследования преступлений, связанных с криптовалютными операциями, становится одной из ключевых задач для правоохранительных органов. Это требует разработки новых подходов, технологий и методик, которые позволят эффективно отслеживать, анализировать и пресекать такие преступления[124].

---

[121] *Baravalle, A.* Dark Web Markets: Turning the Lights on AlphaBay / A. Baravalle, S. Lee // 19th International Conference, Dubai, United Arab Emirates, November 12-15, 2018, Proceedings, Part II. – 2018. – DOI: 10.1007/978-3-030-02925-8_35 (дата обращения: 14.03.2025).

[122] Drugs and the darknet Perspectives for enforcement, research and policy European Monitoring Centre for Drugs and Drug Addiction, 2017. Praça Europa 1, Cais do Sodré, 1249–289 Lisbon, Portugal / https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf (дата обращения: 14.03.2025).

[123] Подобные вопросы приобретают особую актуальность в странах, где экономические ограничения и высокий уровень инфляции способствуют использованию криптовалют для осуществления международных транзакций. Так, например, в июле 2024 г. Правительством Нигерии было инициировано судебное разбирательство по факту незаконной банковской деятельности криптобиржей Binance, ставшей угрозой для и так не совсем стабильной экономики. Nigerian central bank alleges unauthorized transactions by Binance // https://cointelegraph.com/news/cbn-criticizes-binance-unauthorized-banking-nigeria (дата обращения: 14.03.2025).

[124] *Васюков, В. Ф.* Понятие и виды криптовалют / В. Ф. Васюков, А. А. Титов // Противодействие криптовалютным преступлениям в зарубежных странах. – Москва : ООО Издательский дом "Юрлитинформ", 2025. – С. 43-65.

В научном сообществе сформировалась позиция о перспективной роли криминалистики как интегратора, способного объединить потенциал дисциплин уголовно-правового цикла для существенного повышения эффективности борьбы с преступностью, совершаемой в сфере цифровой экономики[125]. Данная концепция предполагает, что криминалистика, обладая инструментами выявления, раскрытия и расследования преступлений, способна аккумулировать и систематизировать знания, накопленные в рамках уголовного права, уголовного процесса, криминологии и оперативно-розыскной деятельности, для разработки комплексных стратегий противодействия преступлениям, характерным для цифрового пространства. Интегративная функция криминалистики в таком контексте предполагает не только адаптацию существующих методов и средств к новым видам преступной деятельности, но и формирование методов, учитывающих особенности цифровой среды, трансграничный характер преступлений и необходимость защиты прав и законных интересов физических и юридических лиц.

Между тем в условиях растущей криминализации сферы криптовалют наблюдается тенденция к формированию подразделений в правоохранительных органах различных стран. Данные структуры создаются как в форме отдельных подразделений, специализирующихся на расследовании криптопреступлений, так и в рамках уже существующих отделов (управлений), занимающихся противодействием киберпреступности[126].

---

[125] *Сотников, К. И.* Потенциал современной криминалистики и показатели раскрытия преступлений / К. И. Сотников // Актуальные проблемы раскрытия и расследования преступлений : сборник материалов Международной научно-практической конференции, Екатеринбург, 29 сентября 2023 г. – Екатеринбург: Уральский юридический институт Министерства внутренних дел Российской Федерации, 2023. – С. 104-110; *Степаненко, Д. А.* Цифровизация как фактор и условие развития современной криминалистики / Д. А. Степаненко, А. А. Митрофанова // Российский следователь. – 2023. – № 4. – С. 16-22; *Кустов, А. М.* К вопросу о «цифровой» криминалистике / А. М. Кустов // Цифровые технологии в юриспруденции: генезис и перспективы : Материалы I Международной межвузовской научно-практической конференции, Москва, 28 февраля 2020 г. – Москва: Красноярский государственный аграрный университет, 2020. – С. 90-94 и др.

[126] Примером первого подхода является опыт создания отдела по расследованию криптопреступлений в структуре Департамента по борьбе с экономическими преступлениями Королевской полиции Малайзии, Объединённого центра по борьбе с киберпреступностью при

В целом эта тенденция, охватывающая различные юрисдикции, свидетельствует о растущем признании правоохранительными органами необходимости консолидации специализированных знаний и инструментов для эффективного противодействия криптопреступности на национальном уровне.

Кроме того, активизировалось международное полицейское сотрудничество в области обмена криминалистически значимой информацией и передовым опытом в сфере раскрытия и расследования рассматриваемой группы преступлений. Так, Международной организацией уголовной полиции (далее – Интерпол) в структуре Центра кибербезопасности, базирующегося в Сингапуре, создана спецгруппа по оказанию содействия правоохранительным органам в расследованиях, связанных с цифровыми активами[127].

Инициированный Интерполом проект «Серебряное уведомление» («Silver Notice») знаменует собой важный шаг в развитии международной системы обмена информацией, имеющей решающее значение для раскрытия, расследования и судебного преследования за криптопреступления. Эта инициатива, реализуемая через национальные центральные бюро Интерпола, представляет собой стандартизированный механизм направления запросов о предоставлении информации, ориентированный на выявление, отслеживание и возврат активов, полученных в результате преступной деятельности, в том числе связанной с использованием криптовалют[128].

Министерстве внутренних дел Австралийского Союза, формирование Национальной группы по борьбе с криптовалютами при Министерстве юстиции Соединенных Штатов Америки и др. Второй подход нашел отражение в расширении полномочий и компетенций существующих структур. Примером может служить дополнение функций Управления по расследованию преступлений против информационной безопасности и интеллектуальной собственности главного следственного управления центрального аппарата Следственного комитета Республики Беларусь, Третьего отдела кибербезопасности Почтовой полиции Итальянской Республики, Отдела по расследованию экономических преступлений Национального следственного управления Республики Корея, Центрального управления по борьбе с киберпреступностью Федеративной Республики Германия и т.д.

[127] Ранее Интерполом была создана своя модель криптовалюты для более глубокого понимания механизмов рынка и, как следствие, повышения эффективности работы с сетями блокчейн при расследовании преступлений, совершаемых в криптовалютной среде.

[128] Возврат преступных доходов из-за рубежа через задействование межведомственных сетей по возврату активов – Париж, ФАТФ, 2023. http://www.fatf-

В целях усиления противодействия криптопреступности на международном уровне Управление ООН по наркотикам и преступности (УНП ООН) и Королевская полиция Малайзии в 2022 г. при финансовой поддержке правительства Японии инициировали создание первой в Юго-Восточной Азии специализированной лаборатории, задачей которой стало расширение оперативных возможностей полиции в области расследования, анализа и конфискации активов, связанных с криптовалютными преступлениями. В частности, сотрудники лаборатории на регулярной основе привлекаются к проведению курсов подготовки сотрудников оперативных и следственных органов для получения навыков работы с криминалистически значимой информации, выявленной в сети блокчейн[129].

С развитием цифровых технологий и ростом популярности криптовалют вопросы их регулирования приобретают всё большее значение для обеспечения безопасности как на международном, так и на национальном уровнях. В связи с этим криминалистическое обеспечение раскрытия и расследования преступлений, связанных с криптовалютами, развивается в различных направлениях.

В соответствии с позицией, обозначенной В. А. Ализаде и А. Г. Волеводзом, одним из приоритетных направлений стало формирование надлежащей регуляторной модели финансовых отношений, возникающих между пользователями криптовалют, и разработка комплекса соответствующих мер, направленных на противодействие противоправным действиям в этой сфере[130].

Ввиду отсутствия унифицированных нормативных рамок, регулирующих обращение криптовалют в различных юрисдикциях, международные

---

gafi.org/publications/Methodsandtrends/recovering-proceeds-crime-inter-agency-networks.html (дата обращения: 14.03.2025).

[129] UNODC opens the first cryptocurrency analysis laboratory in Southeast Asia // https://www.unodc.org/roseap/en/malaysia/2022/05/cryptocurrency-analysis-laboratory/story.html (дата обрщения: 14.03.20205).

[130] *Ализаде, В. А.* Неприменение ст. 174.1 Уголовного кодекса РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов / В. А. Ализаде, А. Г. Волеводз // Наркоконтроль. – 2018. – № 1. – С. 5-13.

правоохранительные организации стали активно разрабатывать систему методов контроля за этой деятельностью[131].

В контексте противодействия криптопреступлениям одним из определяющих элементов регуляторной стратегии, формирующим основу для накопления криминалистически значимой информации, стала политика ФАТФ, направленная на всестороннюю интеграцию сферы виртуальных активов в существующую систему противодействия отмыванию доходов, полученных преступным путем, финансированию терроризма и распространения оружия массового уничтожения (ПОД/ФТ/ФРОМУ)[132]. Данный подход предполагает не только адаптацию действующих стандартов и рекомендаций к специфическим особенностям криптовалют, но и разработку правил, направленных на эффективное регулирование данного сегмента финансовой системы[133].

В регуляторной стратегии ФАТФ центральное место занимает так называемое «Правило путешествий». Это правило, применявшееся в отношении традиционных финансовых институтов, в настоящее время распространяется на поставщиков услуг виртуальных активов (далее – ПУВА)[134], обязывая их собирать и передавать информацию об отправителях и получателях

---

131 *Титов, А.А.* Понятие, признаки и правовая природа цифровых финансовых активов: уголовно-правовой аспект / А. А. Титов // Пролог: журнал о праве. – 2022. –№ 4(36). – С. 105-113.

132 International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF. – Paris, France. 2025 // URL: www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (дата обращения: 05.04.2025).

133 *Levi, M.* Understanding the laundering of organized crime money / M. Levi, M. Soudijn // Crime and Justice. – 2020. – Vol. 49. – P. 579–631. – DOI: 10.1086/708047.

134 Провайдер услуг в сфере виртуальных активов - это любое физическое или юридическое лицо, которое осуществляет на коммерческой основе один или более из перечисленных видов деятельности или операций для или от имени другого физического или юридического лица: 1) обмен виртуальных активов на фиатную валюту и обратно; 2) обмен между одной или более формами виртуальных активов; 3) перевод виртуальных активов; 4) ответственное хранение и/или управление виртуальными активами или инструментами, позволяющими контролировать виртуальные активы; и 5) участие в предоставлении и предоставление финансовых услуг, связанных с предложением и/или продажей виртуальных активов эмитента. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. – Paris, France. 2021 // URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (дата обращения: 14.03.2025).

криптовалютных транзакций. Соответственно указанные сведения должны аккумулироваться благодаря обязательной аутентификации личности абонентов путем сбора их полных имен, адресов проживания и реквизитов счетов отправителя и получателя (правило «Знай своего клиента», с англ. – «know your customer», далее – KYC)[135].

Как справедливо отмечается в работе индийских криминалистов Д. Халдера и А.А. Сайеда, «…в контексте формирования эффективной глобальной системы противодействия преступлениям в секторе виртуальных активов внедрение «Правила путешествий» является обязательным условием. Эффективное применение этого регуляторного инструмента способствует минимизации рисков, связанных с финансовыми злоупотреблениями, повышает уровень доверия к операциям с виртуальными активами и легитимизирует их функционирование в парадигме общественного и регуляторного признания»[136].

В результате создаются благоприятные условия для повышения эффективности работы оперативных и следственных органов за счёт отслеживания транзакций и идентификации субъектов, вовлечённых в незаконные операции. При этом о значимости указанных правил упоминается в работе профессора М. Наззари. По мнению автора, «…решающее значение приобретает обеспечение строгого соблюдения конфиденциальности данных, передаваемых в рамках реализации «Правил путешествий»[137].

Стремительное увеличение количества криптовалют и их использование в различных преступных схемах обусловило необходимость разработки новых подходов к системе противодействия транснациональной организованной

---

[135] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. – Paris, France. 2021 // URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (дата обращения: 14.03.2025).

[136] *Halder, D.* Legal Challenges to Cryptocurrency and its Guardian-Less Victims in India: A Critical Victimological Analysis / D. Halder, A. A. Saiyed // International Annals of Criminology. – 2022. – Vol. 60, No. 1. – P. 79-98. – DOI: 10.1017/cri.2022.6.

[137] *Nazzari, M.* From payday to payoff: Exploring the money laundering strategies of cybercriminals / M. Nazzari // Trends in Organized Crime. – 2023. – DOI: 10.1007/s12117-023-09505-w.

преступности[138]. Рекомендации ФАТФ, направленные на регулирование этой сферы, стали важным этапом в формировании правовой базы, направленной на противодействие отмыванию денег, финансированию терроризма и распространению оружия массового уничтожения.

По уместному замечанию Д.А. Кунева «…государствам предписано срочно принять законодательные и практические шаги, направленные на предотвращение злоупотребления виртуальными активами, включая оценку и понимание связанных с ними рисков, что также нашло отражение в принятой ФАТФ в 2019 г. пояснительной записке к 15-й рекомендации»[139]. Причем реализация этих рекомендаций в национальном законодательстве позволила укрепить систему финансового мониторинга и повысить прозрачность операций с криптовалютами[140].

В одной из своих работ П.А. Литвишко обоснованно утверждает, что положения руководства ФАТФ, касающиеся лицензирования и регистрации ПУВА, рассматриваются как ориентир при определении правил установления и осуществления более широкой территориальной и экстерриториальной

---

[138] *Бессонов, А.А*. Проблемные вопросы установления признаков организованной группы по преступлениям, совершенным с использованием информационно-телекоммуникационных технологий / А. А. Бессонов // Журнал российского права. – 2024. – Т. 28, № 1. – С. 108-119.

[139] *Кунев, Д. А.* Международно-правовые стандарты противодействия криминальному обороту криптовалют и иных виртуальных активов / Д. А. Кунев // Вестник Университета прокуратуры Российской Федерации. – 2022. – № 1(87). – С. 146-151.

[140]Также следует упомянуть и о том, что в соответствии с одним из требований ФАТФ в государствах-участниках были созданы подразделения финансовой разведки (далее – ПФР), которые служат национальными центрами для сбора и анализа сообщений о подозрительных операциях (сделках) и иной информации, связанной с отмыванием денег, предикатными преступлениями, финансированием терроризма, и для передачи результатов анализа в компетентные правоохранительные органы (Рекомендация 29). В связи с отсутствием в стандартах ФАТФ требований к организации и структуре специализированных органов в настоящее время ПФР стран мира существенно различаются по своему правовому статусу и объему полномочий. Например, в Австрии, ФРГ, Великобритании подразделения финансовой разведки входят в состав федеральных управлений уголовной полиции и являются правоохранительными органами. ПФР Дании, Швеции, Гонконга, Саудовской Аравии также имеют статус правоохранительного органа. *Тисен, О. Н.* Использование результатов деятельности Росфинмониторинга в уголовном судопроизводстве / О. Н. Тисен, А. В. Гриненко // Всероссийский криминологический журнал. – 2022. – Т. 16. № 4. – С. 492-504.

уголовной юрисдикции[141]. Опираясь на такой ориентир, государства могут использовать принципы, изложенные в руководстве ФАТФ, для расширения своей юрисдикции в делах, связанных с криптопреступлениями, даже если деяние совершено за пределами их территории. Подобный подход способствует уголовному преследованию лиц, причастных к преступной деятельности, и привлечению их к ответственности, в том числе в случаях нахождения за рубежом. Стандарты ФАТФ оказывают значительное влияние на развитие международного сотрудничества в обозначенной сфере.

Указанный аспект приобретает первостепенное значение в контексте цифрового обмена информацией между национальными подразделениями финансовых разведок, вошедших в состав Группы Эгмонт (с англ. – «Egmont Group of Financial Intelligence Units»), которая была сформирована в целях оптимизации работы каналов взаимодействия оперативного отслеживания подозрительных финансовых операций[142]. С помощью созданной защищенной сети (Egmont Secure Web, ESW) между участниками Группы Эгмонт могут отправляться запросы в круглосуточном режиме для срочного исполнения. В условиях осуществления молниеносных транзакций между криптобиржами, находящимися в различных юрисдикциях и зачастую характеризующихся различным уровнем регуляторного контроля, сведения, полученные по каналам ESW, становится важнейшим источником криминалистически значимой информации.

В условиях сложившейся политической обстановки участие ПФР Российской Федерации в Группе Эгмонт было приостановлено. Однако

---

[141] *Литвишко, П.А.* Юрисдикционные и международно-правовые аспекты обеспечительных и конфискационных мер в отношении виртуальных активов / П. А. Литвишко // Законность. – 2021. – № 3. – С. 10–11.

[142] Principles for information exchange between financial intelligence units approved by the heads of fius july 2013 [Electronic resource] // Egmont Group. – URL: https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf (дата обращения: 14.03.2025).

сотрудничество в по обмену информацией с отдельными странами в рамках действующих договоров о взаимном сотрудничестве продолжается[143].

Современные подходы к регулированию криптовалютной индустрии в различных странах напрямую влияют на возможности правоохранительных органов по сбору криминалистически значимой информации, необходимой для эффективного раскрытия и расследования преступлений, связанных с цифровыми активами.

В юрисдикциях, характеризующихся установлением тотального запрета на использование криптовалют, как это наблюдается, в частности, в Алжире, Бангладеш, Боливии, Египте, Иране и Непале, процесс получения криминалистически значимой информации сопряжен с возникновением существенных правовых и технологических трудностей. Данное обстоятельство обусловлено прежде всего перемещением преступной активности в теневой сегмент криптоэкономики, что, в свою очередь, приводит к ограничению доступа к первичным данным, генерируемым криптографическими биржами. Фактически это исключает возможность легитимного получения информации о транзакциях и лицах, представляющих оперативный интерес, из источников, функционирующих в рамках правового поля.

В обозначенных условиях эффективность мероприятий оперативно-розыскного характера оказывается в прямой зависимости от разработки и внедрения инновационных методов и инструментов, нацеленных на преодоление механизмов анонимизации и выявление преступных схем, которые, как показывает иностранная практика, все чаще выстраиваются трансграничными организованными преступными сообществами (синдикатами) на территории сразу нескольких государств. Особую актуальность приобретают методы

[143] Например: Соглашение о сотрудничестве между Генеральной прокуратурой Российской Федерации и Верховной народной прокуратурой Лаосской Народно-Демократической Республики (заключено в г. Владивостоке 04.09.2024); Соглашение о сотрудничестве между Генеральной прокуратурой Российской Федерации и Центральной прокуратурой Корейской Народно-Демократической Республики (заключено в г. Пхеньяне 22.07.2024); Меморандум о взаимопонимании в сфере обучения между Генеральной прокуратурой Российской Федерации и Генеральной прокуратурой Арабской Республики Египет (подписан в г. Москве 17.06.2024) и др. // СПС «КонсультантПлюс» (дата обращения: 14.03.2025).

активного получения информации, такие как внедрение агентов в криминальные сообщества, использование «кибер-приманок» и перехват трафика в Даркнете.

Причем в государствах, имплементировавших «разрешительную модель» регулирования операций с криптоактивами, к числу которых относятся США, Канада, Япония, Сингапур, Южная Корея, страны Европейского Союза и др., сформированы относительно благоприятные условия для получения правоохранительными органами информации, представляющей существенную значимость для целей расследования преступлений. Это обстоятельство обусловлено прежде всего наличием легальных каналов доступа к сведениям, находящимся в распоряжении лицензированных криптовалютных бирж, включая детальную информацию о транзакциях, идентификационные данные клиентов, собираемые в рамках процедур KYC, IP-адреса[144], а также иные сведения, позволяющие идентифицировать участников операций и проследить движение активов.

Вместе с тем, несмотря на наличие обозначенных преимуществ и расширенные возможности для получения информации, сохраняются риски злоупотребления легальными сервисами, связанные с использованием лицензированных бирж преступными элементами через подставных лиц. В этой связи усилия правоохранительных органов закономерно концентрируются на выявлении латентных связей между операциями, формально осуществляемыми в рамках правового поля, и нелегальными транзакциями, проводимыми с использованием механизмов анонимизации. Дополнительным направлением деятельности является разработка специализированных методов работы с анонимными децентрализованными платформами, в том числе с использованием техник деанонимизации, анализа графовых структур и внедрения агентурных методов.

---

[144] IP-адрес (Internet Protocol address) – это уникальный числовой идентификатор, присваиваемый каждому устройству, подключенному к компьютерной сети, использующей протокол IP (Internet Protocol) для связи.

В юрисдикциях, придерживающихся «ограничительной модели» регулирования оборота криптовалюты, к числу которых относятся в частности Китай[145], Индия, Турция и Индонезия, отмечается тенденция активного использования P2P-платформ[146] для осуществления криптовалютных транзакций. Это обстоятельство приводит к увеличению доли операций, проводимых вне рамок регулируемых каналов, что, в свою очередь, существенно усложняет процесс получения криминалистически значимой информации для целей расследования преступлений.

В таких условиях получение релевантной информации становится возможным главным образом в рамках активного использования оперативно-розыскных методов, направленных не только на выявление и пресечение деятельности нелегальных обменных пунктов и P2P-платформ, но и на извлечение данных из электронных устройств, изъятых у фигурантов уголовных дел.

Российская Федерация также относится к данной категории юрисдикций, что обусловливает аналогичные трудности в обеспечении законности в сфере оборота криптоактивов. Так, Федеральный закон от 31 июля 2020 г. № 259-ФЗ (в ред. от 25.10.2024) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[147] достаточно подробно регламентирует учет и обращение цифровых финансовых активов (ст. 4), а также устанавливает требования к операторам информационных систем и их деятельности (ст. 5–14). Однако указанный нормативный правовой акт не охватывает весь спектр отношений,

---

[145] Китайская «модель неполного отказа», по меткому определению Э.Л. Сидоренко, представляет собой уникальный гибрид запретительной политики и вынужденного признания цифровых реалий. Эта двойственность отражает глобальный вызов: как совместить контроль над финансовой системой с защитой имущественных прав в эпоху цифровизации. *Сидоренко, Э. Л.* Криптовалюта и будущее цифровых финансов / Э. Л. Сидоренко. – Москва : МГИМО МИД России, 2023. – 36 с.

[146] P2P-платформы (с англ. - «peer-to-peer platforms»), также известные как одноранговые платформы, представляют собой цифровые площадки, которые позволяют непосредственно соединять людей, желающих продать или предоставить что-либо, с людьми, желающими купить или получить это, без участия традиционного посредника.

[147] Собрание законодательства РФ. 2020. № 31 (ч. 1). Ст. 5108.

возникающих в сфере оборота криптовалют, оставляя значительную часть операций в «серой» зоне[148].

В этой связи возрастает значимость деятельности подразделений финансовой разведки, в частности Федеральной службы по финансовому мониторингу (Росфинмониторинг), в сфере выявления и анализа подозрительных финансовых операций, осуществляемых с использованием криптовалют. В качестве инструмента, способствующего повышению эффективности работы правоохранительных органов в данной области, следует отметить отечественный аналитический сервис «Прозрачный блокчейн»[149], апробированный Росфинмониторингом в 2021 г. Данный сервис предоставляет оперативным и следственным подразделениям бесплатный доступ к комплексному инструментарию, обеспечивающему возможность отслеживания, анализа и визуализации транзакций, проводимых с использованием наиболее востребованных криптовалют[150].

В современной парадигме борьбы с криптопреступностью сервис «Прозрачный блокчейн» демонстрирует значительный потенциал, получив широкое распространение в правоохранительных органах России и стран СНГ. Согласно утверждению О.Н. Тисен эмпирические данные, накопленные в процессе применения сервиса, подтверждают его существенную роль в раскрытии преступлений, где криптовалюты выступают в качестве объекта или

---

[148] Действующее законодательство Российской Федерации не признает криптовалюту денежным средством или его суррогатом, что влечет за собой запрет на ее использование в качестве платежного инструмента. Вместе с тем, физические и юридические лица сохраняют право владеть криптовалютой на праве собственности. Данный подход, впервые сформулированный в 2018 г. в рамках гражданско-правовых отношений по делу И.И. Царькова, ознаменовал собой прецедент включения криптовалюты в имущественную массу в процессе банкротства, что стало знаменательным шагом в определении правового статуса криптоактивов в России. Постановление Девятого арбитражного апелляционного суда от 15.05.2018 № 09АП16416/2018 по делу № А40-124668/2017 (дата обращения: 14.04.2025).

[149] Свидетельство о государственной регистрации программы для ЭВМ № 2023664920 Российская Федерация. Прозрачный блокчейн. Государственный модуль : № 2023663888 : заявл. 04.07.2023 : опубл. 10.07.2023 ; заявитель - Федеральная служба по финансовому мониторингу.

[150] *Тисен О.Н.* Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют // Уголовное право. 2024. № 3. С. 69-80.

инструмента совершения противоправных деяний[151]. Тем не менее для достижения максимальной эффективности в противодействии криптопреступности целесообразно расширить функциональные возможности сервиса «Прозрачный блокчейн» в части охвата анализируемых криптовалют. Учитывая наличие значительного числа анонимных криптовалют, дальнейшее развитие сервиса может быть направлено на интеграцию механизмов, позволяющих выявлять и анализировать транзакции в сетях блокчейн в условиях международного сотрудничества, в том числе в рамках региональной межведомственной сети по возврату активов (далее – МСВА).

Интеграция с МСВА позволит не только расширить горизонты отслеживания и возврата активов, полученных преступным путем с использованием криптовалют, но и существенно повысить качество получаемой криминалистически значимой информации[152]. Благодаря обмену данными о подозрительных транзакциях, идентификации криптокошельков, используемых в преступных схемах, и координации оперативно-розыскных мероприятий и следственных действий станет возможным более эффективно выявлять и пресекать законспирированные преступные сети, а также формировать доказательственную базу, необходимую для привлечения причастных лиц к ответственности.

---

[151] *Тисен, О. Н.* Использование сервиса отслеживания криптовалютных транзакций «Прозрачный блокчейн - 2» при выявлении и расследовании преступлений, совершенных с использованием криптовалют / О. Н. Тисен // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов, Москва, 30 марта 2023 г. / сост. А.В. Константинов. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 195-200.

[152] Стоит акцентировать внимание на том, что в последние годы географический охват МСВА значительно расширился, увеличилось число стран-членов и количество сетей МСВА. Региональные МСВА теперь охватывают Западную Европу и Северную Америку, Азиатско-Тихоокеанский регион, Карибский бассейн, Восточную Африку, Латинскую Америку, Центральную Африку и Восточную Европу. Сегодня сети МСВА насчитывают в общей сложности 178 стран-членов, из которых 159 также являются членами Глобальной сети ФАТФ, объединяющей 205 стран и юрисдикций. Это означает, что 77% стран глобальной сети входят в состав МСВА. Двадцать три процента членов Глобальной сети ФАТФ не связаны с МСВА // Отчет ФАТФ. Возврат преступных доходов из-за рубежа через задействование межведомственных сетей по возврату активов // https://mumcfm.ru/mediateka/international/fatf/otcet-fatf-vozvrat-prestupnyx-doxodov-iz-za-rubeza-cerez-zadeistvovanie-mezvedomstvennyx-setei-po-vozvratu-aktivov (дата обращения: 05.04.2025).

Вместе с тем осознание необходимости более комплексного подхода к регулированию криптоактивов стимулирует разработку нормативных правовых актов на международном уровне, которые будут направлены на обеспечение прозрачности и снижение рисков использования криптоактивов в незаконных целях.

Разработка Регламента о рынках криптоактивов[153] (MiCA) на территории Европейского союза является ответом на эти вызовы, поскольку он предусматривает механизмы получения криминалистически значимой информации, необходимой для расследований. В частности, MiCA предполагает обязательное лицензирование поставщиков услуг, связанных с криптоактивами, что позволяет правоохранительным органам получать информацию об идентификационных данных клиентов, объеме и характере осуществляемых ими операций[154].

Кроме того, устанавливаются требования к хранению данных, что позволяет проследить цепочку транзакций и выявить бенефициарных владельцев. Такая информация в свой черед может быть использована для установления связи между транзакциями и конкретными преступными организациями, а также для замораживания и конфискации незаконно полученных средств. В случае расследования межгосударственных преступлений была упрощена процедура обмена информацией между компетентными органами разных стран, способствуя координации расследований (ст. 68 MiCA)[155].

Банкротство криптовалютной биржи FTX, произошедшее в конце 2022 г., стало катализатором для активизации подобных мер и одновременно породило

---

[153] Regulation (EU) 2023/1114 of the European Parliament and of the Council of May 31, 2023 on markets in crypto-assets and amending Directives 2009/65/EC, (EU) 2019/1937 // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114 (дата обращения: 05.04.2025).

[154] Wronka, C. Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight / C. Wronka // J Bank Regul. – 2024. – Vol. 25. – P. 84–93. – DOI: 10.1057/s41261-023-00217-8. (дата обращения: 05.04.2025).

[155] *Barczentewicz, M.* Crypto-Asset Market Abuse Under EU MiCA / M. Barczentewicz, A. de Gândara Gomes // European Journal of Risk Regulation. – 2024. – P. 1-18. – DOI: 10.1017/err.2024.80.

потребность в разработке новых криминалистических методов выявления подобных инцидентов. Созданная в 2019 г. криптобиржа благодаря специализации на торговле криптовалютными фьючерсами быстро заняла заметное место на рынке и привлекла значительные инвестиции[156]. Рост платформы сопровождался увеличением объемов торгов и капитализации, при этом оценка FTX к середине 2022 г. достигала 32 млрд долл. США. Однако, как показал последующий анализ, предпосылки для кризиса, а возможно и для совершения противоправных действий, возникли ранее. В частности, в июне 2022 г. Alameda Research, компания, связанная с FTX, подверглась обвинениям в манипулировании рынком, что является признаком потенциального использования инсайдерской информации и других форм мошенничества.

В подобных ситуациях криптовалютная среда приобретает статус ключевого объекта внимания в рамках процесса получения криминалистически значимой информации. В частности, при проведении расследования осуществлялось детальное изучение транзакций с использованием криптовалют, проводившихся между FTX, Alameda Research и ассоциированными с ними организациями, в результате чего были выявлены признаки неправомерного использования средств, принадлежащих клиентам из двенадцати стран, расположенных на разных континентах. Как следствие, проведенный анализ данных о торгах позволил обнаружить признаки осуществления действий, направленных на манипулирование рыночной конъюнктурой и извлечение незаконной прибыли[157].

Учитывая опыт Европейского союза в разработке и внедрении Регламента MiCA, представляется перспективным инициирование процесса разработки аналогичной регуляторной структуры для криптоактивов в рамках

---

[156] После этого случая также были совершены хищения криптовалют, однако в меньших объемах.

[157] *Nimalendran, M.* Informational Efficiency of Cryptocurrency Markets / M. Nimalendran, P. Pathak, M. Petryk, L. Qiu // Journal of Financial and Quantitative Analysis. – 2024. – P. 1-30. – DOI: 10.1017/S0022109024000310.

сотрудничества стран БРИКС[158]. Реализация данного проекта может включать в себя последовательность определенных этапов и элементов, направленных на адаптацию европейского опыта к специфическим условиям и потребностям стран-участниц[159].

Во-первых, для успешной разработки модели регулирования криптоактивов, адаптированной к специфике стран БРИКС, необходимо сформировать экспертную рабочую группу, в задачи которой войдет комплексный анализ международного опыта, основанного в том числе на имплементацию стандартов ФАТФ. Ключевым элементом разрабатываемой модели должно стать создание эффективных механизмов получения криминалистически значимой информации в максимально оперативном режиме. В частности, это предполагает установление строгих лицензионных требований к поставщикам услуг, связанных с криптоактивами, в обязательном порядке включающих процедуры идентификации клиентов (KYC) и мониторинга транзакций (AML).

Во-вторых, для обеспечения прозрачности операций с криптоактивами необходимо внедрение инструментов анализа блокчейна, создание централизованных реестров транзакций и установление четких требований к хранению данных, обеспечивающих возможность отслеживания цепочки транзакций и выявления бенефициарных владельцев. Важным элементом предлагаемой модели является создание защищенного механизма обмена информацией между компетентными органами стран БРИКС, что позволит оперативно обмениваться данными о подозрительных транзакциях, выявлять преступные организации и замораживать незаконно полученные активы. С

---

[158] БРИКС – объединение 10 государств (Бразилия, Россия, Индия, КНР, ЮАР, ОАЭ, Иран, Египет, Эфиопия, Индонезия), основанное в 2009 году. В 2024 году в состав БРИКС пригласили новых членов, а также сформировали категорию «стран – партнёров БРИКС» (12 государств с 2025 года) // https://infobrics.org/ (дата обращения: 05.04.2025).

[159] *Волеводз, А.Г.* Международно-правовое регулирование возврата преступных активов в рамках БРИКС: современное состояние и перспективы / А. Г. Волеводз // Актуальные проблемы международного сотрудничества в борьбе с преступностью : Сборник научных трудов Международной научно-практической конференции, Москва, 16 ноября 2023 года. – Москва: Московский университет МВД РФ им. В.Я. Кикотя, 2023. – С. 18-24.

целью гармонизации регуляторной среды целесообразно рассмотреть возможность создания общего регуляторного органа, ответственного за разработку стандартов, лицензирование поставщиков услуг и надзор за рынком криптоактивов.

В-третьих, целесообразно обеспечить подготовку квалифицированных кадров в области кибербезопасности и криптотехнологий, а также разработать образовательные программы для правоохранительных органов и участников рынка. Таким образом, предлагаемый подход позволит положить начало созданию международной системы регулирования криптоактивов, обеспечивающей защиту интересов государства, инвесторов и стимулирующую развитие инноваций в сфере финансовых технологий.

Проведенный анализ позволил сформулировать ряд ключевых выводов, отражающих роль криптовалютной среды как источника криминалистически значимой информации и специфику её использования в раскрытии и расследовании преступлений.

1. Информация, имеющая криминалистическое значение и получаемая из криптовалютной среды, представляет собой специфическую категорию данных, характеризующую механизм совершения преступлений, связанных с цифровыми активами, и особенности их отражения в цифровом пространстве. Данная категория информации обладает комплексом общих и уникальных атрибутов, определяющих ее качество и, следовательно, доказательственное значение в условиях высокой степени анонимности и трансграничности транзакций с использованием криптовалют. При этом свойства и характеристики криминалистически значимой информации подлежат тщательной оценке с учетом специфики криптографических методов защиты данных и особенностей функционирования технологий распределенного реестра.

2. Ключевым условием эффективного расследования преступлений, связанных с криптовалютой, является получение криминалистически значимой информации, позволяющей идентифицировать владельцев криптографических кошельков и устанавливать признаки их возможной причастности к

противоправной деятельности. Этот процесс основан на многоаспектном анализе шаблонов использования криптокошельков, характеристик сетевой активности и корреляции данных из различных источников информации.

3. С целью обеспечения прозрачности операций с криптоактивами представляется необходимым внедрение инструментов анализа блокчейна, создание централизованных реестров транзакций, установление требований к хранению данных, обеспечивающих отслеживание цепочки транзакций и выявление бенефициарных владельцев, а также формирование защищенного механизма обмена информацией между компетентными органами государств – членов БРИКС[160].

4. Создание условий для оперативного получения криминалистически значимой информации, необходимой для раскрытия и расследования преступлений, связанных с использованием криптоактивов, может быть реализовано в условиях создания международных экспертных групп, внедрения строгих лицензионных требований с обязательной идентификацией клиентов и мониторингом транзакций, обеспечения прозрачности операций посредством инструментов анализа блокчейна, а также формирования защищенного механизма. Комплексный подход, основанный на опыте ФАТФ, представляет собой перспективную основу для формирования эффективной системы выявления, отслеживания, ареста и возвращения криптоактивов в рамках сотрудничества правоохранительных органов стран – участников БРИКС.

5. Формирование механизма обмена информацией между компетентными органами будет способствовать созданию благоприятной среды для развития инноваций в сфере финансовых технологий, обеспечению защиты интересов государства и инвесторов, а также для минимизации рисков использования

---

[160] Стоит отметить, что подавляющее большинство опрошенных нами сотрудников правоохранительных органов (95%) считают необходимым разрабатывать новые методы, адаптированные под криптовалютную среду и практически все (98%) считают необходимым усиление международного сотрудничества в борьбе с криптовалютной преступностью. См.: Приложение 1.

криптоактивов в незаконных целях. Как представляется, предлагаемый подход позволит заложить фундамент международной системы регулирования криптоактивов, отвечающей современным вызовам и обеспечивающей устойчивое развитие цифровой экономики.

§ 2. Механизм следообразования преступной деятельности в элементах инфраструктуры криптовалюты

Процесс подготовки, совершения и сокрытия преступлений формирует систему взаимосвязанных следовых комплексов различной этимологии, обусловленную непрерывным взаимодействием предметов и объектов, участвующих (используемых) в механизме противоправного события, с окружающей средой. Наибольший объем в таких комплексах формируется благодаря криминалистически значимой информации, получаемой преимущественно в процессе осуществления первоначальных проверочной, поисковой, удостоверительной деятельности субъекта расследования.

Уместно в этом плане акцентируется внимание О.Б. Дроновой и Б.П.Смагоринского на том, что полноценное изучение структурных элементов преступной деятельности, которые с учетом их взаимосвязи и совокупности образуют общие закономерности, может происходить только в условиях правильной оценки совокупности оставленных событием следов[161].

Развивая данное положение, следует отметить, что, как справедливо отмечает профессор А.Г. Волеводз, механизм следообразования, объединяя все элементы процесса формирования следовой информации, представляет собой

[161] *Дронова, О.Б.* Интеграция данных экспертно-криминалистических и оперативных учетов как способ повышения уровня информационного обеспечения раскрытия и расследования преступлений / О.Б. Дронова, Б.П. Смагоринский // Юридическая наука и правоохранительная практика. – 2024. – № 2(68). – С. 51–58.

устойчивую систему, отражающую общие закономерности данного явления[162]. Вместе с тем он раскрывает динамические аспекты процесса, обеспечивая возможность проникновения в сущность следа как объекта криминалистического познания и установления его генезиса[163]. Это, в свою очередь, создает предпосылки для научного объяснения возникновения следа, его свойств и связей, а также для разработки эффективных методов его обнаружения, фиксации, изъятия и исследования.

В данном контексте особую значимость приобретает постулат профессора Р.С. Белкина, согласно которому общность и устойчивость процесса следообразования объясняются его независимостью от рода, вида и качественных особенностей следообразующих и следовоспринимающих объектов, а также различиями в ситуациях, при которых возникают следы. Знание механизма следообразования является необходимой предпосылкой для получения доказательственной и ориентирующей информации, содержащейся в следе, поскольку в нем проявляются закономерности возникновения такой информации, являющиеся базовыми для процесса доказывания. Именно на их познании в первую очередь основываются средства и методы работы со следами[164].

Прогресс науки и техники, в особенности в области цифровых финансовых инструментов, оказал существенное влияние на развитие криминалистических знаний, касающихся разработки средств и методов получения доказательств, содержащих сведения о лицах, использующих криптовалюты. Данное обстоятельство наглядно подтверждает тезис о том, что развитие

---

[162] *Волеводз, А.Г.* Следы преступлений в сфере компьютерной информации / А.Г. Волеводз // Российский следователь. – 2001. – № 7. – С. 2–11.

[163] *Шампаров, А. В.* Механизм следообразования информации о соединениях между абонентами и (или) абонентскими устройствами / А. В. Шампаров // Вестник Удмуртского университета. Серия Экономика и право. – 2014. – № 4. – С. 202-207.

[164] *Белкин Р.С.* Курс криминалистики: в 3 т. Т. 2: Частные криминалистические теории. – М., 1997. – С. 56.

криминалистики обусловлено общим законом развития науки, заключающимся в ускорении прогресса в условиях технологического развития[165].

В общей теории криминалистики след, понимаемый как результат отражения процесса совершения преступления, выступает гносеологической основой принципиальной возможности раскрытия преступления. Это обусловлено тем, что к моменту начала расследования само преступление всегда находится в прошлом и недоступно для непосредственного наблюдения. Именно следы, оставленные преступлением, являются тем материалом, который позволяет следователю восстановить действительную картину событий.

В криминалистической науке применительно к следам, оставляемым в цифровой среде, существует терминологическое разнообразие. Например, В.А.Мещеряков в своих работах обозначает их как «виртуальные следы», понимая под ними любые изменения в автоматизированной информационной системе, связанные с событием преступления и зафиксированные в виде компьютерной информации на материальном носителе[166]. В литературе также используются термины «информационный»[167], «электронный»[168], «цифровой»[169],

---

[165] *Гриненко, А. В.* Противодействие легализации (отмыванию) доходов, полученных преступным путем: уголовно-правовые, уголовно-процессуальные и криминалистические аспекты / А. В. Гриненко, А. В. Коляда, С. Н. Хорьяков ; Московский государственный институт международных отношений (университет) министерства иностранных дел Российской Федерации. – Москва : Общество с ограниченной ответственностью "Проспект", 2022. – 184 с.

[166] *Мещеряков В. А.* Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. … д-ра юрид. наук. - Воронеж, 2001. – С. 22.

[167] *Матренин, М. О.* Информационные следы в сети интернет и последствия их оставления / М. О. Матренин // Инновации и научно-техническое творчество молодежи : Материалы Российской научно-технической конференции, Новосибирск, 20–21 апреля 2022 г. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. – С. 615-619.

[168] *Перов, В. А.* Доказательственное значение электронных следов при расследовании преступлений с использованием блокчейн-технологий / В. А. Перов // Российский следователь. – 2021. – № 4. – С. 38-40; *Карепанов, Н. В.* Особенности технологии агрегирования, исследования и использования электронно-цифровых следов преступления / Н. В. Карепанов // Технологии XXI века в юриспруденции: Материалы четвёртой международной научно-практической конференции, Екатеринбург, 20 мая 2022 г. – Екатеринбург: Уральский государственный юридический университет, 2022. – С. 86-104.

[169] *Россинская, Е. Р.* Система теории цифровизации судебно-экспертной деятельности / Е. Р. Россинская // Теория и практика судебной экспертизы. – 2024. – Т. 19, № 3. – С. 20-32; *Россинская, Е.Р.* Теория информационно-компьютерного обеспечения судебно-экспертной

«электронно-цифровой»[170] для обозначения той же категории следов. Оставим за рамками данной работы полемику о предпочтительном термине, и в нашем исследовании они будут использоваться как синонимы, поскольку в целом авторы понимают под ними одну и ту же категорию. Между тем термин «цифровые следы» является наиболее распространенным и подразумевает следы, которые существуют в виде информации, представленной в двоичном коде и записанной на цифровых носителях. Соответственно в большинстве случаев нами будет использоваться именно он.

Так же, как и при образовании следов-отображений в физическом мире, в процессе цифрового следообразования устанавливается причинно-следственная связь между следообразующими и следовоспринимающими объектами. Это означает, что цифровые следы возникают в результате взаимодействия этих объектов, связанного с событием преступления. В этой связи А.В. Шампаров достаточно обоснованно утверждает, что следовоспринимающий объект несет информацию не только о самом объекте, оставляющем следы (например, о типе используемого программного обеспечения), но и о действиях, совершенных с этим объектом (например, о времени создания файла, отправки сообщения)[171].

Между тем, как упоминают Д.С. Смирнов и Д.С. Селезнев, компьютерное устройство (смартфон, планшет, сервер, сетевое оборудование и т.д.) в данном случае выступает как средство передачи информации о способе действия и

деятельности как новая частная теория судебной экспертологии // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 2. – С. 27-40; *Васюков В.Ф.* К вопросу о сущности следов преступлений, совершаемых в сфере информационно-коммуникационных технологий // Право и образование. – 2016. – № 8. – С. 112-118.

[170] *Сажаев, А. М., Мишуточкин, А. Л.* Значение электронно-цифровых следов в тактике допроса свидетелей и потерпевших // Расследование преступлений: проблемы и пути их решения. 2022. № 3 (37). С. 142-149; *Карепанов, Н. В.* Особенности технологии агрегирования, исследования и использования электронно-цифровых следов преступления / Н. В. Карепанов // Технологии XXI века в юриспруденции: Материалы четвёртой международной научно-практической конференции, Екатеринбург, 20 мая 2022 г. – Екатеринбург: «Уральский государственный юридический университет», 2022. – С. 86-104.

[171] *Шампаров, А. В.* Механизм следообразования информации о соединениях между абонентами и (или) абонентскими устройствами / А.В. Шампаров // Вестник Удмуртского университета. Серия «Экономика и право». – 2014. – № 4. – С. 202-207.

субъектах деятельности, причем не только преступника, но и свидетеля, и потерпевшего как участников события преступления[172].

Первая особенность образования цифровых следов заключается в том, что они остаются в определённой среде (киберпространстве) в результате активности пользователей в определённый промежуток времени. Доступ к этой среде возможен только с использованием электронных носителей.

Вторая особенность определяется разнообразием электронных носителей, с помощью которых информация о совершенном мошенничестве может быть визуализирована. Такими носителями принято считать передвижные полупроводниковые, оптические и стационарные устройства[173].

Третьей особенностью механизма следообразования является форма записи информации на электронном носителе, которая происходит благодаря формированию двоичного кода. Считывание информации требует активации устройства, на котором она хранится. В данном случае, как справедливо отмечает О.Н. Тисен, бережное отношение к электронному носителю имеет первостепенное значение, поскольку повреждение или уничтожение носителя приводит к утрате цифровых следов[174].

При этом, как небезосновательно утверждает И.В. Володикова, «относительная техническая неустойчивость цифровых следов является значимым аспектом, который необходимо учитывать при их выявлении, фиксации, изъятии и исследовании носителей информации»[175]. Подобная «хрупкость» обусловлена возможным внешним воздействием с помощью

---

[172] *Смирнов, В. М.* Проблемы противодействия преступности в сфере информационно-телекоммуникационных технологий и обеспечения информационной безопасности / В. М. Смирнов, Д. С. Селезнев // Криминологический журнал. – 2024. – № 2. – С. 295-298.

[173] *Колычева, А. Н.* Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие / А. Н. Колычева, В. Ф. Васюков. – Москва : Общество с ограниченной ответственностью "Проспект", 2025. – 200 с.

[174] *Тисен, О. Н.* Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют / О. Н. Тисен // Уголовное право. – 2024. – № 3(163). – С. 69-80.

[175] *Володикова, И. В.* Отдельные аспекты механизма образования цифровых следов при совершении дистанционных мошенничеств / И.В. Володикова // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 1 (98). – С. 97–103.

электромагнитных волн, способных исказить компьютерную информацию, а также вероятностью ее «затирания» и безвозвратной утраты из-за перезаписи другими данными. Эти факторы требуют особого внимания к мерам предосторожности при работе, особенно в полевых условиях.

Цифровой след не является изолированным элементом, а представляет собой результат взаимодействия различных данных, возникающих в процессе совершения преступления. Эти данные могут быть связаны между собой по времени, месту, содержанию и другим параметрам. Иными словами, след формируется не одним действием, а цепочкой взаимосвязанных событий, записанных в различных журналах, файлах, базах данных. Все эти данные взаимосвязаны и образуют целостную картину.

Особенности образования цифровых следов, рассмотренные ранее, обусловливают выбор необходимых инструментов для обнаружения сведений, которые представляют собой совокупность цифровых значений, выраженных в определенных параметрах формализованной системы данных. По справедливому утверждению Ю.Б. Давыдовой именно формализованная система данных визуализируется в виде дискретных символов, принимающих одно из значений конкретной буквы или цифры, что требует использования специальных методов и средств для их обнаружения, фиксации и анализа[176].

Российские исследователи, справедливо указывая на уникальную электронную среду, в которой возникают цифровые следы в современных информационных системах, и на их дискретную (часто двоичную) форму представления, к сожалению, зачастую пренебрегают важнейшей характеристикой этих следов – их смысловой нагрузкой[177]. В искусственно

---

[176] *Давыдова, Ю.Б.* Модель информационно-аналитической системы анализа данных при расследовании компьютерных преступлений // Сборник статей III Международной научно-практической конференции: в 2 ч. – Пенза, 2022. – Ч. 1. - С. 19-24.

[177] *Мещеряков, В. А*. Следы цифрового века / В. А. Мещеряков // Вопросы экспертной практики. – 2019. – № 1. – С. 423-426; Родионов, В. С. К вопросу о разработке понятия «цифровой след» в российской и зарубежной криминалистике / В. С. Родионов // Университетские правовые диалоги «право цифровой среды»: материалы Международной научно-практической конференции, Челябинск, 27–28 марта 2020 г. – Челябинск: Издательский центр ЮУрГУ, 2020. – С. 243-247; *Горбунова, К. А.* Тактика производства

созданной цифровой среде, ориентированной на решение конкретных задач, процесс отражения не является прямым, как в случае традиционных криминалистических материальных следов, возникающих при непосредственном контакте между следообразующим и следовоспринимающим объектами[178].

Вместо этого он опосредован сложной системой формализованных, преимущественно математических моделей, используемых для описания физических процессов. Следовательно, набор цифровых значений, зафиксированный на соответствующем физическом носителе (будь то магнитном, оптическом или электронном), представляет собой лишь отражение параметров формализованной модели, встроенной в конструкцию и режимы работы регистрирующего устройства.

В своей монографии, посвященной основам механизма следообразования в цифровой криминалистике, профессор В.А. Мещеряков затрагивает важную проблематику[179]. Дело в том, что свойства искусственной среды (коей и является киберпространство), целенаправленно оптимизированы для решения конкретных прикладных задач, таких как передача данных, обработка информации, хранение файлов и т. п. Эта оптимизация подразумевает, что среда не предназначена для сохранения всей полноты информации, необходимой для криминалистических целей. Однако цифровое отражение предполагает последовательное использование иерархии формализованных моделей для представления и обработки информации. Это означает, что реальное физическое явление проходит через несколько уровней преобразования и абстрагирования, прежде чем стать цифровым следом.

следственных действий при расследовании преступлений в сфере компьютерной информации / К. А. Горбунова, А. С. Киселев. – Москва: Общество с ограниченной ответственностью «Проспект», 2023. – 88 с.

[178] *Смушкин, А. Б.* Криминалистические аспекты использования киберпространства и обеспечения кибербезопасности / А. Б. Смушкин. – Москва : Общество с ограниченной ответственностью "Русайнс", 2024. – 196 с.

[179] *Мещеряков, В. А.* Теоретические основы механизма следообразования в цифровой криминалистике / В. А. Мещеряков. – Москва: Общество с ограниченной ответственностью "Проспект", 2022. – 176 с.

В условиях феноменального развития технологий в области цифровых активов криминалистическая теория механизма следообразования сталкивается с новыми вызовами и требует дальнейшего развития, адаптации и дополнения. Появление криптовалют и способов их реализации в преступных целях сформировало перед криминалистикой потребность в совершенствовании методов и средств работы с цифровыми следами. Об этом в течение нескольких лет на различных форумах неоднократно упоминают ученые и практики[180].

Информация, формирующаяся в среде криптосистем, представляет собой результат особого вида следообразования, который в настоящее время активно изучается криминалистами по всему миру. Этот процесс, хотя и управляется общими закономерностями, присущими механизму образования «традиционных» цифровых следов, имеет свои специфические черты, обусловленные средой его протекания и особенностями субъектов, участвующих в криптоопераций. При этом, как уместно отмечается А.В. Комовым, доказательственный и тактический потенциал этой информации бесценен[181].

Это обусловлено тем, что во всяких следственных ситуациях, как на первоначальном, так и на последующем этапе расследования преступления, механизм которого был реализован благодаря криптовалютам, возникает необходимость установления причинно-следственных связей между цифровыми следами и элементами состава преступления. Другими словами, требуется установить, каким образом конкретные транзакции, IP-адреса, учетные записи и

---

[180] *Хамидуллин, Р. С.* Криминалистическое обеспечение противодействия незаконному обороту наркотических средств и психотропных веществ, осуществляемому в криптовалюте с использованием технологий «blockchain» / Р. С. Хамидуллин // Технологии XXI века в юриспруденции : Материалы четвёртой международной научно-практической конференции, Екатеринбург, 20 мая 2022 г. / отв. ред.: Д.В. Бахтеев. – Екатеринбург, 2022. – С. 52-58; *Озеров, И. Н.* Цифровые следы преступлений как инструмент раскрытия и расследования коррупционных преступлений / И. Н. Озеров, А. М. Журбенко, К. И. Озеров // Актуальные проблемы борьбы с коррупцией: Материалы всероссийской научно-практической конференции, Москва, 27 октября 2023 г. – Москва: Московская академия следственного комитета, 2024. – С. 96-100; *Фельдман, В. В.* Blockchain и криптовалюты / В. В. Фельдман // Оперативно-розыскное противодействие наркопреступности : Всероссийский научно-практический семинар, Красноярск, 9 апреля 2021 г. – Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2021. – С. 46-50 и др.

[181] *Комов, А.В.* Использование компьютерных (цифровых) следов при выявлении, раскрытии и расследовании преступлений. – М.: 2025. – 293 с.

другие цифровые следы связаны с совершением противоправного деяния, установлением его объекта, объективной стороны, субъекта, субъективной стороны.

Процесс доказывания в подобных случаях существенно усложняется ввиду трансграничного характера криптотранзакций, анонимности или псевдоанонимности участников, а также технической сложности интерпретации цифровых следов для лиц, не обладающих специализированными знаниями в области криптографии и информационных технологий.

Уже тогда возникает вопрос о природе цифрового представления виртуальных активов. Цифровое представление, преобразующее информацию в дискретные значения, открывает возможности для автоматизированной обработки данных, в отличие от непрерывных аналоговых сигналов. Физический носитель, будь то флэш-накопитель или компьютерное устройство, может лишь хранить цифровое представление определенной криптовалюты. Однако функциональность этого представления раскрывается только в сети Интернет, где криптовалюты обретают способность быть средством обмена, расчётной единицей и/или средством сохранения стоимости. Иными словами, именно цифровая форма в сочетании с сетевой доступностью делает криптоактив по-настоящему виртуальным.

Как мы уже подробно рассмотрели в предыдущем параграфе, технология децентрализованной системы хранения информации, получившая название «блокчейн», характеризуется высокой степенью устойчивости к изменениям, взлому и фальсификации. Причем анализ закономерностей работы блокчейна позволил выявить ряд специфических характеристик механизма следообразования в цифровой среде, которые принципиально отличаются от традиционных централизованных информационных систем.

Во-первых, блокчейн представляет собой распределённую базу данных, которая согласно мнению В.Н. Варун совместно «используется и синхронизируется в разных сетях, распределённых по нескольким сайтам, учреждениям или географическим регионам, что позволяет транзакциям иметь

несколько частных или публичных «свидетелей»[182]. Эта особенность обеспечивает высокую устойчивость системы к атакам и манипуляциям, поскольку любое изменение данных в одном узле требует подтверждения большинством участников сети. В результате цифровые следы, оставленные в блокчейне, распределяются между всеми узлами, что делает их практически невозможными для модификации или удаления. Это свойство блокчейна не только повышает надежность системы, но и создает уникальные возможности для использования таких следов в криминалистической практике, обеспечивая высокий уровень достоверности и неизменности данных.

Во-вторых, ключевым принципом работы блокчейна является неизменяемость данных. После добавления блока в цепь его содержимое становится необратимым. Любая попытка изменить данные в блоке требует пересчета всех последующих блоков, что практически невозможно без контроля над большей частью вычислительной мощности сети (так называемая «атака 51%»[183]). Это свойство обеспечивает стабильность цифровых следов, оставленных в блокчейне, и гарантирует их сохранность на протяжении длительного времени. Таким образом, блокчейн становится надежным источником криминалистически значимой информации, устойчивой к манипуляциям и искажениям[184].

В-третьих, большинство криптовалют построено на основе блокчейна, который представляет собой открытую систему, где каждая транзакция доступна для просмотра всем участникам сети. Такая прозрачность позволяет осуществлять независимый мониторинг данных, что создает уникальные

---

[182] *Varun, V.M.* Prospects and Models of Combating Cryptocurrency Crimes. The India-EU Dialogue as a Perspective? [Электронный ресурс] // URL: https://eucrim.eu/articles/prospects-and-models-of-combating-cryptocurrency-crimes/ (дата обращения: 14.03.2025).

[183] Постановление № 54-11 Межпарламентской Ассамблеи государств - участников СНГ «О Глоссарии терминов, используемых органами внутренних дел (полицией) государств - участников Содружества Независимых Государств, по вопросам противодействия преступлениям, совершаемым посредством блокчейн-технологий и криптовалют» (Принято в г. Самарканде 28.10.2022) // СПС «КонсультантПлюс» (дата обращения: 14.03.2025).

[184] *Larkin, C.* Criminality and cryptocurrencies: Enforcement and policy responses - Part I / C. Larkin, N. Pearce, N. Shannon // Understanding Cryptocurrency Fraud / ed. S. Corbet. – (Batten-Corbet-Lucey Handbooks in Alternative Investments; vol. 2). – Germany: De Gruyter, 2021. – P. 121-131.

возможности для исследования цифровых следов, оставленных в системе. Это особенно ценно для криминалистического анализа, так как обеспечивает доступ к достоверной и проверяемой информации.

Однако важно учитывать, что в некоторых случаях, например в частных блокчейнах, доступ к данным может быть ограничен определенным кругом лиц, что требует дополнительных усилий для получения необходимой информации.

В-четвертых, каждая транзакция в блокчейне сопровождается цифровым идентификатором, который генерируется с использованием асимметричной криптографии. Это означает, что следы, оставленные в виде транзакций, содержат уникальную цифровую подпись, что позволяет однозначно связать их с конкретным участником сети. Такая особенность обеспечивает высокий уровень прозрачности и подотчетности, что крайне важно для криминалистического анализа. Однако, несмотря на это, анонимность участников может сохраняться благодаря использованию псевдонимов (например, криптографических адресов), что требует дополнительных методов деанонимизации для установления реальной личности[185].

Таким образом, цифровые следы, оставленные в блокчейне, обладают рядом уникальных характеристик, которые делают их ценным источником информации для криминалистического анализа. Как справедливо утверждает О.Н. Тисен, обнаружение и эффективное применение указанных следов в процессе раскрытия и расследования преступлений представляет собой одну из ключевых задач, стоящих перед сотрудниками правоохранительных органов[186].

В деятельности, связанной с выявлением преступлений, совершаемых в отношении и с использованием криптовалюты, важно понимать, что следы блокчейна не имеют какой-либо физической локализации. Копии базы данных располагаются на множестве серверов, находящихся в разных юрисдикциях. Как

---

[185] What Is Blockchain and How Does It Work? // https://academy.binance.com/en/articles/what-is-blockchain-and-how-does-it-work (дата обращения: 14.03.2025).

[186] *Тисен, О. Н.* Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют / О. Н. Тисен // Уголовное право. – 2024. – № 3(163). – С. 69-80.

отмечается Д. Вудом и А. Бьюкененом, «транзакции не привязаны к конкретному географическому месту, а распределены по всей сети»[187]. Иными словами, криптовалюты доступны пользователям по всему миру при условии их подключения к сети Интернет. При всем при этом переводы в криптовалюте могут осуществляться между пользователями сетью блокчейна, находящимися в любой точке планеты.

Поскольку при создании криптовалют используются криптографические методы, именно они выступают гарантом того, что транзакции защищены от подделки и вмешательства третьих лиц[188]. При этом такие методы необходимы для достоверности обладания криптовалютой теми или иными пользователями. По утверждению американского исследователя Дж. Шарфмана «…фактически криптовалюты стали представлять собой согласованную ценность в бартерной системе, благодаря которой они могут обмениваться на фиатные деньги, товары или услуги»[189].

Стремительно усложняющиеся блокчейн-протоколы и динамичное развитие инновационных технологий на их основе, таких как «приватные монеты» (privacy coins) и платформы децентрализованных финансов (DeFi), создают новые вызовы в контексте выявления и расследования преступлений, совершаемых с использованием криптовалютной инфраструктуры. Приватные монеты, использующие передовые криптографические методы для обеспечения абсолютной анонимности транзакций, практически исключают возможность

---

[187] *Wood, G.* Advancing egalitarianism / G. Wood, A. Buchanan // Handbook of Digital Currency. – Cambridge: Academic Press, 2015. – P. 385–402.

[188] Напомним, что определение криптографии в самом простом виде происходит от греческого слова, означающего «тайнопись». Традиционно в это понятие закладывается определенная генерация кодов, которая позволяет сохранить информацию в тайне. *Пермякова К.С.* Криптографические методы защиты информации // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики. Материалы XI Международной научно-практической очно-заочной конференции. – Екатеринбург, 2024. – С. 29-32.

[189] *Scharfman, J.* Cryptocurrency Ponzi, Pyramid, and MLM Schemes: Part 1 / J. Scharfman // The Cryptocurrency and Digital Asset Fraud Casebook. – Cham: Palgrave Macmillan, 2023. – DOI: https://doi.org/10.1007/978-3-031-23679-2_3 (дата обращения: 14.03.2025).

отслеживания движения денежных средств без применения специализированных инструментов и доступа к конфиденциальной информации.

В свою очередь платформы децентрализованных финансов (DeFi) предоставляют широкий спектр сложных финансовых инструментов, включая децентрализованные биржи (DEX), кредитные протоколы и механизмы стейкинга, что открывает дополнительные возможности для отмывания преступных доходов, уклонения от уплаты налогов и реализации других противоправных схем. Децентрализованный характер данных платформ, отсутствие централизованного органа управления, а также применение смарт-контрактов[190] существенно затрудняют процесс анализа и отслеживания транзакций, тем самым усложняя процедуру выявления преступной деятельности.

В своей работе, посвященной «цифровой криминалистике», исследователи из Пекинского университета науки и технологий обращают внимание на необходимость изменения подходов при исследовании следов преступной деятельности, сформировавшихся в ходе реализации криптовалюты[191]. Обосновывается это тем, что, в отличие от обычных информационных систем, где доступ к данным и управление ими осуществляются одним субъектом, децентрализованная природа блокчейна определяет необходимость использования специализированного программного обеспечения, позволяющего анализировать данные об обширной сети узлов. Причем узлом принято обозначать каждое компьютерное устройство, участвующее в поддержании работоспособности сети блокчейн.

---

[190] *Смарт-контракты* – это самоисполняющиеся алгоритмические программы, хранящиеся в блокчейне Ethereum, токены которого могут использоваться в различных приложениях и децентрализованных финансах (DeFi). Смарт-контракты используются для создания сложных финансовых инструментов, децентрализованных бирж и других приложений. Отслеживание транзакций с токенами ERC-20 позволяет исследовать потоки ликвидности на платформе Ethereum, а также выявлять механизмы мошенничества.

[191] *Xiao, N.* A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things / N. Xiao, Z. Wang, X. Sun, J. Miao // Alex. Eng. J. – 2024. – Vol. 86. – P. 631–643.

Узлы в блокчейн-сети выполняют ключевую роль, храня копии блокчейна, проверяя и распространяя транзакции, тем самым обеспечивая целостность и безопасность сети. Они могут быть как «полноценными» узлами, которые хранят всю историю блокчейна, так и «облегчёнными» узлами, сохраняющими только часть данных. Последние занимают меньше места и менее требовательны к ресурсам, что делает их более доступными для использования, но при этом ограничивает их возможности в плане хранения и анализа полной информации[192].

В данном контексте важно подчеркнуть справедливость суждения профессора А.Г. Волеводза, который отмечает, что следы в виртуальном пространстве не могут быть изъяты в традиционном понимании. Вместо этого может быть проведено лишь их копирование с использованием различных программно-технических средств. Однако в процессе копирования изменяются такие параметры, как дата и время последней операции, которые замещаются датой и временем самого копирования. Это может привести к потере существенно важной для доказывания информации о фактических дате и времени создания копируемого файла[193].

Такая особенность обусловлена необходимостью проведения диагностического исследования обнаруженных данных, что позволяет досконально изучить возможные причины наступления негативных последствий от преступного деяния. Диагностический анализ помогает не только установить факт совершения преступления, но и выявить его механизм, что особенно важно в условиях сложности и многослойности криптовалютных операций.

Изучение отечественного и зарубежного опыта раскрытия и расследования преступлений, совершаемых в отношении и с использованием криптовалюты,

---

[192] *Choi, W.* Fractional non-fungible tokens: Overview, evaluation, marketplaces, and challenges / W. Choi, J. Woo, J.W. Hong // Int. J. Netw. Manag. – 2024. – Vol. 34. – P. 22-60.

[193] *Волеводз А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО «Издательство «Юрлитинформ», 2001. С.355; *Волеводз А.Г.* Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 4 – 12; *Волеводз А.Г.* Компьютерная информация, как объект криминалистического следоведения // Криминалистическая техника: Учебник / Отв. ред. И.М. Балашов, рук. колл. С.В. Маликов. М.: ООО Издательство «Юрлитинформ», 2008. С. 336 - 381.

показал, что первый элемент архитектуры криптовалюты, с которым приходится иметь дело правоприменителю в ходе проведения ОРМ, или при проверке сообщения о совершенном криптопреступлении, является так называемый *«криптовалютный кошелек»*[194], подконтрольный подозреваемому либо потерпевшему[195]. Довольно уместно в этой связи привести суждение Д.И. Шнейдеровой о том, что криптокошелек – отправная точка в процессе работы по заявлению о совершенном хищении, «…поскольку он либо выступает средством совершения хищения в случае несанкционированного доступа к кошельку с последующим переводом криптовалют на счет преступника (в этом случае имеют место признаки хищения путем модификации компьютерной информации), либо используется его владельцем для перевода средств злоумышленнику под влиянием обмана (признаки мошенничества), либо выполнения установленного требования под угрозой совершения в отношении него, его семьи и близких родственников противоправных действий (признаки вымогательства)»[196].

В контексте функционирования децентрализованных криптовалютных систем фундаментальную роль в обеспечении контроля над цифровыми активами и проведении транзакций играет концепция «*приватного ключа»*, представляющего собой криптографически сгенерированную последовательность символов. Иначе говоря, приватный ключ функционирует

---

[194] Отметим, что устоявшийся термин, используемый для описания инфраструктуры блокчейна, – *«криптовалютный кошелёк»* – в определенной степени является не совсем корректным, так как не в полном объеме отражает истинную природу этого инструмента. В отличие от традиционного классического материального кошелька криптовалютный кошелёк никогда не содержит и не хранит какие-либо криптовалютные активы. Вместо этого он предназначен для хранения и защиты закрытых криптографических ключей, которые используются для идентификации и распределения средств в системе блокчейна.

[195] Отметим, что опрос сотрудников правоохранительных органов позволил сделать вывод о том, что основными элементами инфраструктуры криптовалют, наиболее часто используемыми преступниками, респонденты называют криптокошельки (75%), криптобиржи (65%) и миксеры криптовалют (40%). См.: Приложение 1.

[196] *Шнейдерова, Д. И.* Осмотр онлайн-криптокошелька заявителя / потерпевшего (по материалам и уголовным делам о хищенияхв сфере оборота криптовалют): процессуальный и криминалистический аспекты / Д. И. Шнейдерова // Алтайский юридический вестник. – 2022. – №4(40). – С. 156-162.

как секретный пароль, позволяющий владельцу кошелька распоряжаться связанными с ним криптовалютными средствами.

Ключевым аспектом является то, что приватный ключ не просто идентифицирует конкретный кошелек, но и определяет право владения и распоряжения определенным набором «неизрасходованных выходов транзакций» (от англ. Unspent Transaction Outputs, сокр. UTXO). В рамках этой модели каждое поступление криптовалютных средств на адрес кошелька не регистрируется как увеличение общего баланса данного адреса, а рассматривается как неделимая единица учёта, имеющая определённое значение в криптовалюте и привязанная к определённому адресу. Этот подход отличается от модели учёта на основе баланса, используемой в традиционных финансовых системах, где средства учитываются как совокупный остаток на счёте[197].

Каждый UTXO может быть использован только один раз. После его расходования в транзакции он перестаёт существовать. Это обеспечивает неизменность и целостность реестра, поскольку вся история движения средств в рамках данной системы может быть прослежена через цепочку создания и расходования. Например, анализ UTXO может показать, что определённый кошелёк часто получает небольшие суммы из множества разных источников, а затем объединяет их в одну крупную транзакцию, что может быть характерно для использования «миксера» лицами, осуществляющими финансовые махинации, легализацию преступных доходов, финансирование терроризма и другие преступления.

Криптовалютными «миксерами» (далее – миксеры) обозначаются специализированные сервисы, предназначенные для смешивания транзакций с цифровыми активами с целью усложнения их отслеживания и повышения уровня псевдоанонимности пользователей. Миксеры принимают криптоактивы от множества отправителей, затем перераспределяют и смешивают эти средства с помощью сложных транзакционных схем и, наконец, отправляют

---

[197] 论刑事涉案虚拟货币处置2024 年 11 月 第 46 卷 第 6 期// Modern Law Science https://qks.swupl.edu.cn/docs//2024-12/eba75d539970461190.pdf (дата обращения: 14.03.2025).

перемешанные активы обратно пользователям на новые адреса, не связанные с первоначальными. Основной целью применения миксеров является разрыв прямых связей между отправителями и получателями транзакций, что затрудняет идентификацию субъектов и отслеживание путей движения денежных средств.

Миксеры различаются по архитектуре (централизованные и децентрализованные), сложности применяемых алгоритмов перемешивания и уровню предлагаемой анонимности. Несмотря на то, что они предоставляют пользователям возможность сохранять конфиденциальность транзакций, их использование конкретными пользователями уже дает определенное основание полагать, что криптоактивы были получены незаконным путем[198].

Установить закономерности использования миксеров возможно посредством тщательного изучения кошельков, имеющихся в распоряжении у лица, представляющего оперативный интерес. Так, регулярные переводы с кошелька подозреваемого на известные адреса миксеров (например, Wasabi Wallet или Tornado Cash) может быть интерпретированы как метод легализации преступных доходов, при котором средства перемещаются через несколько этапов для затруднения отслеживания.

Наличие множества мелких транзакций, которые впоследствии объединяются и направляются на адрес миксера, может быть признаком структурирования («smurfing») – метода, используемого для затруднения отслеживания. Этот подход, направленный на фрагментацию крупных сумм на множество мелких операций, позволяет злоумышленникам минимизировать вероятность обнаружения подозрительной активности системами мониторинга. Важным аспектом в данном контексте является также анализ временны́х меток и частоты транзакций. Если транзакции на миксеры происходят с определенной периодичностью или в конкретное время (например, сразу после получения крупных сумм), это может указывать на систематическое использование

[198] *Kfir, I.* Cryptocurrencies, national security, crime and terrorism / I. Kfir // Comparative Strategy. – 2020. – Vol. 39:2. – P. 113-127. – P. 119.

миксеров, что свидетельствует о заранее спланированной схеме сокрытия средств.

Главная задача при раскрытии и расследовании преступлений, связанных с криптовалютой, заключается в установлении того, каким кошельком пользовалось лицо, представляющее оперативный интерес. Что требует от правоприменителя не только анализа транзакций и связей между адресами, но и понимания технических особенностей различных типов кошельков, которые могут быть использованы подозреваемым[199].

Так, в зависимости от необходимости подключения криптокошельков к сети Интернет их можно разделить на две основные группы: «горячие» и «холодные».

1. «Горячие кошельки» («Hot Wallets»), предназначенные для работы в режиме онлайн, обеспечивают пользователям удобство постоянного доступа к их криптовалютным активам. Однако постоянное присутствие в сети делает их более уязвимыми для атак. Если горячий кошелек находится в скомпрометированной системе, он становится уязвимым для недостатков безопасности этой системы. Кроме того, нельзя игнорировать угрозу вредоносного программного обеспечения, предназначенного для хищения seed-фраз[200] или паролей от кошельков. Практике известны случаи хищений, при реализации которых злоумышленники наблюдали за тем, как жертвы взаимодействуют со своими кошельками, а затем физически захватывали электронные устройства[201]. Таким образом, постоянно работающий онлайн-кошелек по своей конструкции является уязвимым.

---

[199] *Тисен, О. Н.* Установление владельцев криптокошельков, обнаружение и изъятие приватных ключей при расследовании уголовных дел / О. Н. Тисен // Уголовный процесс. – 2024. – № 1(229). – С. 78-83.

[200] *Seed-фраза* представляет собой набор слов, который используется для восстановления доступа к кошельку и, следовательно, к приватным ключам. Получение seed-фразы предоставляет правоохранительным органам возможность получить контроль над криптоактивами, хранящимися в кошельке.

[201] «Your Data is Stolen and Encrypted»: The Ransomware Victim Experience // RUSI Occasional Paper, July 2024 // https://rusi.org/explore-our-research/publications/occasional-papers/your-data-stolen-and-encrypted-ransomware-victim-experience (дата обращения: 14.03.2025).

В свою очередь *горячие* кошельки разделяются в зависимости от типа носителя на следующие категории.

1.1. «Настольные кошельки» – это программные приложения, которые устанавливаются на вычислительное устройство и предлагают пользователям удобный интерфейс для управления цифровыми активами. Некоторые из этих кошельков являются независимыми приложениями, в то время как другие могут быть установлены в качестве расширения для браузеров. Последняя категория получила широкое распространение в качестве средства аутентификации на сайтах, предлагающих услуги, связанные с криптовалютами.

Для получения криминалистически значимой информации необходимо анализировать все приложения, имеющие какое-либо отношение к криптовалютам, а также идентифицировать все расширения браузера, связанных с ними[202]. Сопоставление этих данных с историей использования сети Интернет позволяет уполномоченному сотруднику определить, на каких сайтах, вероятно, проводились криптовалютные транзакции.

Следует также отметить, что не все криптовалютные кошельки требуют традиционной установки и, следовательно, они не будут отображаться в списке программного обеспечения. Примером может служить кошелек Electrum, который можно использовать в виде как традиционно устанавливаемой программы, так и портативного приложения, запускаемого непосредственно из автономного исполняемого файла. Эта функция позволяет подозреваемому запускать кошелек непосредственно с внешнего устройства, например с USB-накопителя или другого съемного носителя. Соответственно все внешние накопители, помимо основной компьютерной системы или любых других портативных вычислительных устройств, необходимо проверять на наличие потенциальных файлов кошельков[203].

---

[202] *Грибунов, О. П.* Криптовалюта и иные виртуальные активы как феномен современной преступности: проблемы раскрытия, расследования и предупреждения / О. П. Грибунов, С. И. Усачев, Е. А. Усачева // Российский следователь. – 2024. – № 4. – С. 7-12.

[203] Отметим, что кошельки с полным узлом работают, запуская полную копию блокчейна и функционируя как узлы в сети блокчейна. Ярким примером этого является Bitcoin Core,

Наличие настольного кошелька может указывать на более низкий уровень понимания или осведомлённости о безопасности криптовалютных транзакций. При этом подозреваемый практически не знаком с потенциальными рисками, связанными с подключением таких кошельков к сети Интернет. Но такой кошелек может быть создан и в целях создания «приманки» для сотрудников правоохранительных органов для направления поисковой группы по ложному следу.

1.2. «Мобильные кошельки» – это приложения для смартфонов, которые позволяют пользователям получать доступ к своим криптовалютам и управлять ими с помощью телефонов и планшетов. Встроенные функции безопасности мобильных операционных систем, включающие в себя доступ по паролю, аутентификацию по отпечатку пальца или распознаванию лица, делают платформу более безопасной, чем стационарные компьютеры, и более доступной для постоянного управления криптовалютами. Это преимущество нивелируется тем фактом, что мобильные устройства становятся более доступной целью для хищения злоумышленниками, которые могут заранее выяснить методы разблокировки мобильного устройства. Однако при проведении оперативно-розыскных мероприятий доступ к кошелькам на мобильных устройствах из-за подобных мер безопасности может быть затруднен. Получить доступ к iPhone, например, с длинным PIN-кодом без сотрудничества с подозреваемым может быть крайне сложно. Как показывает практика, порой оперативному сотруднику проще найти seed-фразу криптокошелька и заново создать кошелек, нежели открыть мобильное устройство.

Наличие мобильного кошелька в пользовании у злоумышленника предполагает, что у него должен быть портативный доступ к криптовалютам. В

который служит одновременно и личным кошельком, и узлом в сети Биткоин. Это означает, что компьютер с установленным и активно работающим Bitcoin Core вносит свой вклад в инфраструктуру распределённого реестра, работающую по всему миру. (https://bitcoin.org/ru/download, дата обращения: 14.03.2025). При этом в Ethereum нет пользовательского кошелька со встроенным узлом; вместо этого нужно установить специальный клиент-узел (https://ethereum.org/ru/запустить-узел). Кроме того, можно управлять узлами-валидаторами, чтобы участвовать в механизме консенсуса Proof-of-Stake, при условии, что у пользователя есть не менее 32 ETH для стейкинга.

свою очередь этот фактор свидетельствует о склонности подозреваемого управлять своими цифровыми активами в постоянном режиме. Данные о местоположении смартфона, на котором установлен такой кошелек, могут указывать на маршруты пользователя и на то, использовался ли кошелек в разных географических регионах[204].

1.3. «*Онлайн-кошельки»* – отличаются от настольных кошельков тем, что закрытые ключи хранятся не локально в системе пользователя, а на удалённом сервере. Это означает, что закрытые ключи хранит провайдер онлайн-кошелька. Поэтому их часто называют кастодиальными[205] кошельками[206]. Функционал кошелька, как правило, аналогичен настольным кошелькам, однако пользователь в данном случае не хранит приватные ключи самостоятельно, а полностью доверяет поставщику услуг виртуальных активов.

Поиск онлайн-кошелька, размещённого на криптовалютной бирже, может оказаться весьма полезным в различных следственных ситуациях. Для доступа к локальным кошелькам часто требуются PIN-коды или пароли, которые может быть получить затруднительно, если подозреваемый отказывается сотрудничать. С другой стороны, получить необходимую документацию для запроса информации с биржи, такую как данные «Знай своего клиента» (от англ know your customer, KYC), сведения о блокировке ордеров, как правило, гораздо проще. Криптовалютные биржи обычно имеют полный доступ к данным учётных записей пользователей, и данные, которые они могут предоставить, порой имеют ценное доказательственное значение.

Такие данные могут включать записи о пополнении и снятии средств со счета, обменах криптовалютами, приобретении криптовалют, идентификационную информацию, IP-адреса, используемые для входа в аккаунт, и другие соответствующие детали. Хотя информация KYC часто оказывается

---

[204] *Васюков, В.Ф.* Использование криптовалюты в преступных целях: некоторые вопросы противодействия / В.И. Ерохов, В.Ф. Васюков // Современная наука. - 2020. - № 2. - С. 5-6.

[205] Термин «кастодиальный» относится к услугам, при которых третья сторона отвечает за хранение и управление активами.

[206] К известным примерам относятся сервисы кошельков, предоставляемые такими платформами, как Coinbase, Binance, Kraken и многими другими.

фальсифицированной, дополнительные сведения об IP-адресе могут быть чрезвычайно ценными. Хотя IP-адреса, используемые преступниками, обычно скрываются с помощью таких инструментов, как виртуальные частные сети или браузер Tor, технические сбои или просто человеческие ошибки очень часто раскрывают «истинный» IP-адрес подозреваемого, благодаря которому устанавливается геолокация устройства, с помощью которого осуществлялась противоправная активность пользователя в сети.

Наличие онлайн-кошелька в обнаруженном у подозреваемого стационарном компьютере или ноутбуке может указывать на то, что он активно использует криптовалюты для конвертации, торговли на бирже и проведения оперативных транзакций с другими кошельками или миксерами для запутывания следов преступной деятельности.

2. «Холодные кошельки» («Cold Wallets») отличаются от предыдущей группы тем, что они работают в автономном режиме, который обеспечивает повышенный уровень безопасности при хранении цифровых активов. В настоящее время в практике встречаются следующие типы холодных кошельков.

2.1. «Аппаратные кошельки» («Hardware Wallets») – это физические устройства, разработанные специально для безопасного хранения приватных ключей криптовалют. Они часто выглядят как USB-ключи или небольшие USB-устройства и почти всегда имеют небольшой экран и кнопки для ввода PIN-кода подключения.

Обнаружение аппаратного кошелька по месту жительства злоумышленника может свидетельствовать о том, что он обладает достаточными навыками, позволяющими не только участвовать в сетевой среде блокчейна, но и успешно сохранять активы в «холодном» режиме. Аппаратные кошельки удобно передавать при личных встречах в качестве оплаты услуг и (или) товаров, запрещенных к обороту. Их также несложно закамуфлировать под электронные носители иного предназначения, бытовые предметы, аксессуары.

Аппаратные кошельки обычно поставляются с картами для записи мнемонических паролей, которые предназначены для резервного копирования на

случай, если аппаратное устройство будет утеряно или выйдет из строя. Создать новый кошелек с помощью мнемонического пароля (seed-фразы) значительно проще, чем пытаться обойти меры безопасности аппаратного кошелька подозреваемого. При поиске карт с паролями в первую очередь следует обратить внимание на оригинальную упаковку, в которой был доставлен аппаратный кошелек. Как правило, пользователи именно там оставляют такие карты.

2.2. «Бумажные кошельки» («Paper Wallets») – представляют собой бумажную распечатку открытых и закрытых ключей пользователя в необработанном буквенно-цифровом формате или в виде QR-кодов. Несмотря на то, что «бумажное» хранение уступает в простоте использования некоторым другим кошелькам, оно представляет собой низкотехнологичный, но исключительно надёжный метод безопасного долгосрочного хранения цифровых активов.

Хотя это может показаться нелогичным, технически возможно создать криптовалютный кошелёк, который никогда не подключался к сети. Средства могут быть отправлены на публичный адрес, созданный пользователем, и кошельку нужно подключаться к сети только при перемещении средств[207].

Бумажные кошельки по своей сути являются холодными кошельками из-за того, что они не могут быть подключены к сети Интернет, поскольку существуют исключительно на бумаге. Хотя в некоторых иностранных источниках бумажные кошельки определяются как «печатные»[208], также распространено использование рукописных мнемонических ключевых фраз, закрытых ключей и связанных с ними заметок о кошельках.

Наличие бумажного кошелька у подозреваемого может говорить о том, что он использует его для долгосрочного хранения больших сумм или редких транзакций, либо для передачи сведений о кошельке лицам, имеющим

---

[207] *Маркарян, Э. С.* Особенности получения данных о механизме следообразования при расследовании преступлений, совершенных с использованием криптовалют / Э. С. Маркарян // Библиотека криминалиста. Научный журнал. – 2017. – № 4(33). – С. 176-187.

[208] *Suratkar, S.* Cryptocurrency Wallet: A Review / S. Suratkar, M. Shirole, S. Bhirud // 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 2020. – P. 1-7.

отношение к преступной организации в условиях, исключающих оставление цифрового следа[209].

Понимание особенностей различных типов кошельков имеет особое значение при проведении документирования преступной деятельности, в ходе которого могут быть обнаружены различные материальные и цифровые следы, по первичным признакам не связанные с криптовалютами.

Установление криптокошелька само по себе является важным фактом и может служить отправной точкой для дальнейшего выстраивания алгоритма расследования преступления[210]. Однако выяснить, откуда поступали средства на кошелек и куда они были переведены, можно только с помощью специализированных обозревателей криптовалют, работающих при подключении к сети Интернет компьютерного устройства, имеющегося в распоряжении оперативного сотрудника или следователя.

Отправной точкой анализа является констатация факта наличия у каждой криптовалюты собственного обозревателя блоков – специализированного инструмента, обеспечивающего возможность отслеживания и анализа всех транзакций[211], зарегистрированных в соответствующем блокчейне. Вместе с тем необходимо учитывать, что для ряда криптовалют, ориентированных на максимальную анонимность пользователей, применение стандартных обозревателей блоков сопряжено со значительными ограничениями, существенно затрудняющими процесс отслеживания транзакций.

---

[209] *Zhang, Q.* Auditable and dynamic access control scheme with behavior and identity tracing / Q. Zhang, L. Yuan, T. Xie, H. Chen // Computer Networks. – 2024. – Т. 251. – P. 623.

[210] *Векленко, В.В.* Особенности противодействия расследованию преступлений, совершенных с использованием криптовалюты в Российской Федерации / В. В. Векленко, А. М. Чихрадзе // Виктимология. – 2024. – Т. 11. № 4. – С. 576-586.

[211] *Транзакция* (с англ. «transaction») – зачисление криптовалюты с одного адреса на другой; действие или последовательность действий, направленных на создание, выпуск, оборот криптоактивов. Транзакция считается завершенной после определенного числа ее подтверждений сетью этой криптовалюты. Постановление № 54-11 Межпарламентской Ассамблеи государств – участников СНГ «О Глоссарии терминов, используемых органами внутренних дел (полицией) государств - участников Содружества Независимых Государств, по вопросам противодействия преступлениям, совершаемым посредством блокчейн-технологий и криптовалют» (принято в г. Самарканде 28.10.2022) // СПС «КонсультантПлюс» (дата обращения: 14.03.2025).

В этой связи для обеспечения эффективности оперативно-розыскных мероприятий и следственных действий требуется не только углубленное понимание технических особенностей конкретной криптовалюты и принципов функционирования соответствующего обозревателя блокчейна, но и использование комплекса специализированных аналитических методов и средств.

Разнообразие криптовалют, основанных на различных блокчейн-протоколах, обусловливает необходимость использования специализированных обозревателей, каждый из которых адаптирован под уникальные технические и функциональные особенности конкретной сети. Эти инструменты играют ключевую роль в анализе данных блокчейна, предоставляя исследователям и практикам доступ к информации о транзакциях, балансах, смарт-контрактах и других элементах, важных для понимания работы криптовалютных систем[212].

История транзакций представляет собой хронологическую запись всех операций с криптовалютными активами, зарегистрированных в блокчейне, формируя при этом цифровые следы, которые являются основой для криминалистического анализа. Каждая транзакция включает данные об адресе отправителя, получателя, сумме перевода, временно´й метке и уникальном идентификаторе (хеше транзакции). Эти элементы создают цифровые следы, позволяющие реконструировать движение средств между кошельками. Например, множественные переводы через промежуточные адреса, часто используемые для сокрытия владельца, оставляют специфические следы, которые могут быть раскрыты с помощью графового анализа. Этот метод

[212] Для Bitcoin (BTC), первой и наиболее капитализированной криптовалюты, разработаны специализированные обозреватели, такие как «blockchain.com» и «blockexplorer.com». Платформа «blockchain.com» выделяется интуитивно понятным интерфейсом и расширенным функционалом, включающим визуализацию цепочек блоков, анализ хешрейта сети и отслеживание транзакций в режиме реального времени. Платформа «blockexplorer.com» предлагает базовые возможности для оперативного мониторинга, что делает ее удобным инструментом для быстрой проверки статуса транзакций или баланса адресов. Данные платформы отражают эволюцию инструментов анализа Bitcoin, сочетая удобство использования с глубиной предоставляемых данных, что является необходимым как для проведения академических исследований, так и для осуществления криминалистической практики.

визуализирует связи между кошельками, выделяя кластеры взаимосвязанных операций и выявляя закономерности, характерные для отмывания средств или финансирования незаконной деятельности.

Цифровое следообразование в блокчейне не ограничивается транзакциями. Баланс кошелька, определяемый как совокупность криптовалютных активов, привязанных к конкретному адресу, также формирует следы, отражающие динамику изменений. Например, резкое увеличение баланса после получения средств с адреса, ассоциированного с незаконным оборотом наркотиков, становится ключевой «зацепкой» в выявлении ячеек «кладовщиков». Обозреватели блокчейна фиксируют эти изменения, создавая основу для анализа. Однако один субъект может контролировать множество кошельков, распределяя активы для минимизации рисков, что требует применения кластерного анализа. Этот метод объединяет адреса по косвенным признакам: общности транзакций, времени активности или связям с идентифицированными кошельками (например, биржевыми), что позволяет реконструировать полную финансовую картину, несмотря на фрагментацию следов[213].

Каждый элемент, доступный через обозреватели блокчейна, формирует цифровые следы, которые служат основой для криминалистического анализа. Однако, несмотря на их детализацию, эти данные остаются псевдонимизированными[214]: идентификация реального владельца кошелька требует взаимодействия с провайдерами услуг виртуальных активов, которые

---

[213] *Васюков, В. Ф.* Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют / В.Ф. Васюков, А.Н. Старжинская // Российское право: образование, практика, наука. – 2024. – № 4. – С. 68-78.

[214] *Псевдонимизация криптокошелька* представляет собой процесс использования уникального, но не связанного напрямую с реальной личностью идентификатора в блокчейн-транзакциях, что создает промежуточный уровень приватности между полной анонимностью и прямой идентифицируемостью. В отличие от классических финансовых систем, где личность пользователя жестко привязана к счету, криптовалютные кошельки оперируют адресами – строками символов, которые, будучи формально открытыми, не содержат явных указаний на владельца, однако при должном анализе цепочки транзакций могут быть деанонимизированы. *Gutiérrez-Agüero, I. et al.* Burnable pseudo-identity: A non-binding anonymous identity method for ethereum // IEEE Access. – 2021. – Т. 9. – С. 108912-108923.

согласно рекомендациям ФАТФ обязаны проводить верификацию клиентов и хранить данные об операциях.

Криптобиржи занимают ключевое место среди провайдеров услуг виртуальных активов. Они представляют собой специализированные провайдеры, формирующие рыночную ликвидность, обеспечивая площадку для взаимодействия между покупателями и продавцами. Этот процесс способствует эффективному ценообразованию, повышая прозрачность и доступность рынка цифровых активов. Объединение спроса и предложения на этих платформах посредством автоматического сопоставления ордеров способствует повышению ликвидности, снижению транзакционных издержек и оптимизации обмена различных криптовалют и фиатных валют[215].

В зависимости от хранения активов и распределения ответственности криптовалютные биржи разделяются на «централизованные» и «децентрализованные».

Централизованные биржи, функционирующие по кастодиальной модели, аккумулируют приватные ключи пользователей и, следовательно, контролируют их средства, принимая на себя ответственность за их безопасность и возможность блокировки подозрительных транзакций. Централизованные платформы генерируют два основных типа цифровых следов: записи о блокчейн-транзакциях между кошельками, принадлежащими бирже и пользователям, а также операционные данные, включающие в себя логи аккаунтов, IP-адреса и информацию об используемых устройствах. Интеграция и анализ указанных данных позволяет сформировать комплексную картину того, каким образом использовались криптовалюты фигурантами.

Возможности приостановки и блокировки подозрительных транзакций, интегрированные в кастодиальную модель централизованных криптовалютных бирж, превращают их в своеобразных регуляторов, контролирующих соблюдение нормативных требований и противодействующих противоправной

---

[215] *Перов, В.А.* Квалификация преступлений, совершаемых с использованием криптовалюты : автореф. дис. … канд. юрид. наук / Перов Валерий Александрович. – Москва, 2023. – 25 с.

деятельности в криптопространстве. В частности, алгоритмы мониторинга транзакций в режиме реального времени позволяют автоматически маркировать транзакции, связанные с адресами, находящимися под санкциями или вовлеченными в иную незаконную деятельность, что дает возможность оперативно реагировать на потенциальные нарушения. Кроме того, для отслеживания перемещения похищенных криптоактивов крупные биржи, такие как Coinbase и Kraken, используют так называемые «медовые кошельки» («honeypot wallets») – кошельки-ловушки, предназначенные для выявления и мониторинга злоумышленников, пытающихся обналичить украденные средства через биржу.

Децентрализованные биржи используют некастодиальный подход, предоставляя пользователям полный контроль над приватными ключами и активами, при этом ответственность за защиту ключей перекладывается на самого пользователя. Это обусловливает необходимость применения методов графовой аналитики для реконструкции цепочек транзакций и выявления взаимосвязей между участниками. Например, анализ транзакций, осуществляемых через такие сервисы, как Tornado Cash, интегрированные с децентрализованными биржами, позволяет отследить движение средств через пулы ликвидности, однако выявить конечных бенефициаров и идентифицировать лиц, извлекающих выгоду из использования анонимизирующих сервисов, зачастую возможно только при проведении комплекса оперативно-технических и оперативно-розыскных мероприятий.

В настоящее время функционирует более 1200 децентрализованных криптовалютных бирж, суммарный суточный оборот которых оценивается в 2,9 млрд долл. США. В число крупнейших децентрализованных бирж по объему торгов входят: Uniswap V3 (Ethereum), PancakeSwap V3 (BSC), Raydium, Orca, Aerodrome SlipStream[216].

---

[216] Лучшие децентрализованные биржи по объему торгов // https://www.coingecko.com/ru/обмен/decentralized (дата обращения: 14.03.2025).

Так, 24 февраля 2025 г. прокуратура США по Южному округу Нью-Йорка (SDNY) и ФБР объявили, что криптовалютная биржа с Сейшельских островов признала себя виновной в ведении бизнеса по передаче денег без лицензии, нарушении законов США о борьбе с отмыванием денег и содействии подозрительным транзакциям на сумму более 5 млрд долл. Биржа согласилась выплатить более 504 млн долл., включая компенсацию в размере 420,3 млн долл. и штраф в размере 84,4 млн долл. Согласно данным SDNY биржа, несмотря на запрет для пользователей из США, привлекала американских клиентов, позволяла использовать VPN для обхода блокировки IP-адресов из США и позволяла пользователям не указывать своё имя или страну. Сотрудники биржи даже давали советы некоторым клиентам, как обойти процедуру KYC и политику, запрещающую клиентам из США торговать на платформе. Соглашение о признании вины предусматривало проведение консультантом двух ежегодных обзоров программ и политик соответствия требованиям, чтобы помешать пользователям из США использовать биржу. SDNY отметила частичное сотрудничество биржи и приняла во внимание ее усилия по исправлению положения[217].

Основываясь на вышеизложенном, следует заключить, что механизм следообразования в среде криптовалют представляет собой комплексный процесс, детерминированный технологическими особенностями блокчейна, выступающего в качестве основы для фиксации цифровых следов, сопутствующих преступной деятельности.

Криптовалюты, будучи псевдонимными, а не полностью анонимными, формируют устойчивые данные о транзакциях, доступные для криминалистического анализа. Публичный характер блокчейна, где каждая операция записывается в виде цепочки блоков, обеспечивает прозрачность и неизменяемость информации, что создает уникальные возможности для реконструкции преступных схем. Однако децентрализация и использование криптографических методов защиты требуют применения специализированных

[217] https://www.lexology.com/library/detail.aspx?g=162ca41d-075b-41af-8433-60ffd32cf33d

подходов к идентификации участников операций и интерпретации собранных данных.

Одним из ключевых элементов следообразования в криптовалютных сетях являются *транзакции*, которые фиксируют перемещения средств между адресами кошельков. Каждый адрес представляет собой криптографический хеш публичного ключа, что обеспечивает псевдонимность, но не исключает возможность установления связи между действиями пользователя и его реальной идентичностью. Транзакция включает в себя «входы» (источники средств) и «выходы» (получатели), она подписывается приватным ключом отправителя и после верификации сетью записывается в блокчейн. Этот процесс создает цифровой след, который сохраняется неограниченно долго благодаря свойствам неизменяемости распределенного реестра. При этом метаданные, такие как временны́е метки, комиссии и в некоторых блокчейнах (например, Ethereum) текстовые комментарии, дополняют основную информацию, предоставляя дополнительные векторы для анализа.

Важным аспектом следообразования выступает взаимодействие криптовалютных адресов с централизованными сервисами, такими как биржи, кошельки с обязательной верификацией (KYC) или миксеры. Биржи, требующие предоставления персональных данных пользователей, становятся точками деанонимизации, поскольку позволяют связать псевдонимный адрес с реальным лицом. В то же время сервисы смешивания монет предназначены для разрыва таких связей, однако их использование оставляет специфические «метки», такие как повторяющиеся суммы на входе и выходе или участие в транзакциях известных контрактов. Подобные «метки», в свою очередь, становятся объектом криминалистического изучения, позволяя выявлять попытки сокрытия преступных доходов.

Нельзя оставить без внимания и то, что цифровые следы в среде блокчейн формируются через совокупность данных, включая графы транзакций, поведенческие аномалии и корреляцию внутрисетевых и внешних данных. Анализ графов транзакций, построенных на основе связей между адресами,

позволяет реконструировать цепочки перемещения средств, выявляя ключевые узлы. Кроме того, интеграция данных из внешних источников (например, IP-адресов, участвующих в передаче транзакций, информации из соцсетей, форумов или утечек баз данных) значительно повышает точность деанонимизации.

Проведенный анализ позволяет сформулировать ряд общих выводов относительно особенностей следообразования, вызовов и перспектив криминалистического исследования блокчейн-среды.

1. Криптовалютная среда, основанная на технологии блокчейн, формирует уникальный механизм следообразования, детерминированный её децентрализованной архитектурой, криптографической защитой и прозрачностью данных. Каждая транзакция, записываемая в распределённый реестр, оставляет цифровые следы, характеризующиеся неизменяемостью и устойчивостью к фальсификации. Эти следы включают хеши транзакций, временны́е метки, цифровые подписи и метаданные, которые, несмотря на псевдоаномность адресов, позволяют реконструировать цепочки перемещения средств через анализ паттернов поведения, кластеризацию адресов и корреляцию с внешними данными.

2. Сочетание специализированных знаний и передового аналитического инструментария позволяет проводить комплексный анализ закономерностей, формирующихся в результате взаимодействия словообразующих элементов, таких как криптокошельки, криптографические адреса, данные, полученные с криптобирж, и сведения о платформах, используемых для осуществления транзакций. Таким образом, расследование преступлений, связанных с криптовалютой, требует постоянного развития специализированных инструментов для анализа блокчейна, деанонимизации транзакций и выявления преступных схем, реализуемых с использованием технологии распределенного реестра.

3. Вариативность хранения данных в криптокошельках определяет специфику применения различных криминалистических подходов к их идентификации и анализу и требует применения специализированных методов

«кластерного» и «графового» анализа для преодоления маскировки осуществляемых транзакций и установления связи между участниками преступной деятельности.

4. Архитектура используемой криптовалютной биржи (централизованной или децентрализованной) существенно дифференцирует «следовую картину», формирующуюся после совершения криптовалютных преступлений, что обусловлено различиями в механизмах функционирования, хранения данных и идентификации пользователей и требует разработки адаптированных криминалистических методик для каждой из архитектур.

§ 3. Типичные способы преступлений, совершаемых в отношении и с использованием криптовалют

Исследование типичных способов преступлений, связанных каким-либо образом с цифровой средой, требует методологически корректного подхода к классификации данных деяний, учитывающего их технологическую специфику и транснациональный характер. Профессор В.А. Образцов справедливо обращает внимание на то, что «…научно продуманное на основе данных следственной практики в сочетании с уголовно-правовыми и иными факторами построение криминалистических классификаций преступлений является важным и необходимым условием разработки эффективных методических рекомендаций по расследованию определенных категорий преступлений»[218].

Классификация в данном контексте выступает инструментом структурирования криминальных проявлений на основе общих признаков, выявленных эмпирически или через системный анализ их операционных механизмов. В данном случае системно-структурный подход позволяет рассматривать данные способы как элементы иерархической модели, где

[218] *Образцов В.А.* Проблемы совершенствования научных основ методики расследования преступлений: автореф. дис. ... канд. юрид. наук. – М., 1985. С. 8.

категория «криптопреступления» подразделяется на подвиды, соответствующие уровням их технической реализации и правового регулирования.

По верному утверждению А.Ю. Головина и Е.В. Головиной, классификация криптопреступлений, формируемая на основе ряда криминалистически значимых признаков (оснований), позволит выделить и изучить их отдельные виды, сформировать качественную криминалистическую характеристику таких деяний, а также определить новые пути уточнения существующих криминалистических методик расследования преступлений, объектом или средством совершения которых выступают криптовалюты[219].

Классификация преступлений, совершаемых в отношении и с использованием криптовалют, получает научную обоснованность при применении методологических принципов, сформулированных профессором Е.Е. Центровым. Согласно его позиции функциональное предназначение классификации заключается в группировке объектов, явлений и процессов на основе общих признаков и закономерных связей между ними, без претензии на раскрытие их сущностных свойств[220].

В данном контексте разделение криптопреступлений на две категории – 1) деяния, направленные на криптовалюту как непосредственный объект посягательства, и 2) деяния, использующие криптовалюту в качестве инструмента реализации противоправных целей – отражает операционно-

---

[219] *Головин, А. Ю.* Задачи криминалистики в сфере противодействия криптопреступности / А. Ю. Головин, Е. В. Головина // Санкт-Петербургский международный криминалистический форум : Материалы международной научно-практической конференции, Санкт-Петербург, 10-11 июня 2024 г. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2024. – С. 119-126.

[220] *Центров, Е.Е.* Теоретико-практический анализ соотношения понятий криминалистическая характеристика и классификация преступлений / Е. Е. Центров // Санкт-Петербургский международный криминалистический форум: Материалы международной научно-практической конференции, Санкт-Петербург, 10–11 июня 2024 г. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2024. – С. 537-542.

функциональные критерии, выявленные через анализ типовых способов преступной деятельности[221].

Для *первой* категории объединяющим признаком выступает целенаправленное воздействие на цифровые активы или их инфраструктуру, что проявляется в таких формах, как хищение средств через эксплуатацию уязвимостей смарт-контрактов, различные схемы обмана и вымогательства, а также манипуляции на крипторынке[222].

Вторая категория объединяет преступления, где криптовалюта играет роль инструмента обеспечения анонимности, скорости или трансграничности транзакций, включая легализацию (далее также – отмывание) преступных доходов, финансирование терроризма, незаконный оборот товаров и услуг, а также иных преступлений, где криптовалюта выступала средством финансирования преступной деятельности[223].

---

[221] *Астахова, Е. А.* Криминалистическая классификация транснациональных преступлений и ее использование в расследовании : дис. ... канд. юрид. наук. / Астахова Екатерина Алексеевна, 2023. – 215 с.

[222] При отнесении в эту группу мошенничеств мы отталкивались от позиции, выраженной в ст. 13 Конвенции ООН против киберпреступности, согласно положениям которой хищение или мошенничество с использованием информационно-коммуникационной системы признаются (a) любого ввода, изменения, удаления или блокирования электронных данных; (b) любого вмешательства в функционирование информационно-коммуникационной системы; (c) любого обмана в отношении фактических обстоятельств, совершенного с использованием информационно-коммуникационной системы и побуждающего лицо к какому-либо действию или бездействию, которого это лицо в противном случае не совершило бы; с мошенническим или бесчестным умыслом неправомерного извлечения для себя или для другого лица денежной или иной имущественной выгоды // Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационнокоммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (Принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 г.) // URL: https://docs.un.org/ru/A/RES/79/24 (дата обращения: 14.03.2025).

[223] В рассматриваемом контексте необходимо отметить существование сложных гибридных схем, в которых криптовалюты выполняют двойную роль, выступая одновременно и в качестве объекта, и в качестве инструмента преступления. Однако, как правило, технологический механизм реализации подобных преступных «гибридов» характеризуется временны́м разделением этапов, что позволяет аналитически дифференцировать различные аспекты преступной деятельности.

Научное обоснование разделения преступлений именно в такой концепции уже получило свое освещение в работах российских[224] и зарубежных ученых[225]. Таким образом, классификация, оставаясь вспомогательным инструментом, структурирует знания о криптопреступности, обеспечивая основу для междисциплинарного синтеза данных оперативно-розыскной деятельности, криминалистики и информационной безопасности.

На основании анализа научных исследований в области криминалистики, материалов следственной и судебной практики, а также принимая во внимание специфику оборота криптовалюты в контексте преступной деятельности, представляется возможным выделить следующие основные типы криптопреступлений.

1. Преступления, совершаемые в отношении криптовалюты. Данный тип преступлений характеризуется тем, что криптовалюта выступает в качестве предмета преступного посягательства. Преступления, связанные с криптовалютой, приобретают все более сложные и изощренные формы, представляя собой серьезную угрозу стабильности и безопасности криптовалютной инфраструктуры.

Одним из наиболее распространенных и опасных видов преступной деятельности являются кибератаки, направленные на криптовалютные платформы, с помощью которых реализуется: 1) незаконный доступ («взлом») к

---

[224] *Сидоренко, Э. Л.* Криптопреступность как новое криминологическое явление / Э. Л. Сидоренко // Общество и право. – 2018. – № 2(64). – С. 15-21; *Кушниренко, С. П.* Оборот криптовалют в механизме совершения преступлений / С. П. Кушниренко, А. Г. Харатишвили // Криминалистъ. – 2022. – № 3(40). – С. 77-83; *Перов, В. А.* О криминалистической методике выявления преступлений, совершаемых с использованием криптовалюты, и расследовании соответствующих уголовных дел // Российский следователь. – 2020. – № 12. – С. 10-13; *Русскевич, Е.А., Малыгин, И.И.* Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики. – 2021. – № 3. – С. 106-125; *Степаненко, Д.А., Гармышев, Я.В.* Криптовалюты как предмет и средство совершения преступлений: проблемы квалификации и расследования // Российский следователь. – 2025. – № 1. – С. 32-35; *Дорошков, В.В.* Уголовно-правовая политика Российского государства в современную эпоху / В. В. Дорошков // Мировой судья. – 2024. – № 5. – С. 2-8 и др.

[225] *Jung, J.* A study on pan-governmental and legislative controls related to cryptocurrency crime - Focusing on the amendments to the specific financial information act / J. Jung // The Journal of Police Science. – 2021. – Vol. 21 (1). – P. 61–89.

инфраструктуре криптовалютных бирж; 2) эксплуатация уязвимостей смарт-контрактов; 3) фишинговые атаки, нацеленные на кражу приватных ключей.

Каждый из указанных способов характеризуется уникальными особенностями реализации и влечет за собой различные последствия как для отдельных пользователей, так и для криптовалютной индустрии в целом.

1.1. Хищения посредством незаконного доступа к инфраструктуре («взлома») криптовалютных бирж. Централизованные криптовалютные биржи, функционирующие на основе кастодиальной модели управления активами, в силу концентрации значительных объемов криптографических средств в так называемых горячих кошельках, представляются для злоумышленников крайне привлекательной целью, что обусловливает высокий уровень риска подверженности данных платформ различного рода киберугрозам. Так, по оценкам аналитической компании Crystal Blockchain, общий объем средств, похищенных с централизованных криптовалютных бирж в период с 2012 по 2023 г.г., превысил 15 млрд долл. США[226]. Эти потери несут как сами биржи, так и их пользователи, инвестировавшие в цифровые активы.

В рамках анализа механизмов атак на такие биржи можно определить несколько ключевых векторов, характеризующихся различной степенью сложности и потенциальными последствиями.

Одним из наиболее распространенных векторов являются *уязвимости в интерфейсах программирования приложений.* Недостаточный уровень защиты таких интерфейсов, выражающийся в использовании слабых алгоритмов аутентификации или отсутствии эффективных механизмов контроля доступа, позволяет злоумышленникам осуществлять несанкционированные транзакции, выводить средства с кошельков пользователей и манипулировать рыночными данными. В качестве иллюстрации можно привести инцидент, произошедший с биржей KuCoin в 2020 г., когда злоумышленники, воспользовавшись

[226] Crypto-Assets Have Been Stolen / https://thefintechtimes.com/12-1billion-in-crypto-assets-have-been-stolen-over-ten-years-crystal-blockchain-analysis-finds/ (дата обращения: 14.03.2025).

уязвимостью в интерфейсах программирования приложений, похитили криптоактивы на сумму около 280 млн долл. США[227].

Второй значимый вектор угроз связан с так называемыми «инсайдерскими угрозами». Наличие у сотрудников биржи расширенного доступа к конфиденциальной информации создает потенциальную возможность для организации хищений или передачи данных третьим лицам. Ярким примером реализации данного вектора атаки является инцидент, произошедший с новозеландской биржей Cryptopia в 2019 г., когда сотрудник биржи умышленно допустил «утечку» конфиденциальной информации, что привело к хищению криптоактивов на сумму более 16 млн долл. США[228].

Еще одним распространенным методом, используемым злоумышленниками для подготовки и проведения атак на централизованные криптовалютные биржи, являются распределенные атаки типа «отказ в обслуживании» (DDoS). Данные атаки, направленные на перегрузку сетевой инфраструктуры и систем безопасности биржи, могут использоваться для отвлечения внимания служб безопасности от подготовки и реализации основной атаки, направленной на компрометацию хранилищ криптографических ключей или систем управления транзакциями[229].

В феврале 2025 г. криптобиржа Bybit также стала жертвой изощренной кибератаки, в ходе которой злоумышленникам удалось скомпрометировать кошелек Ethereum холодного хранения. Инцидент, охарактеризованный экспертами как образец высокотехнологичного цифрового вмешательства,

---

[227] The KuCoin Hack: What We Know So Far and How the Hackers are Using DeFi Protocols to Launder Stolen Funds // https://www.chainalysis.com/blog/kucoin-hack-2020-defi-uniswap/ (дата обращения: 14.03.2025).

[228] *Chen, W.* Phishing scam detection on Ethereum: Towards financial security for blockchain ecosystem / W. Chen, X. Guo, Z. Chen, Z. Zheng, Y. Lu // IJCAI. – 2020. – P. 4506–4512.

[229] Анализ, проведенный специалистами Chainalysis, показал, что компрометация закрытых ключей является наиболее распространенным способом хищения криптовалют, на долю которого приходится 43,8% всех зафиксированных случаев. Особую обеспокоенность вызывает деятельность киберпреступных групп, ассоциируемых с Корейской Народно-Демократической Республикой (КНДР), которыми в 2024 г. было похищено с криптоплатформ 1,34 млрд долл. // https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ (дата обращения: 14.03.2025).

произошел во время планомерной операции по перемещению активов между холодным и горячим кошельками[230]. Как выяснилось в ходе расследования, злоумышленники применили комбинацию методов: манипуляцию визуальным интерфейсом транзакций и скрытую модификацию логики смарт-контракта. Это позволило им сохранить видимость легитимного адреса получателя в интерфейсе, одновременно перенаправляя средства через перепрограммированные алгоритмы, что эффективно нейтрализовало защиту мультиподписи – ключевого элемента безопасности платформы[231].

Детальный анализ активности в блокчейне, проведенный экспертами в области кибербезопасности, выявил, что злоумышленники получили доступ к учетным данным в результате применения методов социальной инженерии, и это стало отправной точкой для последующей компрометации системы[232]. Примечательно, что случившаяся атака имела закономерное сходство с инцидентом, произошедшим на платформе Phemex в январе 2025 г. Это обстоятельство позволило аналитикам предположить связь обоих случаев с деятельностью северокорейской хакерской группировкой Lazarus Group[233].

1.2. Хищение посредством использования уязвимостей смарт-контрактов. Смарт-контракты, функционирующие в децентрализованных сетях (например, Ethereum, Solana и др.), представляют собой программные коды, автоматически исполняемые при наступлении определенных условий. Несмотря на кажущуюся надежность, смарт-контракты уязвимы к различным типам ошибок в коде, позволяющим злоумышленникам манипулировать логикой

---

[230] *Krause, D.* The $1.4 Billion Bybit Hack: Cybersecurity Failures and the Risks of Cryptocurrency Deregulation / D. Krause. – 2025. – Available at SSRN: https://ssrn.com/abstract=5150171 (дата обращения: 14.03.2025).

[231] Chainalysis. Crypto crime report: Blind signing risks and smart contract fraud [Electronic resource]. – 2025. – URL: https://www.chainalysis.com/reports/crypto-crime-2025 (дата обращения: 14.03.2025).

[232] *Lakshmanan, R.* Bybit Confirms Record-Breaking $1.46 Billion Crypto Heist in Sophisticated Cold Wallet Attack/ R. Lakshmanan // The Hacker News. – 2025, February 22. – URL: https://thehackernews.com/2025/02/bybit-confirms-record-breaking-146.html (дата обращения: 14.03.2025).

[233] *Dhage, S.* Crypto exchange Bybit confirms hack as over $1.4 billion worth of ETH leaves wallets / S. Dhage // The Block. – 2025. – February 21. – URL: https://www.theblock.co/post/342667/crypto-exchange-bybit-hacked-as-over-1-billion-worth-of-eth-leaves-wallets (дата обращения: 14.03.2025).

выполнения контракта и получать несанкционированный доступ к активам. Анализ технических аспектов эксплуатации уязвимостей смарт-контрактов позволяет выявить наиболее распространенные векторы атак и разработать эффективные методы защиты[234].

Одной из наиболее опасных уязвимостей является «reentrancy-атака», предполагающая повторный вызов функции смарт-контракта до завершения предыдущей операции. Злоумышленник, обнаружив эту уязвимость, может вызвать функцию контракта, которая в свою очередь повторно вызовет ту же функцию, что позволяет обойти ограничения и получить несанкционированный доступ к средствам. Подобный способ был реализован с криптобиржей DAO в 2016 г., что привело к ущербу, исчисляемому в нескольких десятках миллионов долларов[235].

Другой распространенной уязвимостью являются ошибки в арифметических операциях, известные как «целочисленное переполнение/антипереполнение» (с англ. – «integer overflow/underflow»)[236]. Данные ошибки, возникающие при переполнении или недополнении (выходе за границы) целочисленных переменных, используемых в смарт-контрактах, позволяют злоумышленникам искусственно увеличивать балансы активов или выполнять другие несанкционированные операции. Например, значительный резонанс получило дело криптоплатформы BeautyChain в 2018 г., когда злоумышленники воспользовались указанной ошибкой для увеличения баланса токенов[237].

Некорректная валидация прав доступа представляет собой еще один значимый фактор уязвимости. Недостаточные проверки прав доступа при

---

[234] *Перов, В.А.* Квалификация преступлений, совершаемых с использованием криптовалюты: дис. … канд. юрид. наук / Перов Валерий Александрович. – 2023. – 261 с.

[235] *Baum, C.* A framework for universally composable publicly verifiable cryptographic protocols [Electronic resource] / C. Baum, B. David, R. Dowsley // Cryptology ePrint Archive, Report 2020/207. – 2020. – URL: https://eprint.iacr.org/2020/207 (дата обращения: 14.03.2025).

[236] Breaking the Bank: Exploiting Integer Underflow in Smart Contracts // https://www.kayssel.com/post/web3-8/ (дата обращения: 14.03.2025).

[237] *Sun, T.* A Formal Verification Framework for Security Issues of Blockchain Smart Contracts / T. Sun, W. Yu // Electronics. – 2020. – Vol. 9. – P. 255. – DOI: 10.3390/electronics9020255.

выполнении критических функций смарт-контракта позволяют злоумышленникам вызывать эти функции и манипулировать активами, не имея на это достаточных полномочий.

Атака на криптобиржу Poly Network, произошедшая в 2021 г., является наглядным примером последствий эксплуатации уязвимостей смарт-контрактов. Злоумышленники выявили уязвимость в функции cross-chain свопа, позволявшую подменять параметры транзакции. Эксплуатация данной уязвимости привела к хищению криптоактивов на сумму 611 млн долл. США, распределенных между блокчейнами Ethereum, Binance Chain и Polygon. Уникальность данного инцидента заключается в том, что злоумышленники вернули 99% похищенных средств после оказания на них публичного давления, что свидетельствует о важной роли социальных факторов в обеспечении безопасности децентрализованных финансов[238].

1.3. Фишинговые атаки и хищение приватных ключей. Подобные атаки представляют собой один из наиболее распространенных методов хищения криптоактивов для получения доступа к приватным ключам пользователей, обеспечивающим контроль над криптокошельками.

На этапе составления фишинговых сообщений лица, причастные к преступной деятельности, разрабатывают коммуникативные приманки (электронные письма, SMS, сообщения в мессенджерах или социальных сетях)[239], имитирующие официальные уведомления от легитимных организаций (криптовалютных бирж, кошельков, платежных систем и т. д.)[240]. Эти сообщения

---

[238] Tech. Hacker behind $600 million crypto heist returns final slice of stolen funds // https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html

[239] *Дамирчиев, Э. И.* Социальные сети как источник оперативно значимой информации при выявлении и раскрытии преступлений / Э. И. Дамирчиев, А. А. Комоско, В. Ф. Васюков // Современное общество и право. – 2024. – № 3(70). – С. 72-78.

[240] Illicit Financial Flows from Cyber-Enabled Fraud / FATF – Interpol - Egmont Group // FATF. – Paris, France. – 2023. – URL: www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyberenabled-fraud.html (дата обращения: 14.03.2025).

создаются с использованием элементов социальной инженерии для повышения их правдоподобности и мотивации получателей к немедленным действиям[241].

В процессе реализации следующего этапа происходит распространение фишинговых сообщений посредством специализированных сетей зараженных компьютеров («бот-сетей») для автоматизации процесса отправки электронных писем и SMS-сообщений. Эти программы могут обрабатывать большие объемы данных, отправлять сообщения с различных IP-адресов и обходить некоторые фильтры спама[242].

Фишинговая рассылка становится возможной благодаря получению злоумышленниками несанкционированного доступа к базам данных, содержащим адреса электронной почты, номера телефонов, аккаунтов и иных персональных данных. Такие базы данных становятся доступными благодаря утечкам данных с различных сервисов, сайтов, либо проданных сотрудниками банковских организаций, сервисных служб. Также в настоящее время популярен автоматизированный сбор информации («скрапинг»), который позволяет злоумышленникам с использованием специально разработанного программного обеспечения аккумулировать большие объемы контактной информации из социальных сетей[243]. В такую информацию, как правило, входят демографические данные, интересы, профессиональная деятельность, географическое положение пользователя и др.

При этом злоумышленники тщательно воспроизводят визуальные элементы брендов легитимных компаний, включая логотипы, цветовую гамму, шрифты и другие элементы фирменного стиля, чтобы создать иллюзию аутентичности. В фишинговых сообщениях используются убедительные языковые конструкции, в том числе формулировки, требующие немедленных

---

[241] *Choi, Y.* Messenger phishing modus operandi in South Korea / Y. Choi, S. Choi // Journal of Korean Public Police and Security Studies. – 2021. – Vol. 18 (3). – P. 241–258.

[242] Приговор Дзержинского районного суда г. Перми (Пермский край) от 11 марта 2021 г. по делу № 1-67/2021 // СПС «КонсультантПлюс» (дата обращения: 14.03.2025).

[243] *Sharma, A.* Simulating data breaches: Synthetic datasets for depicting personally identifiable information through scenario-based breaches / A. Sharma, M. Bantan // Data in Brief. – 2025. – Vol. 58. – P. 111-207.

действий («срочно обновите», «подтвердите сейчас», «не упустите шанс»), чтобы снизить критичность мышления получателей. Также используется терминология и профессиональный жаргон для придания сообщению видимости легитимности и авторитетности.

В данном случае прослеживается систематичное обещание материальных выгод, бонусов, выигрышей или других преимуществ для усиления мотивации получателей перейти по ссылке или предоставить данные. Могут также использоваться угрозы о блокировке аккаунта, потере средств или других негативных последствиях в случае игнорирования требований сообщения[244].

В фишинговых сообщениях довольно часто используется замена букв на похожие символы (например, латинскую «О» на ноль «0») для маскировки под похожие домены. Дизайн и структура сообщений разрабатываются таким образом, чтобы соответствовать общепринятым нормам оформления официальных писем и сообщений, что также повышает их правдоподобность[245].

1.4. Использование вредоносных программ для хищения seed-фраз к крипткошелькам, сохраненных в смартфонах. Хищение seed-фраз, являющихся ключами доступа к криптовалютным кошелькам, представляет собой серьёзную угрозу для владельцев цифровых активов. Злоумышленники всё чаще используют вредоносное программное обеспечение, ориентированное на мобильные устройства, для нарушения конфиденциальности этих критически важных данных. Вредоносные программы распространяются различными способами, включая поддельные мобильные приложения, уязвимости в операционных системах и приложениях, а также методы социальной инженерии, направленные на обман пользователей.

После установки вредоносное приложение активирует функции, предназначенные для обнаружения и извлечения seed-фраз. К таким функциям

---

[244] Тренды фишинговых атак на организации в 2022–2023 годах / Positive Technologies. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/phishing-attacks-onorganizations-in-2022-2023 (дата обращения: 14.03.2025).

[245] *Комков, В. В.* Этапы актуальных атак посредством фишинговых писем / В. В. Комков // Журнал высоких гуманитарных технологий. – 2024. – № 3(6). – С. 39-46.

относятся: кейлоггинг[246], позволяющий перехватывать нажатия клавиш; мониторинг буфера обмена для выявления скопированных данных; сканирование файлов в поисках последовательностей, соответствующих формату seed-фраз; захват скриншотов и видеозаписей экрана; а также несанкционированный доступ к данным других приложений. Извлеченные seed-фразы передаются на серверы, контролируемые злоумышленниками, что впоследствии позволяет им получить несанкционированный доступ к криптовалютным кошелькам и похитить все имеющиеся средства.

Так, в феврале 2025 г. экспертами «Лаборатории Касперского» был выявлен ряд вредоносных программных приложений («стилеров») в магазинах приложений Google Play и, впервые, в Apple App Store, предназначенных для несанкционированного доступа к криптовалютным кошелькам пользователей[247]. В ходе исследования было установлено, что приложения, разработанные для операционных систем Android и iOS, содержат встроенное вредоносное программное обеспечение, функционал которого направлен на хищение фраз восстановления, необходимых для получения доступа к криптовалютным кошелькам.

В связи с тем, что фразы восстановления, как правило, хранятся в виде графических изображений, вредоносные программы используют плагины для оптического распознавания текста, разработанные на основе библиотеки Google ML Kit. Таким образом, в очередной раз технологии машинного обучения были использованы для осуществления противоправной деятельности. Криминальная кампания, получившая название среди фигурантов «SparkCat», продемонстрировала высокую эффективность – в магазине приложений Google

---

[246] *Кейлогинг* – (с англ. – «keylogging») - это противоправный механизм использования программного или аппаратного инструмента для записи нажатия клавиш пользователем, отправляемые на сервер, подконтрольный злоумышленнику. *Bhardwaj, A.* Keyloggers: silent cyber security weapons / A. Bhardwaj, S. Goundar // Network Security. – 2020. – P. 14–19.

[247] Новая вредоносная программа SparkCat с помощью нейросети крадёт данные на фото в iOS и Android-смартфонах / 4 февраля 2025 г. – URL: https://www.kaspersky.ru/about/press-releases/novaya-vredonosnaya-programma-sparkcat-s-pomoshyu-nejroseti-kradyot-dannye-na-foto-v-ios-i-android-smartfonah?ysclid=m8bi3y9jlf326805689 (дата обращения: 14.03.2025).

Play зараженные приложения были загружены более 242 000 раз[248]. Причем в магазине приложений Apple App Store они были зафиксированы впервые[249].

1.5. Использование вредоносных программ в целях получения выкупа в криптовалюте («криптовымогательство»). Ключевым механизмом реализации таких преступлений выступает «ransomware» – вредоносное программное обеспечение, осуществляющее блокировку или шифрование данных с последующим требованием выкупа в цифровых валютах. Согласно данным аналитической компании Chainalysis, общий объем выплат жертв таких преступлений к 2024 г. достиг 1,1 млрд долл. США, при этом 70% операций осуществлялись в Bitcoin, а 25% – в Monero, что подчёркивает растущую популярность приватных криптоактивов в преступных схемах[250].

Параллельно с вредоносными программами активизируется метод «DDoS-вымогательства», при котором злоумышленники угрожают перегрузкой серверов жертвы распределёнными атаками «отказ в обслуживании» («Distributed Denial of Service»). Примером служит атака на Новозеландскую фондовую биржу в 2020 г., после успеха которой преступники требовали выплаты в криптовалюте XMR, а также деятельность группировки Armada Collective (2016-2018 гг.), специализировавшейся на шантаже финансовых институтов в азиатских странах.

Одним из ключевых трендов, определяющих современный характер криптовымогательств, является популяризация в преступных кругах модели Ransomware-as-a-Service (RaaS). Данная модель предполагает предоставление вредоносного программного обеспечения в аренду, что позволяет лицам, не

---

[248] Отдельного внимания заслуживает тот факт, что для взаимодействия с контрольным сервером (или серверами) вредоносная программа использовала протокол, структура которого на момент обнаружения не была установлена, разработанный с использованием языка программирования Rust. Язык программирования Rust представляет собой относительно новый язык программирования, который крайне редко используется при разработке мобильных приложений. https://www.tadviser.ru/index.php/Статья:Безопасность_приложений_в_Google_Play_Store?ysclid=m8bi90vip7904781818 (дата обращения: 13.04.2025).

[249] «Лаборатория Касперского» обнаружила первый вирус для кражи данных с фото в iPhone – URL: https://www.forbes.ru/tekhnologii/530142-laboratoria-kasperskogo-obnaruzila-pervyj-virus-dla-krazi-dannyh-s-foto-v-iphone (дата обращения: 13.04.2025)

[250] The 2025 Crypto Crime Report – URL: https://go.chainalysis.com/2025-Crypto-Crime-Report.html (дата обращения: 13.04.2025).

обладающим специализированными техническими знаниями и навыками, осуществлять кибератаки с целью вымогательства, выплачивая разработчикам программного обеспечения определенный процент от полученного выкупа. Параллельно распространяется практика «двойного вымогательства», сочетающая шифрование данных с угрозой публикации конфиденциальной информации, что усиливает давление на жертв.

Лица, занимающиеся распространением программ-вымогателей, привлекают к участию третьих лиц – «денежных мулов»[251]. Зачастую такие лица не имеют опыта работы в сети Интернет и характеризуются низкой цифровой грамотностью. Для них создаются учетные записи электронной почты у анонимных провайдеров, находящихся вне юрисдикции правоохранительных органов, что затрудняет идентификацию владельцев. «Денежные мулы» используют предоставленные кураторами мобильные устройства для регистрации в финансовых учреждениях или у ПУВА. После успешной регистрации устройства возвращаются кураторам, которые используют их для проведения транзакций от имени «денежных мулов». В ряде случаев преступники применяют VPN для анонимизации IP-адресов используемых устройств, что позволяет скрыть фактическое географическое местоположение лица, осуществляющего транзакцию[252].

Новым вектором развития этого способа криптопреступлений является интеграция инструментов искусственного интеллекта для оптимизации атак – нейросети используются для генерации персонализированных фишинговых сообщений, анализа уязвимостей целевых систем и прогнозирования поведения жертв. Иллюстрацией служит инцидент с клиниками Kaiser Permanente в 2023 г., где хакеры, применив алгоритмы искусственного интеллекта, похитили данные

---

[251] *Бекетнова, Ю. М.* Модели и типологии отмывания преступных доходов / Ю. М. Бекетнова. – Москва : Общество с ограниченной ответственностью "Русайнс", 2020. – 84 с.

[252] FATF. Countering Ransomware Financing [Electronic resource]. – Paris, 2023. // FATF. – URL: http://www.fatf-gafi.org/publications/Methodsandtrends/countering-ransomware-financing.htm

10 млн пациентов и потребовали выкуп в 10 млн долл. в криптовалюте Monero[253].

1.5. Мошенничество с инвестициями в сфере криптовалют представляет собой системную угрозу, обусловленную спецификой функционирования криптовалютной экосистемы и эксплуатирующую доверие пользователей к инновационным финансовым инструментам. Данный вид преступной деятельности, демонстрирующий высокую степень адаптивности и изобретательности, включает в себя три основных направления: фиктивные ICO[254], финансовые пирамиды и создание фейковых платформ, каждое из которых обладает уникальными механизмами обмана, нанося значительный ущерб как индивидуальным инвесторам, так и всей экосистеме цифровых активов.

Фиктивные ICO, представляющие собой механизмы привлечения инвестиций посредством выпуска собственных токенов, часто используются злоумышленниками для организации мошеннических схем. Злоумышленники создают проекты с поддельными техническими документами, так называемыми «белыми книгами» («whitepapers»), содержащими преувеличенные обещания доходности, описания нереализуемых технологий и несуществующий состав команды разработчиков. После привлечения средств платформа прекращает свое существование, а собранные активы похищаются. Примером реализации данного типа мошенничества является криптобиржа BitConnect (2017-2018 гг.), руководители которой обещали инвесторам ежедневную доходность в размере до 1% через «торгового бота». После привлечения около 2,4 млрд долл. США

---

[253] Kaiser Permanente: Data breach may impact 13.4 million patients. – URL: https://growthinvests.com/california/story/2024-04-26/kaiser-permanente-notifies-13-4-million-members-of-data-breach (дата обращения: 14.03.2025).

[254] ICO, Initial coin offering (с англ. – первичное предложение (размещение) монет) – форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной генерацией.

платформа прекратила свою деятельность, а стоимость токена BitConnect снизилась практически до нуля[255].

Одним из вариантов совершения мошеннических действия является создание финансовых пирамид («схемы Понци»[256]) – псевдоинвестиционных платформ, обещающих инвесторам высокую доходность (до 10-30% в месяц) за счет использования «уникальной» стратегии арбитражной криптовалютной торговли[257]. Выплаты первым инвесторам осуществляются за счет средств, привлекаемых от новых участников, создавая иллюзию прибыльности и устойчивости системы, что стимулирует дальнейшее привлечение средств. Технологические особенности таких схем включают использование смарт-контрактов для автоматизации выплат, что повышает уровень доверия, а также интеграцию реферальных программ с многоуровневыми бонусами, обеспечивающими экспоненциальный рост привлеченных средств[258].

Одним из самых ярких примеров крупномасштабного мошенничества в сфере криптовалют, совершенного по методу создания финансовой пирамиды, является случай с криптобиржей «PlusToken», произошедший в Китайской Народной Республике в 2019 г. Данный прецедент продемонстрировал деструктивный потенциал финансовых пирамид, искусно замаскированных под инновационные инвестиционные инструменты. Суть схемы заключалась в продвижении псевдоинвестиционного проекта, обещавшего инвесторам стабильно высокую доходность в размере 10-30% ежемесячно, что привлекло

---

[255] Vítimas de pirâmide que deixou prejuízo de US$ 2,4 bilhões só vão receber US$ 17 milhões de restituição – URL: https://portaldobitcoin.uol.com.br/vitimas-de-piramide-que-deixou-prejuizo-de-us-24-bilhoes-so-vao-receber-us-17-milhoes-de-restituicao/ (дата обращения: 14.03.2025).

[256] Во многих юрисдикциях подобный способ обмана называется «Схема Понци» в честь Чарльза Понци - итальянского афериста, который в начале XX века прославился тем, что организовал одну из первых и самых известных финансовых пирамид. *Mukherjee, S.* Cryptocurrency Ponzi schemes / S. Mukherjee, C. Larkin, S. Corbet // Understanding Cryptocurrency Fraud: The Challenges and Headwinds to Regulate Digital Currencies. – 2021. – Vol. 2. – P. 111.

[257] *Мурадян, С. В.* Актуальные проблемы противодействия деятельности криптовалютных пирамид / С. В. Мурадян // Имущественные отношения в Российской Федерации. – 2024. – № 2(269). – С. 93-104.

[258] *Ghani, M.T.A.* An exploratory inquiry on the decision process of Ponzi scheme investor's: A qualitative case study approach / M.T.A. Ghani, B.A. Halim, S.A.A. Rahman // International Journal of Management. – 2020. – Vol. 11 (12). – P. 220–236.

значительное число участников, поверивших в возможность быстрого и легкого обогащения[259].

В ходе реализации схемы организаторы незаконной деятельности привлекли около 3 млрд долл. США в различных криптовалютах. Привлеченные средства не использовались для реальной инвестиционной деятельности, а распределялись между участниками схемы по принципу финансовой пирамиды: выплаты ранним инвесторам осуществлялись за счет средств, поступавших от новых участников.

После реализации основного замысла организаторы предприняли попытки сокрытия следов преступной деятельности, переместив около 194 000 BTC через сервисы смешивания криптовалют, предназначенные для обеспечения анонимности транзакций. Однако, несмотря на предпринятые меры, правоохранительным органам удалось раскрыть схему и привлечь к ответственности организаторов. В результате расследования китайскими правоохранительными органами были арестованы 27 участников преступной группы, шестеро из которых были приговорены к различным срокам тюремного заключения[260].

Однако даже такие резонансные случаи не имеют должного воздействия на лиц, которые вовлекаются в новые криптовалютные пирамиды. Так, в 2022 г. бразильской федеральной полицией совместно с Управлением расследований внутренней безопасности США была проведена операция по разоблачению транснациональной криптовалютной мошеннической схемы, базирующейся в бразильском городе Куритиба. Общая сумма ущерба составила более 4 млрд бразильских реалов[261].

---

[259] *Lee, K.* Recent criminal law issues on cryptocurrency / K. Lee, C. Bae // Northeast Asian Law Journal. – 2023. – Vol. 16 (4). – P. 191–217.

[260] Дело PlusToken оказало значительное влияние на регуляторную политику Китая в отношении криптовалют и стало одним из факторов, ускоривших введение полного запрета на операции с криптовалютами на территории страны. *Riley, J.* The Current Status of Cryptocurrency Regulation in China and Its Effect around the World / J. Riley // China and WTO Review. – 2021. – Vol. 7. – P. 135-152.

[261] Организатором схемы стал Франсиско Вальдевино да Силва (37 лет), известный под псевдонимом «Биткойн Шейх» («Bitcoin Sheikh»). К операции были привлечены более 100

1.6. Создание поддельных криптовалютных бирж и кошельков представляет собой еще один распространенный метод мошенничества. Злоумышленники используют различные тактики, включая создание доменов-клонов, имитирующих интерфейсы известных платформ (например, путём незначительного изменения написания названия или используя поддельные SSL-сертификаты)[262].

Вредоносные приложения, распространяемые под видом легитимных, служат для кражи seed-фраз и приватных ключей. Также используются фиктивные листинги, когда мошенники берут плату за размещение токенов на несуществующих биржах. Для маскировки мошеннической деятельности используются рекламные кампании в социальных сетях с фальшивыми отзывами, а также подделка лицензий и сертификатов. Примером данной тактики является ICOMINI, специально созданная платформа-клон оригинального проекта, которая собрала 10 млн долл. США, имитируя законный интернет-сайт[263].

1.7. Манипулирование рыночной конъюнктурой в сфере криптовалют представляет собой деструктивный феномен, характеризующийся намеренным искажением ценовых параметров и показателей ликвидности с целью получения неправомерной выгоды.

В настоящее время наиболее распространена схема «накачка и сброс» (с англ. – *«pump-and-dump»)*, целью которой является массовая скупка малоликвидных криптоактивов, что приводит к искусственному увеличению их рыночной стоимости. Создаваемый ажиотаж привлекает внимание розничных

сотрудников полиции, которые провели обыски по 20 адресам. US-Brazil investigation leads to disruption of transnational cryptocurrency fraud ring – URL: https://www.ice.gov/news/releases/us-brazil-investigation-leads-disruption-transnational-cryptocurrency-fraud-ring (дата обращения: 14.03.2015).

[262] *Глотов, В. И.* Криптобезопасность криптовалют / В. И. Глотов, Д. М. Михайлов. – Москва : Российский экономический университет имени Г.В. Плеханова, 2019. – 116 с.

[263] *Lin, D.* Towards Understanding Crypto Money Laundering in Web3 Through the Lenses of Ethereum Heists / D. Lin, J. Wu, Q. Fu, Y. Yu, K. Lin, Z. Zheng, S. Yang // Proceedings of the ACM SIGMETRICS Conference 2023 (SIGMETRICS'23), June 19–23, 2023, Orlando, Florida, USA. – New York, NY, USA: ACM, 2023. – P. 21.

инвесторов, которые, поддавшись импульсу, приобретают активы по завышенным ценам. На пике спроса организаторы схемы осуществляют скоординированный сброс активов, получая существенную прибыль, а розничные инвесторы, в свою очередь, несут значительные убытки в результате стремительного обвала рыночной стоимости активов[264].

Еще одним способом манипулирования рынком является *размещение крупных ордеров на покупку или продажу активов без намерения их исполнения.* Данные ордера создают иллюзию высокого спроса или предложения на рынке, что оказывает влияние на решения других участников торгов. После изменения ценовой конъюнктуры в желаемом для манипуляторов направлении ордера отменяются, а участники рынка, принявшие решения на основании ложной информации, несут финансовые потери.

В 2020 г. Комиссия по торговле товарными фьючерсами США оштрафовала криптобиржу BitMEX на 100 млн долл. за допущение незаконных манипуляций. Трейдеры размещали крупные ордера на покупку Биткоина без намерения их исполнять, создавая иллюзию спроса. После роста цены ордера отменялись, а активы продавались по завышенной стоимости[265].

В сфере децентрализованных финансов злоумышленники могут осуществлять *атаки на пулы ликвидности*, используя уязвимости алгоритмов автоматизированного так называемого маркет-мейкинга. Данные алгоритмы определяют цену актива на основании соотношения токенов в пуле ликвидности. Манипулируя балансом пула, фигуранты могут изменять цену актива в желаемом направлении, извлекая прибыль за счет других участников торгов[266].

В качестве иллюстрации атаки на пулы ликвидности можно привести пример «сэндвич-атаки» на протокол SushiSwap в 2023 г. Злоумышленники,

---

[264] *Bhatia, N.* A detailed review of blockchain and cryptocurrency / N. Bhatia, S. Bansal, S. Desai // CoRR. 2023. – URL: https://arxiv.org/abs/2303.06008 (дата обращения: 14.03.2025).

[265] BitMEX crypto exchange agrees to pay $100 million to get financial regulators off its back // https://www.theverge.com/2021/8/10/22619180/bitmex-crypto-fine-fincen-cftc-100-million (дата бращения: 14.03.2025).

[266] *Alrawi, O.* Forecasting malware capabilities from cyber attack memory images / O. Alrawi et al. // USENIX Security. – 2021. – P. 3523–3540.

используя специализированный бот, перехватили крупную транзакцию по покупке криптовалюты WETH. Схема атаки состояла из двух последовательных этапов. На первом этапе бот, принадлежавший злоумышленникам, приобретал WETH до момента исполнения целевой транзакции, тем самым искусственно увеличивая его рыночную стоимость. На втором этапе, после исполнения ордера жертвы, бот продал приобретенные ранее токены, получив прибыль в размере 500 000 долл. США за счет искусственно созданного дисбаланса в пуле ликвидности[267].

1.7. *Мошенничества, связанные с привлечением жертв посредством романтических знакомств.* Методы обмана в современных реалиях высокой организованности преступных сообществ, занимающихся проработкой новых направлений деятельности, преобразуются в комбинированные формы[268]. Изучение полицейских сайтов и иностранной литературы, посвященной противодействию дистанционным формам мошенничества, показало, что для обозначения комбинированных методов в основном используются четыре термина.

1.7.1. *«Романтическая приманка» (с англ. – «Romance baiting»)* – впервые был использован австралийской полицией в пресс-релизе «Scamwatch» – социальной программы, инициированной в феврале 2021 г. для противодействия дистанционным мошенничествам в преддверии Дня Святого Валентина. На тот момент новый вид обмана описывался следующим образом: «Данная техника предполагает установление злоумышленником контакта с потенциальной жертвой в приложениях для знакомств с последующим переносом коммуникации в зашифрованный канал. После установления доверительных отношений, длящихся, как правило, несколько недель, злоумышленник начинает

---

[267] *Stathakopoulou, C.* Adding Fairness to Order: Preventing Front-Running Attacks in BFT Protocols using TEEs / C. Stathakopoulou, S. Rüsch, M. Brandenburger, M. Vukolic // 2021 40th International Symposium on Reliable Distributed Systems (SRDS). – 2021. – P. 34-45.

[268] *Титов, А.А.* Отдельные аспекты выявления и раскрытия криптомошенничеств в Индии / А.А. Титов // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 3 (98). – С. 279-283.

сбор информации о финансовом положении жертвы и предлагает участие в криптовалютной инвестиционной схеме»[269].

1.7.2. *«Крипторомантическая афера» (с англ. – «CryptoRom»)* – упоминается в ряде зарубежных исследований при рассмотрении многоуровневых схем мошенничеств, совершаемых с использованием различных методов «углубленной социальной инженерии», когда злоумышленник «влюбляет в себя» жертву[270].

1.7.3. *«Романтическое мошенничество» (с англ. – «Romantic scam»)* – термин, который довольно популярен среди правоохранительных органов различных стран, которые его используют в своих отчетах и рекомендациях. Так, например, Оперативный отдел по борьбе с преступлениями против личности, совершаемых с использованием компьютерных устройств и социальных сетей Почтовой полиции Италии, рассматривает этот вид мошенничества как главную угрозу финансовой стабильности населения[271]. Подобный термин также используется сотрудниками ФБР США[272] и полицейскими Нового Южного Уэльса[273]

1.7.4. *«Мошенничество с разделкой свиней» (в англ. транскрипции – «Sha zhu pan»).* Широкое распространение это явление получило в Китае. Термин «Sha zhu pan» используется при описании преступной схемы, которая включает в себя: «откорм» жертвы, в ходе которого используются известные методы романтического мошенничества для установления доверия и вероятного

---

[269] Australian Competition and Consumer Commission. Romance baiting scams on the rise [Electronic resource]. – 2021. – URL: https://www.accc.gov.au/media-release/romance-baiting-scams-on-the-rise

[270] Polizia Postale. Report annuale 2024. Aggiornamento 21/12/2024 // Sophos News. – URL: https://news.sophos.com/en-us/2023/08/02/sha-zhu-pan-scam-uses-ai-chat-to-target-iphone-and-android-users (дата обращения: 13.04.2025).

[271] Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche – URL: https://www.commissariatodips.it/docs/____NEW_Report_2024_SPPSC_DEF_____1.pdf (дата обращения: 13.04.2025).

[272] Romance Scams – URL: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams (дата обращения: 13.04.2025).

[273] Dating and romance scams – don't let them break your heart or wallet – URL: https://www.police.nsw.gov.au/crime/frauds_and_scams/fraud_categories/dating_and_romance_scams (дата обращения: 13.04.2025).

выполнения любых требований финансового характера; «забой» жертвы происходит после получения максимального доверия к инвестору. На этой стадии потерпевший переводит все деньги на криптокошелек, подконтрольный мошеннику[274].

Различные термины, несмотря на различие в названиях, описывают схожий способ мошенничества, объединяющий несколько методов обмана. Реализация рассматриваемого преступления начинается с установления контакта с потенциальной жертвой через приложения для знакомств или социальные сети, как правило, под предлогом установления романтических отношений. Например, злоумышленники устанавливают первоначальный контакт через приложения Tandem, Tinder, Badoo, LinkedIn, где пользователи взаимодействуют с носителями их языка[275].

Злоумышленник инициирует контакт с жертвой в приложении, посредством которого произошло первоначальное знакомство. Затем под различными предлогами беседа переносится в иное приложение (например, WhatsApp[276], Telegram, WeeChat), где обсуждаются вопросы торговли криптовалютами. Общение носит систематический характер, в ходе которого жертве демонстрируются детали роскошного образа жизни злоумышленника. Как правило, используются фотографии, предварительно обработанные с целью демонстрации дорогостоящих автомобилей, предметов роскоши и интерьеров фешенебельных отелей и курортов. В контексте переписки мошенник сообщает о своей деятельности в качестве криптоинвестора, ненавязчиво демонстрируя скриншоты регулярно поступающих транзакций.

Китайский исследователь Ф. Ванг отмечает, что в ряде случаев «жертве оказываются знаки внимания, направляются подарки посредством служб

---

[274] *Wang, F.* Victim-offender overlap: the identity transformations experienced by trafficked Chinese workers escaping from pig-butchering scam syndicate / F. Wang // Trends Organ Crim. – 2024. – DOI: https://doi.org/10.1007/s12117-024-09525-5.

[275] Anlagebetrug: Ein andauerndes Phänomen mit hohen Schadenssummen – URL: https://lka.polizei.nrw/artikel/anlagebetrug-ein-andauerndes-phaenomen-mit-hohen-schadenssummen (дата обращения: 14.03.2025).

[276] Продукт компании Meta, признанной в Российской Федерации экстремистской организацией, ее деятельность на территории РФ запрещена.

доставки, а также применяются эффективные методы психологического воздействия для установления устойчивой социальной связи»[277].

Фактически указанные действия направлены на вовлечение потерпевшего в процесс обучения криптоинвестированию с целью получения быстрой прибыли. Для этого потерпевшему предлагается установить приложение, пройти регистрацию и осуществить привязку банковского счета для последующего перевода денежных средств в криптовалюту[278].

Следует отметить, что в традиционных схемах «романтического» мошенничества просьба о переводе денежных средств, как правило, обусловлена чрезвычайными обстоятельствами (медицинские, уголовно-правовые или коммерческие расходы). В рассматриваемых нами случаях жертвам предлагают осуществить прямой перевод денежных средств преступнику, используя различные платежные системы. При этом злоумышленник получает полный контроль над финансовыми активами жертвы, основываясь на доверии к «привлекательному и успешному инвестору». В практике китайских следственных органов зафиксированы случаи, когда жертва «Sha zhu pan» передавала злоумышленнику управление не только личными счетами, но и счетами родственников[279].

Непрекращающееся использование видимости подлинных отношений в целях обмана жертв подчеркивает эффективность данного механизма для установления доверия, взаимопонимания и, как следствие, получения преступной прибыли. Использование романтических отношений в качестве основы позволяет нивелировать подозрения, закономерно возникающие при использовании традиционных инвестиционных схем, где общение с жертвами осуществляется посредством колл-центров, расположенных в иностранных

---

[277] *Wang, F.* Persuasive schemes for financial exploitation in online romance scam: an Anatomy on Sha Zhu pan (杀猪盘) in China / F. Wang, X. Zhou // Vict Offenders. – 2023. – Vol. 18(5). – P. 915–942.

[278] *Sun, Z.* An analysis on the characteristics of «Pig-Butchering Scam» and anti-fraud strategy / Z. Sun, L. Yu // Journal of Jiangsu Police Institute. – 2022. – Vol. 2. – P. 86–92.

[279] *Xie, Z.* «Why did I fall for it?» Exploring internet fraud susceptibility in the pig butchering scam / Z. Xie, Z. Duan // Secur J. – 2025. – Vol. 38, 9. – DOI: https://doi.org/10.1057/s41284-024-00457-x

юрисдикциях[280]. Дополнительно применяются методы убеждения, разработанные опытными психологами и маркетологами, основанные на принципах симпатии и социального доказательства.

Каналы связи, используемые преступником для установления контакта с жертвой, являются неотъемлемой частью структуры преступного деяния. Они представляют собой не только средства коммуникации, но и инструменты, позволяющие злоумышленнику: изучать уязвимые места потенциальных жертв, выявлять их интересы и финансовые возможности; входить в доверие к жертве, используя психологические приёмы и манипуляции[281]; поддерживать связь на различных этапах подготовки и совершения преступления, отдавать распоряжения и взаимодействовать с соучастниками; использовать анонимные каналы связи, затрудняющие отслеживание их деятельности[282].

В своем исследовании профессор Квинслендского технологического университета К. Кросс подчеркивает следующее: «Установление доверительных отношений, основанных на «романтизме», – это преднамеренная тактика, используемая преступниками, которая позволяет им применять целый ряд методов психологического влияния для установления власти и контроля над жертвами и получения/поддержания выполнения любых финансовых запросов»[283].

Такие преступления, как правило, нацелены на все демографические группы, однако больше всего случаев фиксируется, где жертвами становятся люди среднего и пожилого возраста. Например, в Австралии наибольшие потери от романтического мошенничества приходятся на женщин старше 45 лет. Это во

---

[280] United Nations Human Rights. Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response. – 2023 // URL: https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf (дата обращения: 14.03.2025).

[281] *Ордоков, М. Х.* Совершение мошеннических действий в сети интернет / М. Х. Ордоков // Право и управление. – 2024. – № 6. – С. 330-333.

[282] *Мосин, И. В.* Детерминанты преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий / И. В. Мосин // Вестник Уральского юридического института МВД России. – 2024. – № 2(42). – С. 79-84.

[283] *Cross, C.* Romance baiting, cryptorom and ‘pig butchering’: an evolutionary step in romance fraud // Current Issues in Criminal Justice. – 2024. – Vol. 36. – No. 3. – P. 334-346.

многом объясняется тем, что пожилые люди ищут новых отношений, поскольку предыдущий брак распался, а дети выросли и стали жить самостоятельно. Однако переход к сочетанию криптовалютных инвестиционных схем с мошенничеством в сфере романтических отношений привел к значительному изменению демографической структуры жертв. В новой категории «романтических приманок» жертвами чаще становятся люди более молодого возраста по сравнению с традиционным романтическим мошенничеством.

В Китае наибольший ущерб в результате комбинированного мошенничества был нанесен потерпевшим в возрасте 25-34 лет. Многим жертвам сложно осознать реальность своего положения и степень обмана, которому они подверглись. Переход преступников к стратегии получения финансового вознаграждения за счет того, что жертва воспринимает как инвестиции, еще больше снижает вероятность понимания обмана[284].

1.8. *Криптоджекинг.* Данный вид преступления, совершаемого в отношении криптовалют, представляет собой скрытое внедрение вредоносного кода на устройство жертвы с целью эксплуатации его вычислительных ресурсов для добычи Биткоина, как правило, без ведома и согласия пользователя. В отличие от традиционных атак программ-вымогателей, криптоджекинг не блокирует доступ к данным или системе, а скрытно использует ресурсы процессора и графического адаптера для майнинга[285].

Существуют два основных метода криптоджекинга. Первый основан на прямом доступе к вычислительным устройствам, например, к собственному оборудованию злоумышленника или к технике третьих лиц (как в случае с физическим доступом к компьютеру «соседа»). Для этого способа имеет ключевое значение наличие достаточных мощностей, способных обеспечить

---

[284] *Дамирчиев, Э. И.* Некоторые вопросы противодействия дистанционным мошенничествам в Китае / Э. И. Дамирчиев, В.Ф. Васюков // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 2 (99). – С. 161-166.

[285] *Kshetri, N.* CryptoRAN: a review on cryptojacking and ransomware attacks wrt banking industry - threats, challenges, & problems / N. Kshetri, M.M. Rahman, S.A. Sayeed, I. Sultana – URL: https://www.researchgate.net/publication/376045308_cryptoRAN_A_review_on_cryptojacking_and_ransomware_attacks_wrt_banking_industry_-threats_challenges_problems (дата обращения: 14.03.2025).

рентабельность майнинга[286]. Второй метод предполагает создание ботнет-сетей, что технически сложнее, но эффективнее. Злоумышленники внедряют майнер-вирусы, которые незаметно используют ресурсы зараженных устройств. Если нагрузка на систему не превышает 30–50% от её возможностей, это обычно приводит лишь к замедлению работы, что само по себе не подпадает под уголовно наказуемые действия в соответствии с УК РФ[287]. Однако создание и распространение таких вредоносных программ квалифицируется по ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ. Это связано с тем, что майнер-вирусы модифицируют данные без согласия пользователя, нарушая целостность систем, что уголовно наказуемо. Таким образом, ключевым критерием уголовной ответственности становится не факт использования мощностей, а применение вредоносного кода для достижения этих целей[288].

Криптоджекинг, на первый взгляд не предполагающий прямого вымогательства, оказывает воздействие на снижение производительности устройств, перегрев аппаратных компонентов, что приводит к увеличению потребления электроэнергии и, как следствие, сокращению срока службы оборудования. Данный процесс, протекающий в скрытом режиме, не только снижает эффективность использования вычислительных ресурсов, но и создает предпосылки для других форм киберпреступности.

Таким образом, жертвы криптоджекинга несут прямые финансовые потери, выражающиеся в увеличении счетов за электроэнергию, необходимости ремонта или замены оборудования, а также в вероятном ущербе, обусловленном хищением данных или прерыванием деятельности юридического лица.

---

[286] *Lachtar, N.* A cross-stack approach towards defending against cryptojacking / N. Lachtar, A.A. Elkhail, A. Bacha, H. Malik // IEEE Computer Architecture Letters. – 2020. – Vol. 19(2). – P. 126-129.

[287] *Перов, В.А*. Способы совершения, выявления и особенности квалификации преступлений, совершаемых с использованием отдельных видов криптовалют (на примере криптовалюты Zcash) / В.А. Перов // Российский следователь. – 2024. – № 9. – С. 51–54.

[288] Постановление Яковлевского районного суда (Белгородская область) от 4 июня 2019 г. по делу № 1-85/2019 // СПС «КоонсультантПлюс» (дата обращения: 14.03.2025).

2. Преступления, совершаемые с использованием криптовалюты. В эту группу преступлений целесообразно включать категорию противоправных действий, в которых цифровые активы выступают не как непосредственный объект посягательства, а как инструмент, средство или механизм для совершения, сокрытия или финансирования иных преступных деяний.

В отличие от криптопреступлений, непосредственно направленных на хищение криптовалюты, в рассматриваемом случае акцент переносится на *вторичное использование* цифровых активов. К таким преступлениям относятся, например, финансирование терроризма, торговля наркотиками, легализация (отмывание) доходов, полученных преступным путем, и уклонение от уплаты налогов. Данная группа преступлений привлекла пристальное внимание исследователей[289], поскольку с появлением криптовалют традиционные виды преступной деятельности были оперативно трансформированы и интегрированы в новые схемы, основанные на технологиях блокчейна, с целью повышения их эффективности и анонимности.

2.1. Легализация (отмывание) доходов, полученных преступным путем. Легализация (отмывание) доходов, полученных преступным путем[290], является

---

[289] *Волеводз, А. Г.* К вопросу об учете потребностей противодействия отмыванию денег и финансированию терроризма при формировании правовых основ оборота криптовалюты в Российской Федерации / А. Г. Волеводз // Правовое поле современной экономики. – 2016. – № 3. – С. 135-145; *Ализаде, В. А.* Судебная практика применения ст. 174¹ УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты / В. А. Ализаде, А. Г. Волеводз // Наркоконтроль. – 2017. – № 4. – С. 8-14; *Волеводз, А. Г.* Особенности криптовалюты в системе денежных инструментов как определяющие факторы правовой регламентации ее оборота / А. Г. Волеводз, В. А. Кутырин // Электронная валюта в свете современных правовых и экономических вызовов : сборник материалов Международной научно-практической конференции, Москва, 2 июня 2016 г. – Москва: Издательство «Юрлитинформ», 2016. – С. 292-308; *Ализаде, В. А.* Неприменение ст. 174.1 Уголовного кодекса РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов / В. А. Ализаде, А. Г. Волеводз // Наркоконтроль. – 2018. – № 1. – С. 5-13; *Волеводз, А. Г.* Оценка криптовалюты как предмета преступления, предусмотренного ст. 174.1 УК РФ / А. Г. Волеводз // Уголовное право: стратегия развития в XXI веке : Материалы XV Международной научно-практической конференции, Москва, 25–26 января 2018 г. – Москва: РГ-Пресс, 2018. – С. 597-603.

[290] В соответствии со ст. 3 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (Собрание законодательства Российской Федерации, 2001, №33,

серьезной проблемой, особенно в контексте развития и распространения криптовалют. Анонимность и децентрализованный характер криптовалютных транзакций создают благоприятную среду для сокрытия преступных доходов и их интеграции в легальную экономику. В связи с этим понимание механизмов и этапов отмывания денег с использованием криптовалюты приобретает особую актуальность для правоохранительных органов и финансовых институтов[291].

Злоумышленники постоянно совершенствуют свои методы, используя различные комбинации технологий и финансовых инструментов для обхода существующих мер контроля. Однако в основе большинства схем отмывания денег лежит общая логика, включающая несколько последовательных этапов, направленных на сокрытие истинного происхождения средств и придание им видимости законности. Традиционно выделяют три основных этапа отмывания, каждый из которых характеризуется специфическими методами и задачами.

На этапе «размещения» происходит первичное внедрение «грязных» активов в экономическую систему. Часто это реализуется через конвертацию фиатных валют в криптовалюты, использование криптовалютных банкоматов с минимальными требованиями к идентификации пользователей (KYC) либо внесение крупных сумм на счета подставных лиц. Этот этап является наиболее уязвимым для обнаружения, поскольку предполагает прямое взаимодействие с регулируемыми финансовыми институтами. Основная цель – рассредоточение средств и минимизация прямой связи с источником незаконной деятельности.

Специфика преступной деятельности на данном этапе предполагает осуществление большого количества последовательных переводов денежных средств между различными криптовалютными кошельками и торговыми платформами, расположенными в разных юрисдикциях. Подобная

ст. 3418; 2021, № 1, ст. 18; 2024, № 33, ст. 4971) легализацией (отмыванием) доходов, полученных преступным путем является деятельность по приданию правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления.

[291] *Волеводз, А. Г.* Розыск, арест и обеспечение конфискации за рубежом денежных средств и имущества, нажитых преступным путем (вопросы организации и методики) / А.Г. Волеводз // Российский следователь. – 1999. – №2. – С.40-50.

противоправная тактика позволяет затруднить отслеживание первоначального источника средств и запутать финансовые потоки. Например, лицо может последовательно переводить средства между кошельками, зарегистрированными на подставных лиц на различных биржах в странах с лояльным регулированием криптовалют, таких как, например, некоторые страны Карибского бассейна[292].

На втором этапе – «расслоения» [293] – осуществляется деятельность, направленная на разрыв связей между активами и их преступным происхождением. Методы, используемые на данном этапе, включают в себя так называемое «веерное распыление», многократные переводы средств между множеством криптовалютных кошельков[294], часто расположенных в различных юрисдикциях, использование миксеров и приватных криптовалют (чаще всего – Monero и Zcash[295]) для маскировки транзакций, а также сложные схемы обмена между различными цифровыми активами[296].

---

[292] К таким странам относятся, например, Сент-Винсент и Гренадины, Пуэрто-Рико (юрисдикция США), Виргинские острова (Британские и Американские). Crypto Assets and CBDCs in Latin America and the Caribbean: Opportunities and Risks. – URL: https://www.researchgate.net/publication/368869923_Crypto_Assets_and_CBDCs_in_Latin_America_and_the_Caribbean_Opportunities_and_Risks [accessed Mar 16 2025].

[293] Термин, используемый экспертами ФАТФ для обозначения большого количества криптовалютных кошельков, зарегистрированных на подставных лиц. Легализация (отмывание) преступных доходов от киберпреступлений, а также финансирование терроризма за счет указанной преступной деятельности, в том числе с использованием электронных денег или виртуальных активов и инфраструктуры их провайдеров // Типологический проект ЕАГ. – 2022. – URL: https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_rus.pdf (дата обращения: 14.03.2025).

[294] В отчете Федерального управления полиции Швейцарии используется термин «Peel Chains» (иногда также упоминаются как «peeling chains» или «layering»). В контексте криптопреступлений этот термин используется для обозначения метода, благодаря которому криптоактивы последовательно перемещаются через множество транзакций между разными кошельками, чтобы затруднить отслеживание их происхождения. Суть в том, чтобы «расслоить» транзакции, как очистку луковицы (отсюда и название «peel», что означает «очищать»). Каждая транзакция – это новый «слой», усложняющий задачу отслеживания исходного источника средств. National Risk Assessment (NRA). Risk of money laundering and the financing of terrorism through crypto assets. – 2024. – URL: https://www.fedpol.admin.ch/fedpol/en/home/aktuell/mm.msg-id-100215.html (дата обращения: 14.03.2025).

[295] Необходимо отметить, что криптовалюта Zcash очень похожа на Monero. Ее предпочитают те, кто не хочет давать доступ к своим данным третьим лицам. Zcash реализует шифрование zk-SNARK, шифрующее содержимое защищенных транзакций, т.е. скрывает все транзакции пользователей. Транзакции Zcash зашифрованы, а адреса пользователей, а также сумма их транзакции являются конфиденциальными. См.: *Перов, В.А.* Способы совершения, выявления и особенности квалификации преступлений, совершаемых с использованием отдельных видов

Завершающий этап процесса легализации под названием «интеграция» предполагает соединение «отмытых» активов в легальную экономическую систему. Это достигается путем использования активов для приобретения материальных и нематериальных благ компании, зарегистрированных в юрисдикциях с льготным налогообложением. Главной целью данного этапа является создание видимости законного происхождения средств и их вовлечение в легальный экономический оборот[297].

Анализ специализированной литературы[298], отчётов ФАТФ, следственной и судебной практики позволил выявить *наиболее распространённые схемы легализации доходов, полученных преступным путём*, с использованием технологий децентрализованных финансов.

1. Схема использования децентрализованных «межсетевых мостов» (с англ. – «Cross-Chain Bridges»): децентрализованные межсетевые мосты, такие как RenBridge и Multichain, обеспечивают передачу активов между различными блокчейн-сетями (например, Ethereum, Binance Smart Chain и Solana) без обязательной идентификации пользователя. Лицо, совершившее преступление, переводит криптоактивы, полученные незаконным путем, на адрес моста, получая взамен «обернутые» токены, функционирующие в целевой блокчейн-сети. Такие токены могут многократно перемещаться через другие мосты, обмениваться на децентрализованных биржах (DEX) или выводиться на

криптовалют (на примере криптовалюты Zcash) / В.А. Перов // Российский следователь. – 2024. – № 9. – С. 51–54.

[296] فـ تراضـ ية الـمـشـ فرة فـ ي جريـ مـ تي غـ سل الأموال وتـ مويـ ل الإرهاب // مجـ لة صـ قر, وفـ اء. دور الـ عملات الـ ا ٣٠٥١ .٦٤ .٤٢٠٢ .ية والـ قانوذ ية فـ قهـ ية الـ بحوث الـ ١٤٠٥-

[297] *Перов, В.А.* Квалификация преступлений, совершаемых с использованием криптовалюты : автореф. дис. … канд. юрид. наук / Перов Валерий Александрович. – Москва, 2023. – 25 с.

[298] *Гриненко, А. В.* Противодействие легализации (отмыванию) доходов, полученных преступным путем: уголовно-правовые, уголовно-процессуальные и криминалистические аспекты / А. В. Гриненко, А. В. Коляда, С. Н. Хорьяков; Московский государственный институт международных отношений (университет) министерства иностранных дел Российской Федерации. – Москва : Общество с ограниченной ответственностью "Проспект", 2022. – 184 с.; *Сидоренко, Э. Л.* Легализация преступных доходов с использованием DeFi: типовые схемы и индикаторы риска / Э. Л. Сидоренко // Russian Journal of Economics and Law. – 2023. – Т. 17, № 4. – С. 822-836; Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С. В. Иванцов, Э. Л. Сидоренко, Б. А. Спасенников [и др.] // Всероссийский криминологический журнал. – 2019. – Т. 13, № 1. – С. 85-93.

централизованные биржи (CEX) для конвертации в фиатную валюту. Распространенность этой схемы обусловливается отсутствием KYC/AML-проверок и сложностью отслеживания из-за фрагментации транзакций между сетями.

По обоснованному утверждению Э.Л. Сидоренко подозрительная деятельность пользователей в такой схеме выявляется благодаря многократному использованию нескольких мостов для одной транзакции и (или) переводы между криптовалютами с высоким уровнем конфиденциальности в короткий промежуток времени[299].

2. Схема с использованием конфиденциальной (приватной) криптовалюты. Как было уже неоднократно нами упомянуто, само по себе использование таких валют говорит о том, что фигурант, в отношении которого проводятся оперативно-розыскные мероприятия, пытается замаскировать источник получения средств. Ключевым индикатором противоправной деятельности в такой схеме выступает механизм «цикличной конвертации», сущность которого заключается в частых переходах между прозрачными и приватными блокчейнами, сопровождающихся резкими изменениями объёмов транзакций[300]. Например, около 30% всех активов, поступающих с даркнет-магазинов и конвертируемых в криптовалюту Monero, практически сразу перенаправляются в стейблкоины, и уже только после этого – в фиатную валюту.

Пресечь подобные схемы практически невозможно, так как децентрализованная природа конфиденциальных валют исключает возможность прямого воздействия на разработчиков протоколов. Хотя ФАТФ в 2021 г. рекомендовала распространить «Правило путешествия» на все ПУВА, включая те, что работают с приватными активами, реализация этой нормы сталкивается с техническими ограничениями, например, с невозможностью предоставить полные данные о бенефициарах для транзакций в Zcash с активированным

---

[299] *Сидоренко, Э. Л.* Defi-преступность: состояние, тенденции и криминологические модели / Э. Л. Сидоренко // Russian Journal of Economics and Law. – 2023. – Т. 17, № 2. – С. 327-341.

[300] Приговор Шуйского городского суда (Ивановская область) от 7 декабря 2023 г. по делу № 1-60/2023 // СПС «КонсультантПлюс» (дата обращения: 14.03.20215).

режимом «shielded addresses». В результате даже санкционные меры, подобные блокировке миксера Tornado Cash Министерством финансов США в 2022 г., дают ограниченный эффект, поскольку злоумышленники быстро адаптируются, переключаясь на альтернативные сервисы или модифицируя алгоритмы смешивания.

3. Схема с использованием первичного размещения монет (ICO). Данная схема представляет собой механизм привлечения инвестиций посредством выпуска токенов. Лица, совершающие преступления, создают фиктивные проекты, приобретают токены на незаконные средства, а затем «обналичивают» их через децентрализованные или централизованные биржи. Для этой схемы характерна гибридная модель, сочетающая элементы краудфандинга и венчурного инвестирования, а также отсутствие предварительных проверок, что в целом создает благоприятную среду для мошеннических действий.

На отмывание преступных доходов через механизмы первичного предложения монет (ICO) могут указывать следующие закономерности. Во-первых, аномальная активность инвестора на децентрализованных биржах, выражающаяся в попытках массовой продажи вновь выпущенных токенов на стейблкоины или высоколиквидные криптоактивы без очевидной экономической логики, например, в обход рыночных трендов или фундаментальных показателей проекта. Во-вторых, отсутствие временно´го лага между покупкой токенов и их последующей конвертацией, что противоречит стандартным инвестиционным стратегиям, ориентированным на долгосрочную доходность, и свидетельствует о попытке оперативного вывода средств. В-третьих, структурная непрозрачность ICO-проекта, отсутствие надлежащих процедур KYC/AML, сокрытие информации об учредителях, юрисдикции регистрации и юридической структуре, что создает условия для псевдоанонимности транзакций. В-четвертых, игнорирование регуляторных требований ключевых юрисдикций — например, отсутствие явных ограничений на участие резидентов США или ЕС, где действуют строгие правила для ценных бумаг и виртуальных активов, что позволяет предположить умышленное избегание контроля.

Наконец, отсутствие регистрации проекта в качестве провайдера финансовых услуг (ПУВА, брокера или эмитента) в странах, где такая регистрация обязательна, прямо нарушает принципы риск-ориентированного подхода, закрепленные в рекомендациях ФАТФ. Совокупность этих факторов формирует «красные флаги», указывающие на использование ICO в качестве инструмента интеграции криминальных активов в легальный финансовый оборот.

4. Легализация преступных доходов посредством внутриигровой валюты и невзаимозаменяемых токенов NFT. Схема заключается в приобретении таких активов за криптовалюту, имеющую сомнительное происхождение, с последующей перепродажей этих активов на P2P-платформах или специализированных торговых площадках. Такой процесс позволяет замаскировать происхождение нелегальных средств, интегрируя их в легитимный финансовый оборот.

Приобретение редких или востребованных игровых активов и невзаимозаменяемых токенов по ценам, значительно превышающим их объективную рыночную стоимость, может выступать признаком намерения оперативно конвертировать криптовалютные активы в активы, которые могут быть реализованы за денежные средства, не имеющие признаков незаконного происхождения, без учета экономической целесообразности осуществляемой операции[301].

Кроме того, частые и значительные по объему переводы активов между игровыми аккаунтами, особенно в случаях, когда данные аккаунты связаны с анонимными криптовалютными кошельками, могут указывать на попытки сокрытия путей движения денежных средств и затруднения идентификации конечного бенефициара[302].

---

[301] Приговор Ленинского районного суда г. Оренбурга от 09.07.2019 по делу № 1-346/2019 // СПС «КонсультантПлюс» (дата обращений: 14.03.2025).

[302] *Золин, И. Ю.* Легализация (отмывание) наркодоходов: использование цифровой валюты / И. Ю. Золин, С. И. Земцова // Научный компонент. – 2023. – № 4(20). – С. 5-14.

В настоящее время распространены гибридные модели легитимизации активов. Например, фиктивные ICO имитируют механизмы краудфандинга и венчурного финансирования, а игровые токены маскируют криминальные потоки под легальную торговлю цифровыми активами. Подобные схемы используют доверие пользователей к инновационным финансовым инструментам, что соответствует концепции «криптографической театральности» («crypto performativity»).

В большинстве случаев схемы опираются на системные регуляторные лакуны. Децентрализованные платформы не подпадают под традиционные определения финансовых институтов, что исключает применение стандартов ФАТФ к их операторам. Более того, юрисдикционная рассредоточенность участников (разработчики смарт-контрактов, валидаторы, поставщики ликвидности) создает правовую неопределенность в вопросах ответственности, что соответствует выводам А.Г. Волеводза о «регуляторной несостоятельности» (regulatory incapacity) в отношении DeFi[303].

Анализ последних отчетов международных организаций свидетельствует о том, что легализация преступных доходов, полученных от незаконной деятельности с использованием криптовалют, приобрела мировые масштабы[304]. Успех теневой индустрии обусловил разработку сложных методов обработки и отмывания крупных сумм, полученных в результате незаконных операций и преступной деятельности. Это привело к повышению спроса на специализированные сервисы по отмыванию денежных средств, которые стали

---

[303] *Волеводз, А. Г.* Криптовалюта и цифровые финансовые активы как предмет и способ преступного посягательства / А. Г. Волеводз // Цифровое право : Учебник. – Москва : ООО Издательский дом "Юрлитинформ", 2024. – С. 589-599.

[304] Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape // United Nations Office on Drugs and Crime (UNODC). – Southeast Asia and the Pacific. – 2024 // https://humantraffickingsearch.org/resource/transnational-organized-crime-and-the-convergence-of-cyber-enabled-fraud-underground-banking-and-technological-innovation-in-southeast-asia-a-shifting-threat-landscape/ (дата обращения: 30.03.2025).

активно использоваться транснациональными преступными организациями Юго-Восточной Азии[305].

Согласно оценкам УНП ООН, масштабы незаконной деятельности в данном регионе увеличиваются угрожающе быстрыми темпами. Начиная с 2021 г., в районе бассейна реки Меконг, в частности, на территории стран «Золотого треугольника»[306] (Мьянмы, Камбоджи и Лаоса[307]), наблюдается строительство крупных бизнес-центров, в которых содержатся по несколько тысяч человек (в большинстве случаев – принудительно), занятых осуществлением незаконной деятельности с использованием компьютерных устройств и сети Интернет. Эта деятельность включает в себя дистанционное мошенничество, организацию и проведение онлайн-гемблинга[308], кибершпионаж, а также торговлю многими запрещенными товарами.

Методическое и техническое обеспечение[309] деятельности «сотрудников» таких центров осуществляется специалистами в различных областях, включая психологию, информационную безопасность, юриспруденцию и

---

[305] Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security // https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security (дата обращения: 30.03.2025).

[306] Термином «Золотой треугольник» принято обозначать регион в Юго-Восточной Азии, известный как один из крупнейших производителей опиума в мире.

[307] Полное наименование: Республика Союз Мьянма, Королевство Камбоджа, Лаосская Народно-Демократическая Республика.

[308] *«Онлайн-гемблинг»* – мероприятия по организации игровой деятельности в режиме реального времени, где платежными средствами выступают криптовалюты. Постановление № 54-11 Межпарламентской Ассамблеи государств - участников СНГ «О Глоссарии терминов, используемых органами внутренних дел (полицией) государств - участников Содружества Независимых Государств, по вопросам противодействия преступлениям, совершаемым посредством блокчейн-технологий и криптовалют» (Принято в г. Самарканде 28.10.2022) // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[309] Следует отметить, что в техническое оснащение криминальных центров вкладываются значительные средства. Так, в апреле 2024 г. полиция г. Чианграя (Таиланд) провела операцию, в ходе которой было изъято значительное количество высокотехнологичного оборудования, перевозимого из Мьянмы через Таиланд в Особую экономическую зону Лаоса. Среди изъятого оборудования были обнаружены 4998 SIM-карт британских операторов, десять спутниковых терминалов Starlink, а также различные дебетовые карты, банковские карты и иные финансовые документы, связанные с крупными суммами, полученными в результате мошеннических операций и хранившимися на банковских счетах, использовавшихся для легализации денежных средств. Taiwan Police Department PoC. 台灣警政署165防騙網111/7/18-111/7/24民眾通報假投資(博弈)詐騙網站 // Public Notice. – URL: https://165.npa.gov.tw/lineId (дата обращения: 30.03.2025).

инвестирование, что свидетельствует о высокой степени организации и профессионализации преступной деятельности. Руководящим звеном криминальных бизнес-центров был разработан комплекс механизмов для отмывания похищенных средств, ключевую роль в котором играют стейблкоины (USDT) – криптовалюты, «привязанные» к стоимости доллара США. Так как стейблкоины обеспечивают относительную стабильность стоимости криптовкладов, они получили большую популярность среди фигурантов, стремящихся сохранить и переместить похищенные средства с минимальным риском их волатильности[310].

В странах Юго-Восточной Азии широкое распространение получили схемы отмывания денег с помощью множества подставных лиц, так называемых «караванов муравьев», которыми «по цепочке» осуществляются переводы похищенных средств через криптовалютные биржи. Участники таких групп, завербованные с помощью социальных сетей (чаще всего – нетрудоустроенные молодые люди), предоставляют свои криптокошельки для осуществления операций по «прокрутке» – сбору и переводу денежных средств неизвестного происхождения – в обмен на комиссионное вознаграждение. Лица, находящиеся в начале «цепочки» (с наибольшим риском обнаружения), получают комиссию 20-40%. Эти схемы широко используются для финансирования различной преступной деятельности, в том числе торговли наркотиками, кибермошенничества и нелегальных азартных игр[311].

---

[310] Правоохранительные органы и органы финансовой разведки в Восточной и Юго-Восточной Азии также сообщают, что USDT является одной из самых популярных криптовалют, используемых организованными преступными группами, о чем свидетельствует рост числа случаев кибермошенничества, отмывания денег и деятельности, связанной с подпольными банковскими операциями. Official announcement issued by the Wenzhou People's Procuratorate, 29 November 2021 – URL: https:// www.12309. gov.cn/12309/gj/zj/wzs/zdajxx/202111/.shtml; Association of Certified Anti-Money Laundering Specialists, 2023 // https://www.moneylaundering.com/news/ cryptocurrency-research-firms-vastly-underestimate-illicitpayments-critics-claim (дата обращения: 30.03.2025).

[311] Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat // United Nations Office on Drugs and Crime (UNODC). – 2024 – URL: https://www.unodc.org/roseap/uploads/documents/Publications/2024/ Casino_Underground_Banking_Report_2024.pdf (дата обращения: 30.03.2025).

2.2. Незаконный оборот наркотиков. Он характеризуется массовым характером и возможностью бесконтактного взаимодействия между участниками, традиционно является одним из основных предикатных преступлений по отношению к легализации (отмыванию) преступных доходов. С учетом активного использования криптовалют в данной сфере эта тенденция приобретает особую актуальность, поскольку цифровые активы создают наиболее благоприятные условия для выстраивания схем оплаты наркотиков, которые чаще всего распространяются посредством заранее сделанных тайников или, как их еще часто называют, «закладок»[312].

Система «закладок» в контексте незаконного оборота наркотиков представляет собой логистическую схему, основанную на скрытом размещении товара и анонимных расчетах. Она функционирует в несколько последовательных этапов, каждый из которых использует преимущества современных технологий для обеспечения конфиденциальности и минимизации рисков для фигурантов[313].

Первый этап предполагает согласование условий незаконной сделки между «оператором» и покупателем[314]. Общение, как правило, происходит через зашифрованные мессенджеры, в чате которых обсуждается объем, цена и ассортимент наркотических веществ, а также определяются все ключевые параметры оплаты[315]. На втором этапе покупатель переводит заранее

---

[312] Приговор Кировского районного суда г. Саратова от 10 марта 2021 г. по делу № 1-274/2020; Приговор Ханты-Мансийского районного суда № 1-263/2020 от 24 июля 2020 г. по делу № 1-263/2020 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[313] *Сидоренко, Э. Л.* Даркнет и наркопреступность: криминологические вызовы и актуальные уголовно-правовые вопросы / Э. Л. Сидоренко // Наркоконтроль. – 2023. – № 2. – С. 9-15.

[314] Приговор Московского областного суда № 2-106/2024 от 26 августа 2024 г. по делу № 2-106/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[315] Приговор Промышленного районного суда г. Курска № 1-121/2024 от 20 августа 2024 г. по делу № 1-121/2024; приговор Череповецкого городского суда (Вологодская область) от 17 июля 2024 г. по делу № 1-637/2024; приговор Ивдельского городского суда (Свердловская область) от 16 июля 2024 г. по делу № 1-60/2024; Приговор Свердловского районного суда г. Костромы от 15 июля 2024 г. по делу № 1-166/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

оговоренную сумму в криптовалюте на кошелек «оператора»[316]. После подтверждения успешного перевода криптовалюты продавец сообщает покупателю детальную информацию о месте, где спрятаны наркотические вещества[317]. Эта информация, как правило, включает в себя координаты GPS, словесное описание места, а также фотографии со специализированными метками[318]. Завершающий этап заключается в получении товара покупателем. Покупатель прибывает в указанное место, находит «закладку» и забирает наркотики, тем самым завершая незаконную сделку[319].

При этом отсутствие непосредственного контакта между продавцом и покупателем, а также использование анонимных способов оплаты минимизируют риски для обеих сторон и затрудняют идентификацию правоохранительными органами участников незаконной деятельности.

Активное использование интернет-инструментов, методов и технологий, направленных на дистанционное совершение наркопреступлений, способствует формированию специализированных онлайн-платформ (таких как форумы, интернет-магазины и торговые площадки[320]), функционирующих

---

[316] Приговор Благовещенского городского суда (Амурская область) от 2 февраля 2024 г. по делу № 1-1371/2023; приговор Петрозаводского городского суда (Республика Карелия) № 1-865/2024 от 29 июля 2024 г. по делу № 1-865/2024; приговор Чебоксарского районного суда (Чувашская Республика) от 10 июля 2024 г. по делу № 1-85/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[317] Приговор Новокузнецкого районного суда № 1-95/2023 от 28 ноября 2023 г. по делу № 1-95/2023; Приговор Абаканского городского суда (Республика Хакасия) № 1-203/2024 от 5 июля 2024 г. по делу № 1-203/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[318] Приговор Дзержинского районного суда г. Волгограда № 1-643/2023 от 28 ноября 2023 г. по делу № 1-643/2023; Приговор Новотроицкого городского суда (Оренбургская область) от 9 июля 2024 г. по делу № 1-228/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[319] Приговор Химкинского городского суда (Московская область)№ 1-738/2023 от 9 ноября 2023 г. по делу № 1-738/2023; приговор Московского районного суда г. Твери (Тверская область) от 6 февраля 2024 г. по делу № 1-337/2023; приговор Ленинского районного суда г. Уфы (Республика Башкортостан) от 5 июля 2024 г. по делу № 1-135/2024 // СМС «КонсультантПлюс» (дата обращения: 15.03.2025).

[320] Следует отметить, что на таких ресурсах, функционирующих по аналогии с обычными интернет-магазинами, реализована возможность фильтрации товаров по категориям, таким как оружие, рецептурные препараты и наркотики. Пользователи могут искать товары по заданным ценовым диапазонам, а также сортировать продавцов по странам доставки. Помимо рейтингов на платформах отображается информация о количестве транзакций, проведённых продавцом, а также о количестве покупок, совершённых покупателем. Это позволяет участникам рынка оценивать надёжность друг друга. Некоторые продавцы предлагают компенсацию в случае

преимущественно в псевдо-доменной зоне «.onion», предназначенной для обеспечения доступа к адресам в сети Tor.

В качестве примеров таких специализированных платформ можно привести Mega, Solaris, BlackSprut, ориентированные преимущественно на предоставление услуг по бесконтактному сбыту различных наркотических средств. География деятельности данных интернет-площадок, помимо России, охватывает и такие страны, как Украина, Беларусь, Казахстан, другие страны СНГ, а также некоторые другие страны Европы и Азии.

Финансовое обеспечение деятельности подобных платформ, включая оплату услуг и легализацию доходов, полученных от незаконного оборота наркотиков, играет ключевую роль в их функционировании и осуществляется преимущественно с использованием цифровых валют и, в меньшей степени, электронных платежных систем[321].

В современной криминальной среде использование криптовалют стало одним из ключевых факторов, стимулирующих рост преступлений, связанных с незаконным оборотом наркотиков. Этот рост обусловлен не только увеличением бесконтактного сбыта и распространением наркосделок с использованием цифровых активов, но и относительной простотой последующей легализации (отмывания) доходов, полученных преступным путем, а также сложностью отслеживания финансовых потоков, связанных с данной деятельностью.

Подтверждением этой тенденции служат многочисленные примеры из следственной и судебной практики, которые свидетельствуют о широком распространении криптовалютных транзакций в схемах незаконного оборота

потери отправления в процессе доставки, размер которой может зависеть от количества отзывов, оставленных покупателем. Представленные меры, направленные на повышение уровня доверия, способствуют привлечению клиентов и позволяют продавцам выделиться среди конкурентов. Примечательно, что участники этих платформ стремятся создать образ серьезных и надежных партнеров.

[321] *Исаков, Р. В.* О противодействии легализации (отмыванию) наркодоходов с использованием финансовых активов (криптовалют) / Р. В. Исаков, Д. В. Теткин, А. М. Попов // Вестник Воронежского института МВД России. – 2021. – № 2. – С. 267-271.

наркотиков[322]. По справедливому утверждению М.М. Долгиевой применение инновационных технологий в незаконном обороте наркотических средств, анонимность криптовалют и потенциальная прибыль делают данную сферу особенно привлекательной для злоумышленников[323].

Криптовалюты, обладающие способностью обеспечивать трансграничные финансовые операции по конвертации больших сумм, стали ключевым инструментом торговли мексиканских наркокартелей. Причем механизмы цифровых перемещений значительно эволюционировали в сторону сотрудничества наркокартелей с китайскими подпольными финансовыми сетями, специализирующимися на транснациональном перемещении незаконных доходов посредством криптовалют.

Типичная схема предполагает конвертацию наличных средств, полученных от продажи наркотиков в США, в цифровые активы через китайских брокеров, с последующим их переводом или использованием для закупки прекурсорных химических веществ, важных для производства синтетических наркотиков (фентанил, метамфетамин). Так, в июне 2024 г. Министерство юстиции США предъявило обвинения сообщникам картеля «Синалоа» в Лос-Анджелесе за реализацию наркотиков на сумму свыше 50 млн долл. через китайские подпольные фирмы с использованием криптовалютных операций[324].

---

[322] Приговор Петропавловского-Камчатского городского суда № 1-272/2021 от 13 июля 2021 г. по делу № 1-272/2021; приговор Томского областного суда (Томская область) от 14 февраля 2024 г. по делу № 2-23/2023; приговор Кировского районного суда г. Ростова-на-Дону от 26 января 2024 г. по делу № 1-157/2023; приговор Королёвского городского суда (Московская область) от 16 января 2024 г. по делу № 1-46/2024; приговор Абаканский городской суд (Республика Хакасия) от 30 июля 2024 г. по делу № 1-257/2024; приговор Петропавловск-Камчатского городского суда (Камчатский край) от 18 июля 2024 г. по делу № 1-535/2024; приговор Щелковского городского суда (Московская область) от 16 июля 2024 г. по делу № 1-450/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[323] *Долгиева, М. М.* Криптовалютная наркоторговля в России и за рубежом / М.М. Долгиева // Вестник Воронежского института МВД России. - 2018. - № 4. - С. 177-182.

[324] Understanding the Use of Cryptocurrencies By Cartels // https://www.trmlabs.com/post/understanding-the-use-of-cryptocurrencies-by-cartels (дата обращения: 30.03.2025)

3. Финансирование терроризма[325]. Начиная как минимум с 2015 г. отмечаются случаи, когда экстремистские организации пытались использовать криптовалюты для организации краудфандинговых кампаний с целью финансирования своей деятельности.

В большинстве случаев подобные схемы были организованы группировками, действующими на Ближнем Востоке и придерживающимися радикальных идеологических взглядов. Однако незаконная деятельность, связанная с использованием криптовалют и финансированием терроризма, также наблюдается по всему миру. Как показывает изучение отчетов иностранных правоохранительных органов, криптовалюты создают террористическим организациям дополнительные возможности для расширения масштабов и повышения эффективности сбора средств на незаконную деятельность[326].

Криптоактивы могут быть использованы для оказания финансовой поддержки террористической деятельности. Финансирование терроризма с использованием виртуальных валют ассоциируется, в частности, с исламским фундаментализмом и обходом экономических санкций, введённых в отношении государств, не соблюдающих нормы и принципы функционирования финансового рынка, установленные западными либеральными демократиями. В кругах исламских фундаменталистов велись дискуссии о допустимости использования криптовалют с точки зрения норм шариата. В 2014 г. организация

---

[325] В соответствии со ст. 3 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (Собрание законодательства Российской Федерации, 2001, № 33, ст. 3418; 2021, № 1, ст. 18; 2024, № 33, ст. 4971) финансированием терроризма является предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки и совершения хотя бы одного из преступлений, предусмотренных статьями 205, 205.1, 205.2, 205.3, 205.4, 205.5, 206, 208, 211, 220, 221, 277, 278, 279, 360 и 361 УК РФ, либо для финансирования или иного материального обеспечения лица в целях совершения им хотя бы одного из указанных преступлений, либо для обеспечения организованной группы, незаконного вооруженного формирования или преступного сообщества (преступной организации), созданных или создаваемых для совершения хотя бы одного из указанных преступлений.

[326] *Brill, A.* Cryptocurrencies: the next generation of terroristfinancing? / A. Brill, L. Keene // Defense Against Terrorism Review. – 2014. – Vol. 6. – No. 1. – P. 7–30.

«Аль-Каида»[327] опубликовала в Интернете манифест под названием «Биткойн ва Садакат аль-Джихад», в котором пропагандировалось использование биткоина в качестве удобного средства для поддержки борьбы с «неверными» в обход западной банковской системы, ограничивающей пожертвования на «джихад»[328].

В манифесте содержались рекомендации по использованию криптовалютных транзакций по идеологическим и религиозным соображениям и приводилось описание технических преимуществ виртуальных валют, таких как устойчивость к подделке, анонимность отправителей и получателей, глобальный охват и сложность обнаружения платежей правоохранительными органами.

Авторы манифеста подчёркивали превосходство системы «Биткоин» над такими платёжными системами, как PayPal или eBay, которые характеризовались централизованным управлением. Целью разработчиков манифеста было создание полностью анонимной системы для осуществления пожертвований в биткоинах из США, Великобритании, Южной Африки, Ганы, Малайзии, Шри-Ланки и других стран мира в адрес DarkWallet, управляемый моджахедами[329].

В заключение авторы манифеста отметили, что, несмотря на наличие определённых этических вопросов, связанных с использованием биткоина, и его распространённость среди «неверных» для приобретения наркотических веществ, криптовалюты могут быть использованы для достижения широкого спектра целей, включая приобретение оружия и получение пожертвований в пользу моджахедов. Подобная позиция привела к появлению многочисленных страниц в социальных сетях, предназначенных для организации сбора криптовалют в поддержку исламских террористических организаций, действующих в разных странах. Сбор средств осуществляется не только

---

[327] Деятельность запрещена на территории Российской Федерации.

[328] *Opitek, P.* Selected aspects of crime involving virtual currencies / P. Opitek, A. Butor-Keler, K. Kanclerz // Terroryzm – studia, analizy, prewencja. – 2023. – P. 325–376.

[329] Przewłoka E., Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej (Eng. Methodology of basic actions carried out by a police officer and related to the crime of "theft" of virtual currency). – Bydgoszcz, 2023. – P. 14-18.

структурами, непосредственно связанными с преступными элементами, но и их сторонниками, проживающими на территории США и европейских государств.

Организация «Аль-Каида»[330] использовала форумы и чаты в открытом сегменте интернета с момента своего основания, однако после масштабных репрессий в 2000-х г.г. и ареста ряда сторонников джихадистского движения значительное количество платформ было перенесено в Даркнет. В настоящее время наиболее продвинутые джихадистские форумы обеспечивают защиту от мониторинга со стороны разведывательных служб с помощью криптографического шифрования и таких специализированных инструментов, как Sigaint или TorBox, а доступ к платформам осуществляется на основе верификации со стороны администраторов. В интернете активно функционируют форумы, связанные с радикальными движениями, в частности «Шумух аль-Ислам», объединяющий сторонников ИГИЛ[331] и «Аль-Каиды»[332].

В 2019 г. военное крыло организации ХАМАС (Бригады Изз ад-Дин аль-Кассам) разместило в социальных сетях и на своих официальных веб-сайтах (alqassam.net, alqassam.ps, qassam.ps) обращение с призывом делать пожертвования в биткоинах на финансирование «кампании террора». В то же время участники незаконных формирований изучали методы обеспечения кибербезопасности. Изначально «Бригады Изз ад-Дина аль-Кассама» [333] использовали единый адрес для сбора пожертвований в криптовалюте, размещённый на американской криптовалютной бирже, однако впоследствии разработали технологию генерации уникального адреса для каждого поступающего взноса с целью затруднить идентификацию источника происхождения и направления последующего движения денежных средств[334].

---

[330] Деятельность запрещена на территории Российской Федерации.
[331] Деятельность запрещена на территории Российской Федерации.
[332] *Irwin, A.* The use of crypto-currencies in funding violentjihad / A. Irwin, G. Milad // Journal of Money Laundering Control. – 2018. – Vol. 19, iss. 4. – P. 407–425.
[333] Деятельность запрещена на территории Российской Федерации.
[334] *Almaqableh, L.* An investigative study of links between terrorist attacks and cryptocurrency markets / L. Almaqableh, K. Reddy, V. Pereira, V. Ramiah, D. Wallace, J.F. Veron // Journal of Business Research. – 2022. – Vol. 147. – P. 177-188.

Внедрение террористическими структурами инновационных технологических решений свидетельствует об их адаптации к стратегиям, направленным на минимизацию потенциальных рисков и использование существующих технологических уязвимостей. Кибертеррористическая деятельность не ограничивается исключительно сбором денежных средств с помощью краудфандинговых платформ.

В начале 2021 г. медиаподразделение организации «Аль-Каида»[335] объявило о назначении вознаграждения в размере 1 биткоина (что на тот момент эквивалентно 60 000 долл. США) за убийство сотрудника правоохранительных органов в одной из стран западного мира. За два года до этого Брентон Таррант, совершивший террористический акт, связанный с нападением на мечети в Крайстчерче (Новая Зеландия), заявил, что получил средства для совершения преступления благодаря операциям с криптовалютами[336].

В то же время сторонник теории расового превосходства, совершивший нападение на синагогу в Германии, указывал на получение финансовой поддержки посредством биткоин-транзакций. Существуют многочисленные свидетельства того, что лица, совершившие теракты в Париже 13 ноября 2015 г., получали поддержку в виде криптовалютных переводов в период подготовки к совершению преступления. Деятельность террористических организаций в онлайн-среде была выявлена и детально проанализирована правоохранительными органами.

Также в 2021 г. была проведена масштабная международная кибероперация, направленная на пресечение деятельности виртуальной инфраструктуры «Бригад Изз ад-Дин аль-Кассама». Начиная с октября 2019 г., оперативные сотрудники, действовавшие под прикрытием, осуществляли переводы в биткоинах в пользу террористических организаций с целью выявления и установления связей между организациями, осуществляющими

---

[335] Деятельность запрещена на территории Российской Федерации.

[336] *Opiatek, P.* Cryptocurrencies in the aspects of police investigative activities / P. Opiatek // Przegląd Policyjny. – 2017. – № 2. – P. 138–158.

онлайн-сбор денежных средств для ХАМАС. Данные действия позволили идентифицировать лиц, поддерживающих данную организацию, проживающих на территории Соединенных Штатов Америки, а также продолжить отслеживание движения переведенных денежных средств. В ходе проведения операции было выявлено 64 уникальных канала связи (включая адреса электронной почты), что дало возможность установить соответствие между этими каналами и биткоин-кошельками жертвователей[337].

В рамках операции были установлены методы деятельности террористических организаций в сети Интернет, в том числе используемые ими способы вербовки сторонников, схемы финансирования, а также применяемые домены и элементы IT-инфраструктуры, функционирующие, в частности, на территории России, США, Канады, Германии и Саудовской Аравии[338].

В рамках проведенных 24 санкционированных федеральным судом обысков были изъяты криптовалютные активы, а также получены сведения из многочисленных онлайн-бирж и от поставщиков сетевых услуг, включая почтовые сервисы, VPN-провайдеры и платежные системы. В результате были конфискованы серверы, заблокированы многочисленные домены и почтовые ящики, связанные с осуществлением террористической деятельности. Привлечение к проведению кибероперации партнерских служб из различных стран мира позволило изъять терабайты данных, контролируемых террористами, идентифицировать сотни биткоин-кошельков, конфисковать криптовалютные активы на сумму, эквивалентную нескольким миллионам долларов США, а также ликвидировать интернет-ресурсы, предназначенные для приема пожертвований в биткоинах[339].

---

[337] *Almaqableh, L.* Is it possible to establish the link between drug busts and the cryptocurrency market? Yes, we can / L. Almaqableh, D. Wallace, V. Pereira, V. Ramiah, G. Wood, J.F. Veron, I. Moosa, A. Watson // International Journal of Information Management. – 2022. – DOI: 10.1016/j.ijinfomgt.2022.102488 (дата обращения: 30.03.2025).

[338] *Neumann, P.* Don’t follow the money: The problem with the war on terrorist financing / P. Neumann // Foreign Affairs. – 2017. – Vol. 96 (4). – P. 93-102.

[339] Opiatek, P. Cryptocurrencies in the aspects of police investigative activities / P. Opiatek // Przegląd Policyjny. – 2017. – № 2. – P. 138–158.

В ходе другого расследования, проведенного в 2020 г., были идентифицированы 24 криптовалютных счета, классифицированных как иностранные активы или источники финансирования организации «Аль-Каида»[340]. В результате проведения кибероперации, направленной на пресечение использования криптовалют для поддержки и финансирования террористической деятельности, было изъято 60 виртуальных кошельков, использовавшихся в преступных целях[341].

Радикально настроенные лица способны осуществлять относительно недорогие и несложные, но приводящие к значительным жертвам теракты с применением холодного и огнестрельного оружия, а также транспортных средств. Данная деятельность упрощается за счет использования онлайн-коммуникаций и криптовалютных переводов, совершаемых в скрытом режиме непосредственно на криптокошельки исполнителей, что минимизирует финансовый след.

Так, сотрудниками УФСБ России по Вологодской области был пресечен законспирированный канал финансирования международной террористической организации с использованием криптовалюты. В ходе проведения оперативно-розыскных мероприятий выявлена преступная деятельность жителя региона 1991 года рождения, ранее судимого за совершение преступлений, предусмотренных ч. 3 ст. 30 ч. 1 ст. 205^1 (приготовление к вовлечению лиц в террористическую деятельность), ч.1 ст. 205^2 (публичное оправдание терроризма) УК РФ, который после освобождения из мест лишения свободы установил контакты с участниками международной террористической организации «Исламское государство»[342]. Также было установлено, что мужчина, находясь в г. Вологде, создал и администрировал криптокошелек и закрытые сообщества в мессенджере Telegram, посредством которых осуществлял сбор денежных

[340] Деятельность запрещена на территории Российской Федерации.
[341] Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis // https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer (дата обращения: 30.03.2025).
[342] Деятельность запрещена на территории Российской Федерации.

средств для боевиков указанной организации. Кроме того, он проводил обучение участников террористической организации анонимной работе в сети Интернет, готовил и направлял им инструкции по соблюдению мер конспирации[343].

Между тем проблема использования криптовалют в экстремистской деятельности не ограничивается только террористическими организациями, но и затрагивает другие деструктивные объединения, представляющие угрозу для стабильности и безопасности демократических государств.

Вербовочная деятельность джихадистских формирований в онлайн-пространстве зачастую сопровождается обращениями к общественности с просьбой об оказании финансовой помощи террористическим элементам. Простота осуществления пожертвований и возможность перевода относительно небольших денежных сумм создают благоприятные условия для оказания существенной финансовой поддержки.

На основании изложенного выше стоит сделать ряд выводов следующего характера.

1. Классификация криптопреступлений, основанная на разграничении деяний, направленных на криптовалюты (как предмет посягательства) и деяний, использующих криптовалюты (как инструмент), обеспечивает структурирование знаний о преступной деятельности в цифровой среде, учитывая технологическую специфику и транснациональный характер подобных правонарушений. В частности, кибератаки на криптобиржи, эксплуатация уязвимостей смарт-контрактов и фишинговые атаки представляют собой основные способы хищения криптоактивов. Анализ международного опыта свидетельствует о подверженности даже платформ с высоким уровнем защиты от рисков, что обусловлено человеческим фактором, социальной инженерией и недостатками в программном коде.

---

[343] УФСБ России по Вологодской области пресечен законспирированный канал финансирования МТО ИГИЛ. Национальный антитеррористический комитет // https://nac.gov.ru/view/92305198-b769-40fc-a44d-1e282142e5fd (дата обращения: 12.03.2025).

2. Мошеннические схемы, адаптируясь к цифровой среде и используя доверие пользователей к инновационным технологиям, приобретают комбинированные формы, сочетающие методы психологического манипулирования с техническими средствами. Децентрализованные платформы и анонимные криптовалюты формируют системные риски для глобальной финансовой безопасности.

3. Деятельность организованных преступных сообществ, осуществляемая в различных юрисдикциях, обусловливает необходимость международного сотрудничества. Кроме того, злоумышленники активно внедряют технологии искусственного интеллекта для оптимизации фишинговых атак, анализа уязвимостей и прогнозирования поведения потенциальных жертв, что создает новые вызовы для правоохранительных органов и требует адекватного технологического ответа.

ГЛАВА II. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ АСПЕКТЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ОТНОШЕНИИ И С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

§ 1. Особенности проведения оперативно-розыскных мероприятий при раскрытии преступлений, совершаемых в отношении и с использованием криптовалюты

Современный этап трансформации политической, экономической и социальной сфер в Российской Федерации характеризуется тревожной тенденцией роста преступности в сфере информационных технологий, что представляет собой серьезный вызов для системы правоохранительных органов. Преступления, связанные с цифровыми активами, демонстрируют несостоятельность традиционных методов борьбы с преступностью перед лицом этой динамично развивающейся угрозы. Следовательно, возникает острая необходимость в разработке и внедрении новых алгоритмов, регламентирующих деятельность подразделений, уполномоченных осуществлять оперативно-розыскную деятельность.

В этой связи, как справедливо отмечает профессор А.Ю. Шумилов, совершенствования требует не только нормативно-правовой инструментарий оперативно-розыскной деятельности, но и тактические и стратегические методы противодействия преступности, которая приобретает все более организованный характер[344]. Развивая эту мысль, профессора С.И. Захарцев, И.Н. Кондрат и В.П. Сальников подчеркивают, что эволюция оперативно-

[344] *Шумилов, А. Ю.* Совершенствование законодательного регулирования оперативно-розыскной деятельности таможенных органов / А. Ю. Шумилов // Регулирование внешнеэкономической деятельности и эволюция таможенной политики России : Тезисы докладов международной научно-практической конференции (22-23 октября 1996 г.): в 2 частях, Москва, 22–23 октября 1996 г. / Российская таможенная академия; председатель редколлегии Н.М. Блинов. Том Часть 2. – Москва: Российская таможенная академия, 1996. – С. 34-37.

розыскных мероприятий обусловлена накоплением научных знаний и развитием технических средств[345]. Таким образом, появление новых средств коммуникации и технологий обусловливает необходимость разработки новых или совершенствования существующих оперативно-розыскных мероприятий[346].

Действительно, еще десять лет назад было сложно представить, что сотрудники оперативных (разведывательных) подразделений большинства стран будут озадачены вопросами отслеживания экономического фантома, популярность которого достигнет невиданных пределов. Однако цифровая реальность определила новые тенденции в развитии криминалистической науки с учетом потребности выявлять закономерности между следами и преступным событием, произошедшим в нематериальной сложноструктурированной системе блокчейна[347]. В данном контексте особую актуальность приобретает тезис профессора А.С. Подшибякина о том, что «не может успешно осуществляться противодействие преступности в условиях отстающего нормативного регулирования и криминалистического обеспечения оперативно-розыскной деятельности»[348].

Основываясь на сказанном, подчеркнем, что традиционная трактовка объектов оперативно-розыскной деятельности, включающая лиц, предметы, события и сведения, демонстрирует ограниченную применимость в контексте криптопреступлений. Высокая технологическая сложность актуализируют потребность в разработке инновационных методов выявления и всестороннего

---

[345] *Захарцев, С. И.* Оперативно-розыскные мероприятия: вопросы правового регулирования / С. И. Захарцев, И. Н. Кондрат, В. П. Сальников // Мониторинг правоприменения. – 2024. – № 3(52). – С. 54-60.

[346] *Зуев, С.В.* IT-следователь в цифровой среде уголовного судопроизводства / С.В. Зуев А.И. Зазулин // Правопорядок: история, теория, практика. – 2024. – № 2(41). – С. 48-54.

[347] Информационные технологии в уголовно-правовой сфере: монография / под ред. А.И. Бастрыкина, А.Н. Савенкова. — М.: ЮНИТИ-ДАНА, 2023. — 279 с.

[348] *Подшибякин, А. С.* Правовое и криминалистическое обеспечение оперативно-розыскной деятельности : Сборник составлен из статей, опубликованных профессором А.С. Подшибякиным в 1983-2010 годах в научных и в специальных изданиях / А. С. Подшибякин. – Москва, 2010. – 352 с.

изучения новых объектов, особенно в условиях дефицита исходной информации[349].

Существующее положение вещей во многом связано с переплетением нескольких технологий, позволяющих дистанционно совершать весь цикл преступной деятельности, которая успешно анонимизируется злоумышленниками. Такая деятельность имеет трансграничный характер, то есть ее осуществление происходит в двух или нескольких юрисдикциях.

Сложившиеся условия придают особое значение словам Ю.В. Астафьева: «Не бывает раскрытия без расследования, а расследования – без раскрытия. Невозможно раскрыть преступление без проведения надлежащих процессуальных процедур. В противном случае раскрытие будет лишено своей цели – борьбы с преступностью и восстановления нарушенных прав граждан. Вместе с тем процессуальные процедуры требуют в большинстве своем оперативного обеспечения, установления оперативным путем оснований проведения, а также оперативно-розыскной подготовки»[350].

Напомним, что изучение типовых способов совершения криптопреступлений, проведенное в первой главе настоящего исследования, позволило выделить две принципиально различные категории противоправных деяний: (1) деяния, направленные на криптовалюту как непосредственный предмет посягательства, и (2) деяния, в которых криптовалюта используются в качестве инструмента реализации противоправных целей. Данная классификация, основанная на операционно-функциональных критериях, является ключевым элементом предлагаемого алгоритма, поскольку обусловливает специфику применяемых ОРМ и следственных действий.

---

[349] Теория оперативно-розыскной деятельности : Краткие учебные курсы юридических наук / О. А. Вагин, К. К. Горяинов, А. В. Земскова [и др.]. – 5-е издание, переработанное. – Москва : Издательский Дом "Инфра-М", 2021. – 352 с.; Оперативно-розыскная деятельность : Научно-практический комментарий (постатейный) к Федеральному закону / А. И. Бастрыкин, В. М. Егоршин, С. И. Захарцев [и др.]. – Москва : Издательство "Юрлитинформ", 2020. – 280 с.

[350] *Астафьев, Ю.В.* Методологические основы соотношения оперативно-розыскной и доказательственной информации в расследовании преступлений // Вестник ВГУ. Серия Право. 2007. № 1. С. 284.

Представляется, что структура алгоритма расследования криптопреступлений должна учитывать не только общие этапы, присущие любому уголовному делу, но и специфические особенности, обусловленные характером преступления и используемых технологий. Переходя к детальному рассмотрению алгоритма, необходимо подчеркнуть, что он представляет собой не просто набор последовательных шагов, а гибкую систему, адаптируемую к конкретным обстоятельствам каждого расследуемого дела.

На начальном этапе раскрытия и расследования ключевую роль играет первичная проверка и оценка поступившей информации о действиях, имеющих криминальный характер. По *преступлениям первой категории* чаще всего основанием проведения проверочных мероприятий является заявления от граждан, а также от организаций, в отношении которых была реализована противоправная схема.

После получения заявления о произошедшем криптопреступлении, в ходе которого, как правило, был причинен значительный материальный ущерб, проводится *опрос* лица, пострадавшего от противоправного деяния. При проверке мошеннических схем в ходе опроса устанавливаются обстоятельства знакомства с предполагаемым злоумышленником, например, через социальные сети, мессенджеры или инвестиционные онлайн-платформы. Выявляется характер и содержание сообщений, предшествовавших совершению транзакций. Уточняются технические детали осуществления транзакций, включая тип используемых криптовалютных бирж, виды криптовалют, объемы транзакций, а также адреса кошельков отправителя и получателя. Кроме того, у опрашиваемого запрашивается документальное подтверждение факта совершения транзакций, например, скриншоты транзакций, выгруженные данные оплаченных ордеров на криптобиржах и т.п.[351]

---

[351] *Титов, А.А.* Отдельные особенности рассмотрения сообщений (заявлений) о преступлениях, совершенных с использованием криптовалют / А.А. Титов // Вестник Академии Следственного комитета Российской Федерации. – 2023. – № 2. – С. 121-128.

Типичным является случай, когда потерпевший, будучи введенным в заблуждение обещаниями быстрого обогащения, переводит свои криптовалютные активы на кошелек, контролируемый злоумышленниками. При этом в ходе опроса выясняется, что общение с мошенниками осуществлялось через мессенджер Телеграм, где они представлялись сотрудниками инвестиционной компании и убедили потерпевшего вложить средства в «перспективный» проект. Потерпевший, доверяя полученной информации, перевел средства на указанный кошелек, после чего связь с мошенниками прервалась, а его активы были утрачены.

При опросе пострадавших от случаев манипулирования рынком криптовалют в протоколе фиксируется, посредством каких ресурсов лицо получило информацию о конкретной криптовалюте, ICO-проекте или лицах, подозреваемых в манипулировании рынком.

Источники информации могут включать рекламные кампании в социальных сетях, рекомендации и продвижение от влиятельных лиц, блогеров и аналитиков. Также зачастую информация распространяется в закрытых группах или каналах в мессенджерах, где представляются инсайдерские сведения или торговые рекомендации. При опросе следует уточнять, какого рода обещания высокой доходности и минимизации рисков инвестирования поступали от злоумышленников, использовались ли приемы давления на потерпевшего, направленные на стимулирование покупки криптовалюты или токенов.

Целесообразно приобщать к опросу скриншоты: переписок с предполагаемыми злоумышленниками; рекламных объявлений, обещаний, торговых сигналов и других материалов; выгрузки данных ордеров на криптобиржах; скриншоты графиков изменения цен; выписки из криптокошельков; документы, удостоверяющие личность, и иные данные, предоставленные организаторам ICO или участникам манипулятивных схем.

По преступлениям *второй категории, где криптовалюта является средством осуществления преступной деятельности* и где источником оперативной информации являются данные о транзакциях и подозрительной

активности, связанной с криптовалютными кошельками, целесообразно организовать опрос сотрудника финансовой организации или представителя ПФР для установления обстоятельств, способствующих раскрытию преступления[352]. При обнаружении транзакции, которая соответствует определенным критериям подозрительности, она отмечается системой мониторинга и направляется на дальнейшее расследование. В ходе расследования анализируется дополнительная информация о транзакции, контрагентах и клиенте. Соответственно, в ходе опроса уполномоченный сотрудник может дать пояснения по поводу данных обстоятельств.

После получения установочной информации о произошедшем событии в ходе проверки деяний, как первой, так и второй категории целесообразно организовать *ОРМ «Наведение справок»*[353]. Аналогичный механизм получения оперативно значимой информации гласными методами в иностранных юрисдикциях также обозначается как «Разведка из открытых источников» (с англ. – Open source intelligence; OSINT)[354]. По справедливому утверждению профессора А.Л. Осипенко, анализ полученных данных в результате такой деятельности позволяет выявлять потенциальные угрозы и новые тенденции в преступной деятельности, планировать оперативные мероприятия[355].

В ходе наведения справок в адрес криптобирж и обменников могут быть направлены запросы для установления личности владельцев криптовалютных кошельков, участвующих в преступных транзакциях.

---

[352] *Фомичев, А.В.* Использование возможностей Федеральной службы по финансовому мониторингу в ходе предварительного расследования: Методическое пособие / под ред. Д.А. Кунева; под общ. ред. А.В. Лавренко. – М., 2016. – С. 20.

[353] *Сергеев, С. М.* Возможности ОРМ «Наведение справок» при проверке сообщения о преступлении экономической направленности / С. М. Сергеев // Криминалистика: вчера, сегодня, завтра. – 2022. – № 4(24). – С. 161-167.

[354] *Pastor-Galindo, J.* The not yet exploited goldmine of OSINT: opportunities, open challenges and future trends / J. Pastor-Galindo, P. Nespoli, F.G. Mármol, G.M. Pérez // IEEE Access. – 2020. – Vol. 8. – P. 10282–10304.; *Hayes, D.R.* Open-source intelligence for risk assessment / D.R. Hayes, F. Cappa // Business Horizons. – 2018. – Vol. 61. № 5. – P. 689–697.

[355] *Осипенко, А. Л.* Информационное воздействие на криминальную среду в условиях цифровизации / А. Л. Осипенко // Вестник Краснодарского университета МВД России. – 2024. – № 4(66). – С. 6-14.

Рассматривая специфику проведения ОРМ в таких условиях, Ю.В. Гаврилин, И.С. Бедеров и А.А. Хайдаров исследуют вопрос о необходимости предварительного поиска криптобиржи оперуполномоченным в рамках мониторинга общедоступных ресурсов в сети Интернет[356]. Соглашаясь с важностью подобного мониторинга, отметим, что подобные сведения могут быть также получены в ходе иных оперативно-розыскных и оперативно-технических мероприятий.

Следует в том числе учитывать, что оперативным сотрудником в рамках наведения справок также может быть направлен запрос: 1) интернет-провайдерам и другим организациям для установления IP-адресов и других технических данных, связанных с использованием криптовалютных сервисов; 2) регистраторам доменных имен и хостинг-провайдерам для установления владельцев веб-сайтов и доменов, используемых в преступных целях; 3) в банковские организации для получения информации о транзакциях, связанных с выводом криптовалютных средств в фиатные деньги.

Также подчернем, что оперативно значимые сведения при выявлении преступной деятельности могут быть получены из самой инфраструктуры криптовалют[357]. Как было отмечено в предыдущей главе, транзакции с биткоином и большинством других криптовалют основаны на существовании публичного реестра – блокчейна, в котором они подтверждаются и записываются в хронологическом порядке для обеспечения целостности системы. При этом блокчейн фиксирует все транзакции, проведенные владельцем определенного криптокошелька, в хронологическом порядке. Для каждой транзакции записывается идентификатор транзакции, дата и время

---

[356] *Гаврилин, Ю.В.* Установление личности владельцев цифровой валюты: методологические основы / Ю.В. Гаврилин, И.С. Бедеров // Труды Академии управления МВД России. – 2021. – № 4 (60). – С. 101–108; *Хайдаров, А.А.* Установление владельца адреса криптокошелька в практике правоохранительных органов // Российский следователь. – 2024. – № 8. – С. 39–42.

[357] Об этом же упоминают и другие авторы. *Карымсаков, Р. Ш.* Вопросы прав и обязанностей органов, осуществляющих оперативно-розыскную деятельность в рамках борьбы с преступлениями, связанными с использованием криптовалют / Р. Ш. Карымсаков, Д. Ж. Молдакулова // Вестник науки. – 2025. – Т. 4. – № 1(82). – С. 293-303.

транзакции, адрес отправителя и получателя[358], переведенная сумма, стоимость транзакции и остаток. Вся вышеуказанная информация является общедоступной и может быть проверена на различных сайтах. В блокчейне можно проверить и баланс каждого адреса криптоактива, в котором хранится полная история транзакций, общая сумма отправленных и полученных средств, а также итоговый баланс.

Таким образом, при наведении справок оперативный сотрудник может получить историю транзакций определенного адреса криптовалюты, включая адреса всех пользователей, с которыми он совершал транзакции, а также дату, время и точную сумму перевода. Это является полезным критерием при одновременном анализе большого количества транзакций.

Помимо этого, представляется целесообразным отследить всю совокупность транзакций, осуществленных с каждым криптоактивом с момента его эмиссии, а также IP-адреса, ассоциированные с каждым криптокошельком. Комплексный анализ полученного массива данных и его сопоставление со сведениями из иных источников имеет определяющее значение для выявления признаков преступной деятельности, идентификации причастных лиц и установления их роли в совершении преступления.

По *криптопреступлениям второй категории* при наведении справок полезно ввести имеющиеся данные о фигуранте (никнейм, адрес электронной почты, адрес криптокошелька и др.) в поисковые браузеры сети Интернет, поскольку лица, участвующие в незаконной торговле, часто публикуют свой адрес, связывая его со своим аккаунтом и псевдонимом. При этом на форумах или в разделах комментариев специализированных криптовалютных сайтов могут быть установлены дополнительные сведения. Аналогичный метод используется для получения информации в сети Даркнет, где существует множество форумов (Dread, Darknet Avengers, The Hub, Exploit.in и др.), на которых устанавливаются сведения о скрытых сервисах, их адресах,

[358] Для каждой транзакции может быть один или несколько адресов отправителя и один или несколько адресов получателя.

комментарии о качестве обслуживания, псевдонимы самых (или наименее) успешных продавцов и т.д.

В данном контексте важно учитывать три ключевых аспекта. Во-первых, псевдонимы или имена, используемые в сети лицами, осуществляющими противоправную деятельность, могут остаться неизменными. Это обусловлено, с одной стороны, тем, что успешность их незаконной коммерческой деятельности в сети Интернет, как правило, тесно связана с их репутацией среди клиентов (то есть с отзывами, оставленными о них на криптобиржах или форумах). Во-вторых, лица, проводящие значительную часть своей жизни в «виртуальном мире», склонны формировать устойчивую привязанность к псевдонимам, которые идентифицируют их в сети, и неохотно отказываются от их использования даже в целях соблюдения конспирации[359].

В-третьих, необходимо учитывать, что цифровые псевдонимы зачастую имеют корреляцию либо в открытом сегменте сети, либо в реальной жизни, что при мониторинге форумов и сайтов позволяет установить связь между противозаконной деятельностью и его верифицированной личностью. В данном контексте целесообразно использовать ошибки, которые часто допускают злоумышленники (например, используется один и тот же адрес криптокошелька как для законных, так и для незаконных операций), или же в общении с покупателями предоставляется адрес электронной почты, связанный с реальным именем[360].

В ходе расследования деятельности торговой площадки «Шелковый путь» правоохранительным органам США удалось идентифицировать личность её

---

[359] Так, причастность знаменитого хакера Альберта Гонсалеса к противоправной деятельности была установлена после ареста его российского покупателя при попытке въезда в США. Ключевым элементом, позволившим связать Гонсалеса с новыми преступлениями, стало использование им старого, хорошо известного псевдонима «Суп Наци». Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets // https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guide-on-relevant-aspects-and-appropriate-steps-for-the-investigation-identification-seizure-and-confiscation-of-virtual-assets.pdf (дата обращения: 30.03.2025).

[360] Barigye, C.K. Chairperson, Virtual Assets Working Group, FIA / C.K. Barigye. – 2023 // https://www.fia.go.ug/sites/default/files/downloads/FIA_Virtual_Assets_Working_Document_12th_June.pdf (дата обращения: 30.03.2025).

администратора, Росса Ульбрихта, используя методы поиска в сети Интернет. На начальном этапе своей преступной деятельности Ульбрихт допустил оплошность, разместив рекламу онлайн-платформы на открытом форуме, посвященном запрещенным наркотическим средствам, под псевдонимом «Altoid». Позднее, исполняя обязанности администратора «Шелкового пути», он использовал псевдоним «Ужасный пират Робертс». Спустя некоторое время он зарегистрировался на другом форуме под тем же псевдонимом («Altoid») и запросил информацию о биткоине, указав свой адрес электронной почты для связи с другими пользователями. Именно эта ошибка позволила установить связь между деятельностью «Шелкового пути» и псевдонимом «Altoid», а затем – с личным адресом электронной почты Ульбрихта, что в итоге способствовало его идентификации.

В контексте раскрытия криптопреступлений анализ в ходе наведения справок является перспективным методом выявления деятельности нелицензированных поставщиков услуг виртуальных активов, криптомиксеров и децентрализованных P2P-платформ обмена криптоактивами.

Примером практического применения такого метода является идентификация нелицензированных ПУВА. Например, анализ открытых реестров компаний, данных о регистрации доменных имён и информации, публикуемой регулирующими органами, позволяет выявлять организации, осуществляющие операции с криптоактивами без соответствующей лицензии. При этом посредством мониторинга форумов и социальных сетей, где обсуждаются вопросы инвестиций в криптовалюты, есть возможность установить нелегальные платформы, предлагающие услуги обмена или инвестирования, но не зарегистрированные в установленном порядке[361].

Изучение деятельности криптомиксеров, используемых для сокрытия происхождения и движения криптоактивов, также способно быть эффективным с

[361] Toezichtsrapport Automated OSINT: tools en bronnen voor openbronnenonderzoek CTIVD nr. 74. 2021. – URL: https://www.ctivd.nl/onderzoeken/aivd-mivd-onderzoek-automated-osint/ (дата обращения: 30.03.2025).

применением указанного метода. Анализ трафика, метаданных транзакций и информации о серверах, предоставляющих услуги микширования, позволяет идентифицировать связанные с ними адреса и оценивать объемы обрабатываемых транзакций. Например, обнаружение упоминаний конкретного криптомиксера в связи с отмыванием средств, полученных в результате кибервымогательства, вполне может стать начальным звеном в «цепи» транзакций, которые осуществлялись причастными лицами.

Это обусловлено тем, что операционная деятельность указанных структур основана на той же системе репутационного контроля, что и у нелегитимных онлайн-маркетплейсов, рентабельность которых во многом зависит от обратной связи участников рынка в специализированных разделах или на профильных форумах. Например, на таких ресурсах пользователи предоставляют информацию о качестве обслуживания, его доступности, случаях мошенничества и т. д.[362]

В дополнение к вышесказанному следует отметить, что методы получения информации из открытых источников в рамках ОРМ «Наведение справок» могут быть эффективно применены для установления взаимосвязей между лицами, подозреваемыми в причастности к незаконной деятельности как по преступлениям, совершаемым в отношении криптовалют, так и с их использованием.

Несмотря на широкое распространение инструментов анонимизации и дистанционный характер взаимодействия в киберпространстве, сохраняется возможность установления устойчивых связей между участниками незаконной деятельности. Это обусловлено необходимостью формирования доверительных отношений, поскольку лицо, осуществляющее легализацию доходов, полученных преступным путем, с высокой долей вероятности будет стремиться

[362] В отдельных иностранных юрисдикциях оперативные органы, действуя анонимно, могут получить доступ к указанным форумам. Полученные данные могут быть использованы для идентификации лиц, которые потенциально взаимодействуют с лицами, представляющими оперативный интерес.

к установлению контроля над финансовыми потоками и, как следствие, не сможет делегировать подобные функции лицу, не вызывающему доверия[363].

Необходимо также учитывать, что анализ информации, доступной из открытых источников, включая данные об образе жизни, активах, местах проживания и коммерческой или социальной активности заподозренных лиц, позволяет получить ценные сведения. При этом следует учитывать, что даже лица, придерживающиеся высоких стандартов конспирации, могут не контролировать социальную активность своих родственников и близких. Непреднамеренная публикация информации в социальных сетях, раскрывающая обстоятельства жизни и деятельности, а также связи лиц, причастных к преступлению, может оказать существенную помощь в расследовании преступлений, связанных с использованием криптовалюты.

Одним из примеров использования открытых источников при расследовании криптопреступлений является дело И. Лихтенштейна и Х. Морган, связанных с хищением биткоинов с криптобиржи Bitfinex в 2016 г. на сумму 4,5 млрд долл. США. Указанные лица были задержаны в 2022 г., причем существенную роль в идентификации сыграл анализ их активности в социальных сетях и данных об их окружении[364].

При изучении социальных сетей следует обращать внимание на то, что в рамках каждого интернет-ресурса имманентно присутствует как минимум два уровня данных, которые могут быть использованы при проведении оперативно-розыскных мероприятий. Во-первых, это уровень контента, включающий в себя информацию, «опубликованную» пользователем (сообщения, фотоизображения, видеоматериалы и т.д.). Дело в том, что размещенные визуальные материалы

---

[363] *Ульянова, М. А.* Тактика получения и анализа информации, передаваемой в сетях связи с использованием технологии оконечного шифрования, при расследовании преступлений террористического характера / М. А. Ульянова // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : Сборник статей Международной научно-практической конференции, Москва, 18 мая 2018 г. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2018. – С. 296-299.

[364] Married couple arrested alleged conspiracy // https://www.justice.gov/opa/pr/married-couple-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (дата обращения: 20.03.2025).

способны предоставить значительный объем сведений о субъекте, включая не только его физиологические данные, но и информацию о социокультурном окружении, географическом местоположении, социальном статусе, идеологических убеждениях и т.д. В частности, это происходит и тогда, когда визуальные материалы «маркируются» тегами, ассоциирующими их с профилями пользователей социальной сети или с лицами, не зарегистрированными в данном сервисе[365].

Так, в ходе проведения поверочных мероприятий сотрудниками ПФР Косово была обнаружена страница в социальной сети Facebook[366], принадлежащая одному из местных владельцев компании OneLifeNetwork Ltd. Изучение размещенных на странице фотографий позволило установить, что указанное лицо, по всей видимости, является работником физического труда, возможно, маляром или строителем. Такой вывод был сделан из-за загрязненности ногтевой части рук лица, изображенного на фотографии. В связи с этим ПФР Косово совместно с банком, предоставившим сообщение о подозрительной операции, инициировало проверку наличия у данного лица специальных знаний, необходимых для реализации продукции в сфере информационных технологий. При проведении личной встречи в банковском учреждении указанное лицо не смогло предоставить убедительные ответы на вопросы, связанные с его официальной деятельностью. Этот факт стал одним из оснований проведения оперативно-розыскных мероприятий по документированию деятельности, связанной с многоступенчатым криптовалютным мошенничеством[367].

Под первым уровнем находится второй уровень, представленный метаданными, которые могут сообщать информацию о компьютерном

---

[365] The changing nature of crime and criminal investigations // Police Executive Research Forum (PERF). – 2018. – P. 51.

[366] Признана экстремистской организацией и запрещена на территории Российской Федерации.

[367] Лучшие дела, расследованные членами Группы «Эгмонт». Дела, при расследовании которых осуществлялся финансовый анализ (2014-2020 годы) // www.egmontgroup.org (дата обращения: 30.03.2025).

устройстве, посредством которого был опубликован контент, о самих пользователях или описательные данные файлов. Характерным примером таких метаданных являются EXIF-данные («формат файлов изображений с возможностью обмена»), которые изначально содержатся в видео- или фотоматериалах и описывают оборудование и параметры, использованные при создании видео- или фотоизображения[368].

В зависимости от характеристик используемого оборудования, метаданные фото- и видеоматериалов содержат информацию о дате, времени и географическом местоположении их создания. Данные сведения позволяют установить эмпирические факты или сформировать аналитические выводы о субъектах или организациях, связанных с этими файлами или аккаунтами в социальных сетях, где они были размещены. Даже такие, на первый взгляд, незначительные детали, как SSL-сертификаты (от англ. Secure Sockets Layer) на интернет-страницах, могут раскрыть информацию о владельце соответствующего ресурса[369].

Посвятив свое исследование вопросам противодействия кибератак на инфраструктуру криптовалют, В.И. Глотов и Д.М. Михайлов справедливо отмечают, что для упрощения и автоматизации процессов поиска в открытых источниках разработан широкий спектр технологических инструментов, каждый из которых обладает уникальными функциональными возможностями[370].

Подтверждением данному выводу служит платформа Maltego, интегрирующая данные из разнообразных открытых источников, которая позволяет визуализировать сложные связи между объектами расследования,

---

[368] *Bartos, P.* Bitcoin Transaction Graph Analysis for Law Enforcement Purposes / P. Bartos, J. Feliks // Security and Safety Challenges for Smart Cities: Proceedings of the 15th International Conference on Cyber Warfare and Security (ICCWS 2020). – Academic Conferences and Publishing International, 2020. – С. 141-148.

[369] *Qureshi, S.U.* Systematic review of deep learning solutions for malware detection and forensic analysis in IoT / S.U. Qureshi, J. He, S. Tunio, N. Zhu, A. Nazir, A. Wajahat, F. Ullah, A. Wadud // Journal of King Saud University - Computer and Information Sciences. – 2024. – Vol. 36, Issue 8. – P. 102-164.

[370] *Глотов, В. И.* Криптобезопасность криптовалют / В. И. Глотов, Д. М. Михайлов. – Москва : Российский экономический университет имени Г.В. Плеханова, 2019. – 116 с.

такими как криптокошельки, адреса электронной почты и идентификаторы пользователей, выявляя потенциальные сети, участвующие в незаконной деятельности[371].

Наряду с общедоступными поисковыми системами, для обнаружения специфических типов данных применяются специализированные инструменты. Так, приложение Shodan ориентировано на поиск устройств, подключенных к сети Интернет, таких как веб-камеры, принтеры, VoIP-устройства и маршрутизаторы. Данный ресурс позволяет идентифицировать потенциально скомпрометированные устройства, используемые для проведения криптовалютных транзакций или хранения криптографических ключей, и тем самым содействовать в расследовании преступлений в сфере цифровых активов.

Другим примером является программа NameCHK, предоставляющая возможность проверки доступности имени пользователя в различных онлайн-сервисах. Функционал программы позволяет выявлять связи между псевдонимами, используемыми злоумышленниками в различных контекстах. Например, с помощью нее существует возможность обнаружения аккаунта подозреваемого на криптовалютной бирже, использующего тот же никнейм, что и на форуме, посвященному участию в фишинговых кампаниях[372].

Также следует упомянуть о программе Pipl, представляющей собой аналитический инструмент. Он позволяет осуществлять поиск совпадений в сети Интернет по различным критериям, включая имена, адреса электронной почты или номера телефонов, что предоставляет возможность агрегировать обширную информацию о фигурантах из разнообразных открытых источников[373].

---

[371] Cryptocurrency Investigations with Maltego: Tips & Tricks for Bitcoin and Ethereum Movement Analysis and Visualization // https://www.maltego.com/blog/cryptocurrency-investigations-with-maltego/ (дата обращения: 30.03.2025).

[372] *Shafee, S.* Evaluation of LLM-based chatbots for OSINT-based Cyber Threat Awareness / S. Shafee, A. Bessani, P.M. Ferreira // Expert Systems with Applications. – 2025. – Vol. 261. – P. 125.

[373] *Васюков, В. Ф.* К вопросу о получении оперативно значимой информации из открытых источников информации сети «Интернет» / В. Ф. Васюков, А. Ю. Афанасьев // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2024. – № 1(65). – С. 79-86.

Кроме того, платформы для совместной разработки, такие как GitHub, могут применяться для поиска и анализа программного кода, имеющего отношение к разработке и эксплуатации криптовалютных мошеннических проектов (скам-проектов) или вредоносного программного обеспечения, предназначенного для хищения криптовалюты. К примеру, анализ репозитория на GitHub, содержащего исходный код мошеннического ICO-проекта, позволяет выявить признаки мошеннической схемы и идентифицировать причастных разработчиков[374].

В тактическом плане данные инструменты OSINT позволяют оперативным сотрудникам формировать целостное представление о деятельности злоумышленников, связанных с криптовалютой, отслеживать движение средств, идентифицировать связанных лиц и выявлять уязвимости в системах безопасности. Использование вышеописанных технологий в совокупности с классическими методами расследования значительно повышает эффективность борьбы с преступлениями в сфере криптовалют.

Следует также отметить, что сотрудниками Базельского института (Швейцария) был разработан специализированный инструмент для оптимизации процесса поиска под названием «Basel Open Intelligence», который выполняет автоматизированный поиск информации о лице или организации, комбинируя запрос с более чем 200 ключевыми словами, связанными с финансовыми преступлениями, судебными разбирательствами, другими преступлениями, а также настраиваемыми списками ключевых слов[375]. Он также выполняет поиск в Даркнете, выделяя любые упоминания в списках санкций и о политически значимых лицах. Этот инструмент может выполнять поиск на нескольких языках и предоставляет пользователям возможность автоматического перевода статей на их язык для облегчения анализа. Документы, найденные в результате поиска,

---

[374] *Toulas, B.* Millions of GitHub repos likely vulnerable to RepoJacking, researchers say [Electronic resource] / B. Toulas. – 2023. – URL: https://www.bleepingcomputer.com/news/security/millions-of-github-repos-likely-vulnerable-to-repojacking-researchers-say/ (дата обращения: 30.05.2025).

[375] *Yamin, M.M.* Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security / M.M. Yamin, M. Ullah, H. Ullah, B. Katt, M. Hijji, K. Muhammad // Mathematics. – 2022. – Vol. 10, No. 12. – P. 2054.

перечисляются вместе с основным текстом, извлечённым с веб-сайта, без ненужного контента (например, реклама, меню или уведомлений о файлах cookie), с выделением ключевых слов для более удобного чтения[376].

В иностранной практике оперативные (разведывательные) службы довольно часто используют информацию, полученную от частных компаний, называемых «дата-брокеры» (от англ. – «data brokers»)[377]. Эти компании занимаются сбором и обработкой информации из множества источников, а также созданием подробных личных профилей, которые включают такие данные, как возраст, пол, образование, место работы, история проживания, семейные связи, количество детей, совершённые покупки, виды деятельности, использование социальных сетей, политические взгляды, расовая и религиозная принадлежность, уровень дохода, владение транспортными средствами и недвижимостью, сведения о приобретённых банковских и страховых продуктах, покупки по кредитным картам за последние 24 месяца, социально-экономический статус, экономическая стабильность и т. д.

Оперативно-розыскное мероприятие «Исследование предметов и документов», рассматриваемое в качестве значимого элемента оперативно-розыскной деятельности, закономерно приобретает особую актуальность при документировании деятельности организованных преступных сообществ[378]. Сущность данного мероприятия заключается в визуальном изучении, анализе и исследовании свойств предметов и документов с целью извлечения значимых сведений, установления их подлинности, выявления признаков фальсификации, а также определения связи с расследуемым преступлением[379].

---

[376] *Medina, M.* Inteligencia de fuente abierta / M. Medina // Basel Institute of Governance, Quick Guide Series. – 2020. – No. 17. – June.

[377] Например, такой деятельностью занимаются следующие иностранные компании: Equifax, Acxiom, Experian, Epsilon, CoreLogic, Datalogix, Intelius, PeekYou, Exactis, and Recorded Future.

[378] Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» / В. С. Овчинский, О. А. Вагин, Б. Я. Гаврилов [и др.]. – Москва : Издательский Дом «Инфра-М», 2022. – 488 с.

[379] *Агарков, А. В.* Оперативно-розыскное мероприятие «исследование предметов и документов»: содержание понятия / А. В. Агарков // Оперативно-розыскное противодействие наркопреступности : Материалы Всероссийского научно-практического семинара, Красноярск,

Практическая реализация данного ОРМ требует учета специфики криптопреступлений, которые, как известно, характеризуются высокой степенью цифровизации и использованием современных информационных технологий[380]. Следовательно, круг предметов и документов, подлежащих исследованию, включает в себя как традиционные материальные объекты, так и электронные носители информации (компьютеры, ноутбуки, смартфоны, USB-накопители)[381].

При раскрытии преступлений «в отношении» криптовалюты исследование предметов и документов направлено, прежде всего, на установление факта хищения, мошенничества или вымогательства криптоактивов, а также на выявление обстоятельств, способствовавших совершению преступления. В этой связи особому вниманию подлежат выписки из криптобирж, переписка с мошенниками, сообщения с угрозами (в случае вымогательства), а также электронные устройства, использовавшиеся для доступа к криптокошельку (компьютеры, смартфоны), на которых могут содержаться логины, пароли, ключи доступа и другая значимая информация.

Между тем при раскрытии преступлений, совершаемых «с использованием» криптовалют, исследование предметов и документов ориентировано на установление связи между криптовалютными транзакциями и основной преступной деятельностью, а также на выявление лиц, причастных к совершению преступления. В данном случае особое значение приобретает изучение электронных устройств, использовавшихся для осуществления транзакций (компьютеры, смартфоны), на которых могут содержаться сведения о

---

8 апреля 2022 г. – Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2022. – С. 53-56.

[380] *Горяинов К. К.* Некоторые вопросы оперативно-розыскной практики в борьбе с коррупционными проявлениями в США и Великобритании / К.К. Горяинов // Современное состояние и актуальные проблемы противодействия коррупции в органах и учреждениях УИС. Сборник материалов круглого стола. 2019. – С. 55-60.

[381] *Васюков, В. Ф.* Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют / В. Ф. Васюков, А. Н. Старжинская // Российское право: образование, практика, наука. – 2024. – № 4. – С. 68-78.

криптокошельках, транзакциях, IP-адресах и других данных, позволяющих установить личности преступников и их сообщников[382].

В процессе исследования предметов и документов необходимо учитывать возможность использования фигурантами различных методов сокрытия информации, таких как шифрование данных, использование стеганографии, удаление файлов и т.д. Как справедливо отмечается В.В. Семенчуком, для проведения качественного и всестороннего исследования необходимо привлекать квалифицированных специалистов в области информационных технологий, которые обладают необходимыми знаниями и навыками[383].

Для выявления преступной деятельности, связанной с криптовалютами, также может проводиться комплекс негласных оперативно-розыскных и оперативно-технических мероприятий, которые рассматриваются в специализированных изданиях. В силу ограничений, накладываемых российским законодательством на раскрытие сведений о тактике проведения таких мероприятий, акцентируем внимание на оперативной (разведывательной) деятельности иностранных государств.

Так, в отдельных странах правоохранительные органы реализуют тактику, связанную с созданием подконтрольных криптовалютных платформ, направленных на противодействие преступлениям, где криптовалюты являются инструментом их совершения. Суть данной тактики заключается в создании специализированных платформ-«приманок», имитирующих деятельность легальных криптовалютных сервисов. Такие структуры предлагают клиентам услуги по конвертации цифровых активов в фиатные валюты, инвестиционные инструменты с заявленной высокой доходностью, а также иные финансовые

---

[382] *Судницын, А. Б.* Отдельные возможности получения и использования сведений об операциях с криптовалютой при раскрытии и расследовании преступлений / А. Б. Судницын, В. В. Молоков // Вестник Восточно-Сибирского института МВД России. – 2019. – № 2(89). – С. 213-221.

[383] *Семенчук, В. В.* Вопросы информационного обеспечения выявления и раскрытия преступлений, совершаемых с использованием криптовалют / В. В. Семенчук // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 81-86.

операции, привлекательные для субъектов, вовлеченных в незаконную деятельность.

При этом ключевым элементом оперативного успеха является систематическая фиксация всех транзакций и коммуникаций, что обеспечивает формирование доказательственной базы, необходимой для уголовного преследования[384]. Технологии блокчейн-аналитики, дополненные традиционными методами оперативного наблюдения, позволяют не только идентифицировать участников преступных схем, но и реконструировать их сетевые взаимодействия, устанавливая ролевую иерархию и масштаб противоправной деятельности[385].

Ярким примером эффективности данного подхода выступает операция «Crypto Sweep», реализованная Федеральным бюро расследований США, в рамках которой были созданы подконтрольные криптобиржи, с помощью которых были задокументированы многочисленные факты незаконной финансовой деятельности строго законспирированных преступных формирований[386]. Подобные операции демонстрируют, что моделирование элементов криптовалютной инфраструктуры под контролем оперативных подразделений создает уникальные возможности для выявления «многослойных» схем отмывания средств, сочетая при этом разведывательный потенциал с оперативной смекалкой.

Между тем успешная реализация тактики создания технологически достоверных платформ-«приманок» требует детального погружения в специфику деятельности криминальных сообществ, включая анализ их операционных моделей, шаблонов общения и используемых инструментов. Ключевым условием является реконструкция цифровой площадки, в которой

---

[384] *Батраченко, Д. А., Васюков, В. Ф.* Некоторые вопросы получения оперативно значимой и криминалистической информации из облачных хранилищ // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2025. № 1 (69). С . 98–107.

[385] *Бабакова, М.А.* Проблемы розыска при расследовании преступлений в сфере высоких технологий : дис. … канд. юрид. наук / Бабакова Мария Алексеевна. – Саратов, 2010. – 268 с.

[386] Operation Cryptosweep // https://www.nasaa.org/policy/enforcement/operation-cryptosweep/ (дата обращения: 30.03.2025).

функционируют фигуранты, с точным воспроизведением не только технических параметров (интерфейсов, алгоритмов транзакций, протоколов безопасности), но и социокультурных норм, характерных для таких торговых площадок. Например, для имитации криптовалютной платформы, ориентированной на «отмывание» средств, необходимо интегрировать функционал, востребованный в криминальной среде: поддержку анонимных кошельков, P2P-обмен без проверки KYC, возможность использования миксеров или иных инструментов сокрытия транзакций. При этом важно учитывать региональные особенности, различия в предпочитаемых криптоактивах, методах вывода средств в фиатные валюты, а также в специфике используемого жаргона при общении[387].

Технологическая достоверность также достигается через комбинацию блокчейн-аналитики, мониторинга Даркнета и внедрения в закрытые форумы, что позволяет выявить актуальные тренды и уязвимости, эксплуатируемые ОПС. Например, если в определенном сегменте теневого рынка растет спрос на децентрализованные биржи с поддержкой криптовалюты Monero, то платформа-«приманка» должна имитировать соответствующий функционал, включая «утечки» фиктивных логов транзакций в обозревателях блокчейна для создания иллюзии реальной активности. Одновременно с этим необходимо моделирование правдоподобных цифровых следов, включающее генерацию легендированных отзывов на форумах, симуляцию рейтингов репутации в Телеграм-каналах и внедрение в цепочки доверия через содействующих посредников.

Однако даже безупречная техническая реализация может быть поставлена под угрозу из-за недостатков в оперативной легенде. Организованные преступные сообщества нередко используют многоуровневую систему верификации новых участников криминального рынка, включающую проверку истории криптокошельков на связь с сомнительными адресами, поиск упоминаний платформы в закрытых источниках, и тестирование на устойчивость

---

[387] *Титов, А.А.* Использование криптовалют в преступных целях: методы выявления и противодействия / А.А. Титов // Современное общество и право. – 2024. – № 4. – С. 138-146.

к DDoS-атакам и попыткам взлома. Поэтому правоохранительным органам необходимо предвосхищать такие сценарии, например создавая искусственные хакерские атаки на собственную платформу с последующей публикацией «исправлений» в Даркнете, что усиливает иллюзию её легитимности.

Для минимизации подобных проблем в ряде юрисдикций применяются гибридные модели, где часть функций платформы делегируется «подсадным» участникам из числа ранее завербованных лиц, чьи действия документируются в режиме реального времени. Примером служит международная операция «Piilopuoti», в ходе которой Таможенной службой Финляндии, Федеральным управлением уголовной полиции Германии и Бюро криминальной полиции Литвы были сымитированы различные элементы технической инфраструктуры, которые были прорекламированы на одном уже получившем известность сервисе[388]. Таким образом, технологическая достоверность становится не самоцелью, а инструментом формирования управляемой криминальной среды, где каждое действие субъекта может быть использовано для его же нейтрализации.

В правоохранительной практике Нидерландов значительное место занимают «особые следственные полномочия», связанные с внедрением агентов под прикрытием в криминальные сети, специализирующиеся на незаконном обороте товаров с использованием криптовалюты. Основной тактикой в данных операциях является имитация агентами роли продавцов или покупателей, заинтересованных в установлении деловых контактов с целью последующего документирования противоправной деятельности[389]. Ключевым элементом

---

[388] Официальное сообщение о проведенной операции получило отражение в сети Интернет. См: International operation closes down Piilopuoti dark web marketplace // https://www.europol.europa.eu/media-press/newsroom/news/international-operation-closes-down-piilopuoti-dark-web-marketplace (дата обращения: 30.03.2025).

[389] Следует отметить, что в соответствии с голландским Законом об Особых следственных полномочиях (Bijzondere Opsporingsbevoegdheden) установлены три формы деятельности тайных агентов: систематический сбор разведывательной информации, покупка нелегальных товаров или веществ (или) оказание нелегальных услуг (тайные закупки) и оперативное внедрение. *Kruisbergen, E.W.* When Other Methods Fail…: Infiltrating Organized Crime Groups in the Netherlands / E.W. Kruisbergen // Contemporary Organized Crime. Studies of Organized Crime,

успешного внедрения выступает демонстрация агентом профессиональной компетентности и операционной надежности, что необходимо для формирования у целевых субъектов восприятия потенциальной выгоды и минимизации рисков при взаимодействии.

Данный подход основывается на принципах социального доверия, характерного для закрытых криминальных сообществ, где установление деловых отношений требует подтверждения репутации и соответствия неформальным нормам. Однако оперативная деятельность в таких условиях сопряжена с высокой степенью неопределенности, обусловленной динамикой нелегальных рынков, включая изменчивость методов коммуникации, эскалацию подозрительности среди участников и использование криминальными группами контрразведывательных механизмов. Эти факторы требуют от агентов адаптивности, глубокого понимания субкультурных особенностей и способности поддерживать правдоподобность легенды в условиях непредсказуемого поведения контрагентов. Эффективность подобных операций напрямую зависит от психологической подготовки сотрудников, их умения балансировать между необходимостью собирания доказательств и избегания провокационных действий, что подчеркивает этико-правовую сложность применения подобных методов в рамках действующего законодательства[390].

В зарубежной практике широкое применение при осуществлении операций по выявлению преступной деятельности в криптовалютной среде получила тактика «восстановления seed-фразы»[391].

---

vol 18. / ed. by H. Nelen, D. Siegel. – Cham: Springer, 2021. – DOI: https://doi.org/10.1007/978-3-030-56592-3_15

[390] *Kruisbergen, E.W.* Combating organized crime A study on undercover policing and the followthe-money strategy / E.W. Kruisbergen. – 2017. – URL: https://www.Ew-Kruisbergen-2/publication/312197822_Combating_Organized_Crime_A_Study_on_Undercover_Policing_and_the_Follow-the-Money_Strategy/links/5875fd1908ae6eb871cdd126.pdf (дата обращения: 30.03.2025).

[391] *Shaik, C.* Securing cryptocurrency wallet seed phrasedigitally with blind key encryption / C. Shaik // International Journal on Cryptography and Information Security (IJCIS). – 2020. – Vol. 10. – No. 4 // https://www.wireilla.com/papers/ijcis/V10N4/10420ijcis01.pdf (дата обращения: 30.03.2025).

Данная тактика предполагает проведение комплекса оперативных (разведывательных) мероприятий, направленных на поиск seed-фразы, представляющей собой уникальный набор из 12 или 24 слов. Указанная фраза является ключом для доступа к цифровым активам, а ее значимость обусловлена тем, что обладание seed-фразой обеспечивает полный контроль над криптовалютным кошельком, включая возможность восстановления истории транзакций и управления всеми средствами, находящимися в кошельке.

Методы получения seed-фразы варьируются в зависимости от юрисдикционных и процессуальных норм. Наиболее законным способом является санкционированный обыск, проводимый на основании судебного ордера, предполагающий изъятие физических или цифровых носителей информации.

Отдельного изучения заслуживает метод выявления криминальных криптовалютных транзакций с использованием искусственного интеллекта в Сингапуре. В рамках созданной межведомственной платформы NAVIGATE сотрудники правоохранительных органов могут не только получать оперативно значимую информацию о подозрительных криптовалютных транзакциях, но и ставить на контроль конкретные криптокошельки, которые были установлены в ходе негласных мероприятий. Созданная платформа стала одним из элементов действующих Общенациональных Руководящих принципов управления активами и криптовалютами, реализация которых правоохранительными органами позволила с января 2019 г. по июнь 2024 г. изъять 6 млрд сингапурских долларов, связанных с преступной деятельностью и легализацией преступных доходов. Из этой суммы 416 млн сингапурских долларов было возвращено жертвам, а 1 млрд – конфискован в пользу государства[392].

Анализ успешных тактических операций, реализованных иностранными правоохранительными органами, свидетельствует о значимости сведений о пользователях открытых и закрытых сетей, геосервисов, приложений

[392] Singapore’s Law Enforcement Strategy to Combat Money Laundering. – October 2024. – URL: https://www.cpib.gov.sg/ (дата обращения: 30.03.2025).

смартфонов, клиентов различных учреждений и организаций, собираемой из различных источников специализированными программными комплексами[393]. Их использование позволяет сотрудникам оперативных подразделений формировать визуализированные отчёты о цифровой активности лиц, представляющих оперативный интерес. Встроенные инструменты «временной шкалы» дают возможность сопоставить эту активность с транзакциями, связанными с криптокошельками. В практике спецслужб США широко используется платформа Locate X, разработанная компанией Babel Street, которая предоставляет возможность отслеживать перемещения отдельных пользователей мобильных устройств по их уникальным идентификаторам мобильной рекламы[394], представляющим собой буквенно-цифровые коды, встроенные во все устройства Google Android и Apple[395]. Указанная платформа обеспечивает отслеживание пользователей, агрегируя данные о местоположении и другую идентифицирующую информацию, собираемую различными сайтами и передаваемую рекламным сетям, которые используют эту информацию для таргетирования рекламы для конкретных пользователей[396].

Перспективным направлением получения оперативно значимой информации в иностранных правоохранительных органах является использование метода «контроль на старте», позволяющего выявлять транзакции

---

[393] Наиболее популярные инструменты - Maltego, SpiderFoot, Gephi, IBM i2 Analyst’s Notebook, Shodan, Linkurious, Intelligence X, Sherlock, Google Dorking, Siren, DataWalk, Visallo, SEON, Lampyre, Maigret. OSINT: Information gathering using Maltego // https://www.maltego.com (дата обращения: 30.03.2025).

[394] Уикальные идентификаторы мобильной рекламы (англ. Mobile Advertising Identifier; MAID) - это уникальные анонимные идентификаторы, присваиваемые мобильным устройствам, таким как смартфоны и планшеты. Эти буквенно-цифровые коды позволяют рекламодателям отслеживать поведение пользователей в приложениях и на веб-сайтах, обеспечивая возможность целевой рекламы и оценки эффективности. См.: *Chasinov, N.* Mobile Advertising ID (MAID) Guide. 2024. – URL: https://www.teknicks.com/blog/capture-mobile-advertising-ids-maids/ (дата обращения: 30.03.2025).

[395] Toezichtsrapport Automated OSINT: tools en bronnen voor openbronnenonderzoek .CTIVD nr. 74. Vastgesteld op 22 december 2021 // file:///C:/Users/NICE/Downloads/CTIVD+NR74+Toezichts-rapport.pdf (дата обращения: 30.03.2025).

[396] The Global Surveillance Free-for-All in Mobile Ad Data // https://krebsonsecurity.com/2024/10/the-global-surveillance-free-for-all-in-mobile-ad-data/?ref=404media.co (дата обращения: 30.03.2025).

во временных хранилищах – «мемпулах»[397], что дает возможность отслеживать потенциально незаконные операции еще до их включения в блокчейн. Применение данного метода, требующего специализированного программного обеспечения и доступа к узлам сети блокчейн, способствует значительному повышению эффективности деятельности по предупреждению и раскрытию преступлений, связанных с использованием криптовалюты.

На основании вышеизложенного можно сформулировать следующие выводы.

1. Современный этап развития преступности, связанной с криптовалютами, характеризуется трансформацией оперативно-розыскной деятельности, обусловленной технологическими вызовами и необходимостью адаптации традиционных методов к цифровой реальности. Анализ представленного материала позволяет констатировать, что преступления, направленные на криптовалюты как объект посягательства или использующие их в качестве инструмента, формируют потребность в решении новых задач к собиранию, и и исследованию и верификации данных. Во-первых, анонимизация транзакций и децентрализованный характер блокчейна существенно усложняют идентификацию субъектов преступной деятельности, что актуализирует необходимость разработки специализированных алгоритмов, интегрирующих методы блокчейн-аналитики. Использование платформ для визуализации связей между криптокошельками и цифровыми идентификаторами демонстрирует эффективность междисциплинарного подхода, сочетающего криминалистические методики с технологиями больших данных.

2. Классификация криптопреступлений на две категории – посягательства на цифровые активы и их использование в противоправных целях – определяет дифференциацию тактических приемов. В первом случае приоритет отдается

[397] Мемпул (с англ. - Mempool, Memory Pool) – это «зона ожидания» транзакций, которые были подтверждены сетью, но ещё не включены в блокчейн. *Trozze, A.* Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering / A. Trozze, T. Davies, B. Kleinberg // Forensic Science International: Digital Investigation. – 2023. – Vol. 46. – 301575. –DOI: https://doi.org/10.1016/j.fsidi.2023.301575.

ретроспективному анализу транзакций через публичные реестры блокчейна с установлением цепочек перемещения активов, тогда как во втором фокус смещается на выявление инфраструктурных элементов (криптомиксеры, нелицензированные биржи), что требует применения превентивных оперативных моделей, включая создание контролируемых платформ-«ловушек». Между тем изучение иностранного опыта подтверждает, что симуляция элементов криптовалютной системы позволяет документировать деятельность организованных преступных групп с высокой точностью, однако успех таких операций напрямую зависит от технологической достоверности и учета субкультурных норм криминальной среды.

3. Трансграничный характер большинства криптопреступлений обусловливает необходимость гармонизации правовых механизмов международного сотрудничества, включая унификацию запросов к криптобиржам и обменникам. Даже частичная деанонимизация транзакций через анализ социальных медиа и метаданных способна стать ключевым звеном в установлении причастных лиц. В свою очередь это требует развития межведомственных баз данных и алгоритмов машинного обучения для обработки массивов неструктурированной информации. При этом сохраняются этико-правовые риски, связанные с использованием методов внедрения агентов под прикрытием, что подчеркивает необходимость четкой регламентации подобных операций в национальных законодательствах.

§ 2. Тактика проведения следственных действий на первоначальном этапе расследования преступлений, совершаемых в отношении и с использованием криптовалюты

Необходимость криминалистических знаний и криминалистических сил и средств возникла на основе не только развития преступности как социального явления, но и роста уровня ее оснащенности и ситуационности, требующей

совершенствования законодательства и процесса расследования, а также роста уровня криминалистического обеспечения соответствующих мер.

По мере развития прогресса в современной криминалистической деятельности теория отражения в ее криминалистической интерпретации приобретает все более значимые и вполне осязаемые практико-значимые черты. В данном ключе нельзя не отметить позицию И.И. Лузгина, который говорит о том, что «как и для правоохранительной системы, в целом рост уровня системности криминалистической деятельности становится все более значимым фактором, обеспечивающим эффективность уровня решаемых задач»[398]. Представляется, что одним из главных факторов системности является надлежащее организационное и тактическое обеспечение проведения следственных действий на первоначальном этапе расследования.

Анализ следственной, судебной практики и специализированной литературы позволяет утверждать, что осмотр является одним из наиболее значимых следственных действий при расследовании преступлений, связанных с криптовалютой.

В частности, *осмотр места происшествия* в расследовании подобных преступлений представляет собой сложную и трудоёмкую разновидность осмотра. Он представляет собой первоначальное следственное действие, определяющее дальнейший ход расследования и во многом формирующее доказательственную базу. Трудоемкость же обусловлена как спецификой цифровой среды, где следы могут быть отображены только в виде данных, так и необходимостью работы с технически сложными системами. Как небезосновательно отмечается итальянскими криминалистами, «эффективность осмотра напрямую влияет на возможность установления обстоятельств

[398] *Лузгин, И. И.* Актуальные вопросы использования цифровых технологий при производстве осмотра места происшествия / И. И. Лузгин // Пенитенциарная система, государство и общество: проблемы взаимодействия : материалы Международной научно-практической конференции, Псков, 15 октября 2021 г. – Псков: Псковский филиал Академии ФСИН России, 2022. – С. 168-172.

произошедшего, идентификацию причастных лиц и восстановления картины преступления»[399].

Общепринято считать, что целью осмотра является установление сущности произошедшего, а также надлежащая фиксация и удостоверение всех обнаруженных сведений, чтобы обеспечить возможность объективной оценки полученных доказательств другими участниками процесса и судом[400]. В контексте расследования преступлений, связанных с криптовалютой, под местом происшествия следует понимать участок цифрового пространства или физическое местоположение оборудования, где обнаружены или потенциально могут быть обнаружены цифровые следы, логи, транзакции, программное обеспечение и иные объекты, относящиеся к исследуемому событию.

Следует отметить, что место происшествия не обязательно совпадает с местом совершения преступления, то есть местом непосредственного осуществления преступного посягательства. Например, местом происшествия может быть компьютер подозреваемого, сервер криптовалютной биржи, электронный кошелек жертвы или иной цифровой ресурс. При расследовании преступлений, связанных с криптовалютой, возможно обнаружение нескольких мест происшествия, что требует комплексного и скоординированного подхода к осмотру и фиксации следов, оставленных в сети блокчейна.

В ходе осмотра места происшествия планомерно должны выполняться общие задачи, такие как:

– формирование чёткого представления и подробная фиксация в протоколе осмотра материальной обстановки, в которой произошло исследуемое событие, с акцентом на детали, способные раскрыть специфику совершения преступления в контексте криптовалютных операций;

– обнаружение, фиксация и изъятие следов использования криптовалюты, к которым могут относиться электронные носители информации (компьютеры,

---

[399] *Bonanni, E.* Tecniche investigative / E. Bonanni, G. Pettenati, F. Garoia, V. Paolillo. – 2010.

[400] *Гриненко, А. В.* Криминалистика : учебник / А. В. Гриненко, В. А. Дударев, С. С. Маевский. – Москва : Общество с ограниченной ответственностью "Проспект", 2025. – 432 с.

смартфоны, USB-накопители), содержащие данные о криптовалютных кошельках, транзакциях, ключах доступа, а также физические объекты, связанные с цифровой деятельностью (например, распечатки seed-фраз, заметки с паролями)[401];

– анализ связи обнаруженных следов с предполагаемым субъектом преступления, потерпевшим (в случаях, когда таковой имеется), иными лицами и объектами, потенциально задействованными в преступной схеме. При этом особое внимание должно уделяться выявлению взаимосвязей между цифровыми идентификаторами (IP-адресами, адресами криптовалютных кошельков) и реальными лицами или организациями[402];

– получение исходных данных, необходимых для установления и розыска лица, совершившего преступление, планирования и проведения оперативно-розыскных мероприятий и следственных действий. В частности, требуется произвести сбор информации, позволяющей отследить движение криптовалютных средств через блокчейн, идентифицировать криптовалютные биржи, используемые для обналичивания средств, и установить личность владельцев криптовалютных кошельков[403].

При расследовании преступлений, совершенных как в отношении, так и с использованием криптовалюты, неукоснительное соблюдение принципов осмотра места происшествия приобретает особую значимость.

Своевременность осмотра места происшествия имеет решающее значение для успешного расследования преступлений, связанных с криптовалютой. Незамедлительный выезд следственной группы на место происшествия после

---

[401] *Бардачевский, Р.И., Соршнев, Ю.Н.* Особенности производства следственных действий, связанных с поиском и изъятием криптовалютных финансовых активов по уголовным делам о коррупционных преступлениях // Российский следователь. – 2021. – № 6. – С. 3-5.

[402] *Бахтеев, Д.В.* Векторы цифрового развития криминалистики / Д. В. Бахтеев // Технологии XXI века в юриспруденции : Материалы Шестой всероссийской научно-практической конференции, Екатеринбург, 24 мая 2024 года. – Екатеринбург, 2024. – С. 13-17.

[403] *Русман, Г.С.* Первоначальный этап расследования преступлений, связанных с использованием криптовалюты / Г. С. Русман // Smart Law for Smart Industry : сборник научных статей / под ред. Е. В. Титовой, Т. П. Подшивалова; Южно-Уральский государственный университет юридический институт. – Москва : РГ-Пресс, 2020. – С. 191-195.

получения соответствующего сообщения имеет ключевое значение, поскольку задержка может привести к утрате важных доказательств.

При расследовании преступлений, связанных с криптовалютой, такая утрата может быть вызвана как преднамеренными действиями, направленными на сокрытие следов преступления (например, удаление информации с носителей, сокрытие оборудования для майнинга, перевод криптовалюты на другие кошельки), так и непреднамеренными обстоятельствами, связанными с изменением обстановки на месте происшествия, повреждением или уничтожением следов и других материальных объектов, имеющих доказательственное значение[404].

Учитывая динамичный характер цифровой среды и возможность быстрого перемещения криптовалютных активов, оперативное проведение осмотра в случаях, не терпящих отлагательств, до возбуждения уголовного дела является необходимой мерой для обеспечения полноты и объективности расследования, позволяющей зафиксировать состояние цифровых активов и оборудования, а также выявить и закрепить электронные следы, имеющие значение для установления обстоятельств совершения преступления и идентификации лиц, причастных к нему[405].

Полнота осмотра места происшествия в контексте расследования преступлений, связанных с криптовалютой, предполагает исследование всей обстановки, всех объектов и следов, потенциально имеющих отношение к делу[406]. Однако данное тактическое положение не следует интерпретировать как механическую фиксацию следователем в протоколе осмотра всех без

---

[404] *Стельмах, В. Ю.* Производство следственных действий, направленных на получение и использование компьютерной информации / В. Ю. Стельмах, О. М. Ефремова, В. Ф. Васюков. – Москва : Общество с ограниченной ответственностью "Проспект", 2021. – 480 с.

[405] *Маркарян, Э. С.* Специфика проведения следственного осмотра при расследовании преступлений, совершенных с использованием криптовалют / Э. С. Маркарян // Актуальные проблемы российского права. – 2018. – № 6(91). – С. 146-152.

[406] *Гаврилин, Ю.В.* Расследование преступлений, посягающих на информационную безопасность в сфере экономики : теоретические, организационно-тактические и методические основы : автореф. дис. … д-ра юрид. наук / Гаврилин Юрий Викторович. – Москва, 2010. – 55 с.

исключения объектов, обнаруженных на месте происшествия. Обеспечение подлинной полноты осмотра достигается за счет всестороннего учета всех объективно возможных версий о механизме события и их тщательной проверки путем анализа материальной обстановки. Требование полноты осмотра приобретает особую значимость в связи с тем, что данное следственное действие зачастую неповторимо.

Перефразируя в позитивном контексте тезис профессора Г.М. Меретукова, можно говорить о том, что упущенные или несвоевременно зафиксированные следы и объекты могут быть утрачены в результате воздействия внешних факторов (погодных условий, технических средств, действий лиц), что приведёт к невосполнимой потере доказательственной информации[407]. Применительно к «криптовалютным» расследованиям это может включать в себя, помимо прочего, исследованиие компьютерного оборудования, носителей информации, сетевого оборудования, документации, связанной с приобретением, хранением и передачей криптовалютных активов, а также любые физические следы, указывающие на связь с совершением преступления, с целью выявления ключевых узлов и маршрутов транзакций, идентификации участников и установления фактических обстоятельств дела.

Планомерность осмотра, понимаемая как последовательное, целенаправленное и активное исследование цифровой среды и связанных с ней физических объектов, является также важным элементом успешного установления обстоятельств дела[408]. Следователь, руководствуясь заранее разработанным планом, должен методично переходить от одного электронного носителя информации к следующему (например, от «холодного»

---

[407] *Меретуков, Г. М.* Осмотр места происшествия как источник криминалистически значимой информации / Г. М. Меретуков // Год науки и технологий 2021 : Сборник тезисов по материалам Всероссийской научно-практической конференции, Краснодар, 9–12 февраля 2021 г. / отв. за выпуск А.Г. Кощаев. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2021. – С. 223.

[408] *Бульбачева, А. А*. Актуальные проблемы осмотра места происшествия / А. А. Бульбачева // Труды Академии управления МВД России. – 2015. – № 2(34). – С. 97-100.

криптокошелька компьютера к «горячему»), тщательно анализируя каждый из них.

Объективность осмотра, подразумевающая беспристрастное изучение и фиксацию цифровых следов, транзакций, идентификаторов и иных релевантных данных, независимо от их соответствия первоначальным гипотезам, также имеет первостепенное значение для исключения предвзятости и обеспечения всесторонности расследования.

Ответственность за организацию и координацию осмотра, как правило, возлагается на следователя, который определяет последовательность действий всех участников, включая специалистов в области блокчейн-технологий и информационной безопасности. Важно отметить, что любые действия, направленные на изменение обстановки или воздействие на электронные устройства, должны осуществляться исключительно с разрешения следователя и под его строгим контролем.

При этом следователь, фиксируя в протоколе осмотра результаты собственного восприятия цифровой среды и физических объектов, должен опираться на мнение участвующих специалистов, учитывая их замечания и рекомендации, что обеспечивает полноту и достоверность собранных доказательств. Соответственно эффективное взаимодействие следователя и оперативных сотрудников УБК МВД России в процессе осмотра места происшествия, связанного с преступлениями в сфере криптовалют, определяется непрерывным обменом информацией, коллегиальным обсуждением эмпирических данных, полученных в ходе осмотра, и последующей проверкой его результатов. Данный процесс предполагает, в том числе, использование подхода, основанного на интеграции криминалистических и оперативно-розыскных методов[409].

---

[409] *Титов, А.А.* Некоторые вопросы обнаружения и исследования компьютерной информации при раскрытии и расследовании преступлений / А.А. Титов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2022. – № 3(37). – С. 39-48.

Осмотр на территории организации, учреждения или предприятия в рамках расследования, связанных с криптовалютой, настоятельно рекомендуется осуществлять в присутствии представителя администрации или частной фирмы. Такая практика обусловлена тем, что представитель организации обладает специальными знаниями о внутренней структуре предприятия, функциональном назначении помещений и используемых механизмах, что существенно облегчает процесс осмотра и повышает его эффективность. Присутствие компетентного представителя позволяет следователю оперативно ориентироваться в сложной обстановке, избегая потенциальных ошибок в интерпретации обнаруженных объектов и процессов. Более того, представитель организации может оказать содействие в предоставлении необходимых технических средств, а также в привлечении квалифицированных специалистов для консультаций и помощи в проведении осмотра, что способствует более глубокому и всестороннему изучению обстоятельств дела, связанных с криптоактивами.

При расследовании преступлений, связанных с криптовалютой, привлечение специалиста является важным элементом эффективного и всестороннего осмотра места происшествия и сопутствующих цифровых активов. Необходимость участия специалиста обусловлена тем, что функционирование криптовалюты, механизмы транзакций, особенности хранения и обеспечения анонимности требуют специальных знаний в области блокчейн-технологий, криптографии и информационных технологий. Специалист помогает следователю ориентироваться в специфической цифровой среде, способствуя пониманию характера происшествия, идентификации и интерпретации релевантных данных, таких как адреса кошельков, идентификаторы транзакций (TxID), записи в блокчейне и особенности используемого программного обеспечения.

В частности, специалист оказывает помощь в корректном описании в протоколе осмотра технических аспектов, связанных с криптокошельками (аппаратными и программными), устройствами для майнинга, криптобиржами и другими элементами инфраструктуры. Используя специализированные

программные и аппаратные средства, специалист способствует выявлению, фиксации и изъятию цифровых следов, которые могут быть невидимы или малозаметны для неспециалиста, таких как логи, файлы cookie, кэшированные данные, записи о транзакциях и метаданные.

Специалист, как правило, обращает внимание на важные обстоятельства, связанные с поиском, обнаружением и анализом цифровых следов и вещественных доказательств, даёт пояснения по поводу выполняемых им действий, обеспечивая надлежащую процессуальную фиксацию и допустимость полученных результатов в качестве доказательств. В сложных ситуациях, когда требуется компетенция в различных областях знаний, таких как анализ блокчейна, выявление схем отмывания денег, криптографический анализ или экспертиза программного обеспечения, целесообразно привлекать к осмотру нескольких специалистов, компетентных в соответствующих областях. Это позволяет обеспечить комплексный и всесторонний подход к расследованию, повышая вероятность установления действительных обстоятельств и привлечения виновных к ответственности[410].

Участие подозреваемого в осмотре места происшествия в контексте расследования криптовалютных преступлений представляется целесообразным в ряде специфических ситуаций. Во-первых, привлечение лица, предположительно причастного к криминальной деятельности, может оказаться необходимым для установления местонахождения виртуальных активов, кодов доступа к криптокошелькам, оборудования для майнинга или иных объектов, имеющих доказательственное значение, информация о которых не была установлена следствием иным путем. Во-вторых, непосредственное участие подозреваемого в процессе фиксации цифровой обстановки, идентификации криптокошельков и транзакций способствует обеспечению объективности следственного действия и минимизирует риски обжалования результатов осмотра в дальнейшем, особенно

---

[410] *Сущенко, С. А.* Недопустимость доказательств в уголовном процессе Российской Федерации и государств англо-американской и романо-германской правовых семей : учебное пособие / С. А. Сущенко, В. Ф. Васюков, А. Г. Волеводз. – Москва : Общество с ограниченной ответственностью "Издательство Прометей", 2022. – 466 с.

в случаях, когда обстоятельства преступления связаны со сложными техническими аспектами обращения криптовалют.

При этом организация осмотра места происшествия с участием подозреваемого требует строгого соблюдения мер предосторожности, направленных на предотвращение сокрытия, уничтожения или изменения цифровых следов, а также на исключение возможности несанкционированного доступа к криптоактивам. Необходима предварительная оценка рисков, связанных с возможным использованием участия подозреваемого для противодействия расследованию, а также планирование технических и тактических мероприятий для нейтрализации этих рисков.

Привлечение подозреваемого к участию в осмотре места происшествия, несмотря на кажущуюся целесообразность, далеко не всегда является оптимальным вариантом в тактическом плане. В ряде случаев, особенно при рассмотрении дел, связанных с незаконным оборотом наркотиков, мошенничеством, финансированием терроризма, участие подозреваемого в первоначальном осмотре может существенно снизить эффективность последующих следственных действий, в частности допроса. После ознакомления с обстановкой на месте происшествия и непосредственного участия в ее исследовании и фиксации обвиняемый утрачивает способность демонстрировать знание специфических деталей и обстоятельств, характерных исключительно для лица, совершившего преступление. Иными словами, предварительное участие в осмотре ставит под сомнение возможность выявления уникальной информации, касающейся как непосредственно события преступления, так и особенностей материальной обстановки, что является ключевым элементом для установления причастности к содеянному.

При этом участие подозреваемого в осмотре цифровых устройств или записей транзакций до проведения полноценного анализа может привести к сокрытию или искажению информации, а также затруднить выявление связей между различными транзакциями и участниками. В частности, показания потерпевшего, касающиеся установления места совершения преступления,

действий с электронными устройствами, особенностями взаимодействия со злоумышленниками, оказывают существенное влияние на целевую направленность поиска криминалистически значимых следов и объектов[411].

В целях обеспечения объективности и предотвращения неточностей в процессе осмотра целесообразно осуществлять предварительную фиксацию информации, предоставленной потерпевшим, в рамках процессуальных документов (заявление о преступлении, объяснение, полученные данные от операторов связи и провайдеров) до начала непосредственного осмотра места происшествия. Данная процедура проводится с целью обеспечения последующей возможности сопоставления представленных данных с материальной обстановкой, зафиксированной на месте происшествия, а также для оценки степени соответствия между устными показаниями и объективными обстоятельствами, установленными в ходе осмотра.

Процедура *осмотра смартфона*, изъятого у подозреваемого, осуществляется в соответствии с нормами уголовно-процессуального законодательства (ст. 176 УПК РФ) и предполагает применение специализированных технических средств для фиксации полученных результатов.

Во-первых, осуществляется визуальная оценка внешних признаков устройства, включая цвет, наличие повреждений, а также других видимых отличий. SIM-карта (при наличии физического слота) извлекается с последующей фиксацией ее идентификационных данных, таких как номер, оператор связи и стандарт связи. При наличии технической возможности фиксируется IMEI устройства. По верному суждению С.Ю. Скобелина дополнительно следует обратить внимание на наличие защитных пленок, чехлов

---

[411] *Титов, А. А.* Процессуальные и тактические проблемы изъятия электронных носителей и копирования информации при расследовании преступлений с использованием криптовалюты / А. А. Титов, В. Ф. Васюков // Российский следователь. – 2023. – № 2. – С. 23-27.

или других аксессуаров, которые могут указывать на повышенное внимание к безопасности устройства[412].

Во-вторых, предпринимается попытка включить устройство для оценки его работоспособности и функциональных возможностей. В случае успешной активации проверяется подключение к сети оператора связи и доступность основных функций устройства. При обнаружении зашифрованных разделов или приложений принимаются меры для их разблокировки или фиксации факта их наличия[413].

В-третьих, на что уместно обращает внимание Г.З. Гаспарян, проводится исследование настроек с целью получения информации об используемых SIM-картах (включая eSIM) и связанных с ними абонентских номерах[414]. Осуществляется документирование абонентских номеров, идентифицированных как используемые на исследуемом устройстве. При обнаружении настроек VPN, прокси-серверов или иных средств, обеспечивающих анонимность, необходимо зафиксировать эти данные, поскольку они могут быть связаны с сокрытием криптовалютных транзакций[415].

В-четвёртых, изучаются приложения, установленные на устройстве. Особое внимание уделяется наличию мессенджеров, социальных сетей, приложений для управления финансами, в том числе криптовалютными кошельками, а также других приложений, используемых для коммуникации и обмена информацией, что обусловлено их распространённостью среди лиц,

---

[412] *Скобелин, С. Ю.* Об использовании специальных знаний при исследовании смартфонов / С. Ю. Скобелин // Судебные экспертизы в уголовном процессе: теория и практика : Материалы II Всероссийской научно-практической конференции, Москва, 19 октября 2023 г. – Москва: Московская академия следственного комитета, 2024. – С. 187-191.

[413] *Галушин П.В., Карлов А.Л.* Сведения об операциях с криптовалютами (на примере биткойна) как доказательство по уголовному делу // Ученые записки Казанского юридического института МВД России. – 2017. – Т. 2 (4). – С. 91.

[414] *Гаспарян, Г.З.* Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : дис. … канд. юрид. наук / Гаспарян Гурген Зорикович. – 2021. – 300 с.

[415] Приговор Мотовилихинского районного суда г. Перми от 19 декабря 2023 г. по делу № 1-500/2023 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

совершающих противоправные деяния[416]. При обнаружении приложений для работы с криптовалютами (кошельки, биржи, обменники) необходимо уделить им особое внимание. Также следует обратить внимание на приложения для двухфакторной аутентификации (2FA), поскольку они часто используются для защиты доступа к криптовалютным аккаунтам[417].

При этом особое внимание следует обращать на фиксации данных всех профилей, авторизованных в приложении, включая псевдонимы (никнеймы), идентификаторы пользователей и привязанные абонентские номера или адреса электронной почты[418]. При анализе приложений для работы с криптовалютами целесообразно зафиксировать и все связанные с ними идентификаторы (адреса кошельков, API-ключи), а также историю авторизаций.

В ходе осмотра следователю необходимо тщательно изучить список чатов, групп и каналов, в которых состоит профиль пользователя. Далее в рамках идентификации потенциально значимой информации фиксируются названия (идентификаторы) чатов, имеющих криминалистическое значение, например, связанных с незаконным оборотом наркотических средств, изготовлением поддельных документов, обсуждением криптовалютных афер, фишингом и т.п. В этом же ключе рассуждают В. Б. Вехов и А. Б. Смушкин[419].

С целью определения степени вовлеченности пользователя в противоправную деятельность устанавливается факт администрирования профилем каких-либо групп или каналов, что может служить свидетельством его роли в организации или координации преступной деятельности. При обнаружении чатов, тематически связанных с криптовалютой, особенно важно

---

[416] Приговор Кировского районного суда г. Саратова от 9 июля 2024 г. по делу № 1-294/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[417] Апелляционное определение Московского городского суда от 11.07.2024 по делу № 10-12074/2024; апелляционное определение Московского городского суда от 08.04.2024 по делу № 10-3606/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[418] Приговор Промышленного районного суда г. Курска от 20 августа 2024 г. по делу № 1-121/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[419] *Вехов, В. Б.* Отдельные аспекты следственного осмотра некоторых электронных устройств / В. Б. Вехов, А. Б. Смушкин // Вестник Саратовской государственной юридической академии. – 2024. – № 4(159). – С. 230-236.

обращать внимание на обсуждение операций с криптовалютами, инвестиционных стратегий, а также любых жалоб на мошенничество или на кражу цифровых активов. Подобные сведения могут указывать на причастность пользователя к конкретным криминальным схемам и служить основанием для дальнейшего более глубокого анализа.

Осмотру подвергаются сообщения, содержащие сведения о координации противоправной деятельности, распределении ролей и обязанностей между участниками группы, совершении финансовых операций, связанных с противоправной деятельностью, использовании поддельных документов и иных средств совершения противоправных деяний, а также взаимодействии с другими участниками организованных групп[420].

В целях выявления специфических признаков криптопреступлений при анализе переписки необходимо уделять приоритетное внимание обсуждению криптовалютных транзакций, адресам криптографических кошельков, криптовалютным биржам и обменным сервисам, а также любым упоминаниям о способах мошенничества, легализации доходов, полученных преступным путем, или уклонении от уплаты налогов. Указанная рекомендация обусловлена тем, что эти элементы выступают в качестве значимых индикаторов деятельности, опосредованной использованием криптографических технологий, и позволяют установить взаимосвязь между цифровыми активами и противоправными действиями. Например, в ходе расследования случаев финансирования терроризма анализ переписки позволял установить факты перевода криптовалюты на анонимные кошельки, используемые террористическими организациями для закупки оборудования и финансирования подпольных ячеек.

В-шестых, на что небезосновательно обращает внимание О.Н. Тисен, просматриваются изображения, видеозаписи и аудиозаписи, хранящиеся на устройстве, с целью выявления информации, имеющей криминалистическое

[420] Приговор Октябрьского районного суда г. Мурманска от 13 сентября 2023 г. по делу № 1-453/2022; приговор Новомосковского городского суда от 29 июля 2024 г. по делу № 1-174/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

значение[421]. Как правило, особое значение приобретают фотографии документов, переписка, скриншоты, записи разговоров, а также скриншоты криптовалютных кошельков, QR-коды для криптовалютных адресов, данные о транзакциях и любые другие данные, связанные с криптовалютой.

В-седьмых, вся информация, полученная в ходе осмотра, подлежит тщательному протоколированию с использованием средств фото- и видеофиксации. Составляется подробный протокол осмотра, содержащий описание всех проведенных действий, выявленных фактов и результатов анализа. В протокол включаются скриншоты, фотографии, а также подробное описание выявленных криптовалютных адресов, транзакций и иных данных, имеющих отношение к криптопреступлениям.

Таким образом, от того, насколько пристально будет проведен осмотр смартфона, изъятого у подозреваемого, зачастую зависит возможность обнаружения цифровых следов, связывающих подозреваемого с криптовалютными транзакциями и другими участниками преступной схемы.

Общепринято считать, что одним из основных следственных действий, производящихся в ходе предварительного расследования, является допрос (ст. 189 УПК РФ)[422]. Приведенный постулат всецело касается преступлений, совершаемых в отношении и с использованием криптовалюты.

Допрос подозреваемого представляет собой важный этап в расследовании, требующий применения специальных знаний и тактических подходов, адаптированных к специфике данной области. В отличие от традиционных видов преступности криптовалютные преступления характеризуются высоким уровнем технологической сложности, анонимности транзакций и трансграничным характером, что предопределяет необходимость тщательной подготовки и осознанного применения методов допроса.

---

[421] *Тисен, О. Н.* Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют / О. Н. Тисен // Уголовное право. – 2024. – № 3(163). – С. 69-80.

[422] *Гриненко, А. В.* Взаимодействие уголовно-процессуальной и криминалистической наук: труды профессора Р.С. Белкина и современность / А. В. Гриненко // Вестник криминалистики. – 2022. – № 3(83). – С. 11-14.

Прежде всего, следователь должен обладать знаниями в области функционирования блокчейн-технологий, механизмов криптографической защиты и специфики функционирования различных криптовалютных платформ и кошельков. В процессе подготовки к допросу необходимо собрать максимально полную информацию о подозреваемом, включая его технические навыки, финансовую историю, связи с криптовалютным сообществом и возможные мотивы совершения преступления. Анализ публично доступных данных, социальных сетей и форумов, посвященных криптовалютам, может предоставить ценные сведения о деятельности и интересах подозреваемого[423].

В ходе допроса следует использовать специализированную терминологию, демонстрируя компетентность в области криптовалют и затрудняя возможность предоставления ложных или уклончивых ответов. Примером может служить вопрос: «Каким образом вы осуществляли транзакции с использованием миксеров криптовалют?» или «Объясните, пожалуйста, принципы работы протокола CoinJoin[424] и его применение для сокрытия связей между транзакциями в блокчейне». Естественно, что при этом следует избегать

---

[423] *Мазуров, И.Е.* Методика расследования хищений, совершенных с использованием интернет - технологий : автореф. дис. … канд. юрид. наук / Мазуров Игорь Евгеньевич. – Ростов-на-Дону, 2017. – 24 с.

[424] CoinJoin, что в переводе с английского означает «соединение монет», представляет собой одну из наиболее распространенных технологий анонимизации транзакций в сети Биткоин, основанную на принципе микширования. Технология CoinJoin, предложенная разработчиком Грегори Максвеллом в 2013 году, позволяет объединять транзакции нескольких пользователей в одну, перемешивая выходы общей транзакции таким образом, что отслеживание отправителя и получателя каждого конкретного платежа становится невозможным. До 2024 года фигуранты использовали ряд популярных сервисов, реализующих протокол CoinJoin, таких как JoinMarket, Wasabi и Samourai, каждый из которых отличался особенностями создания транзакций и функциональными возможностями. Однако в апреле 2024 года сервис Samourai был заблокирован правоохранительными органами, а впоследствии сервис Wasabi прекратил поддержку функции координации CoinJoin. Тем не менее, возможность использования Wasabi для проведения CoinJoin сохраняется при использовании альтернативных сервисов-координаторов. *Prado-Romero, M.A.* Discovering Bitcoin Mixing Using Anomaly Detection / M.A. Prado-Romero, C. Doerr, A. Gago-Alonso // Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications. CIARP 2017. Lecture Notes in Computer Science, vol 10657 / ed. by M. Mendoza, S. Velastín. – Cham: Springer, 2018. – DOI: https://doi.org/10.1007/978-3-319-75193-1_64

наводящих вопросов, поскольку это приводит к недопустимости результатов допроса.

Важным аспектом является выявление и анализ цифровых следов, оставленных подозреваемым в сети Интернет. Сюда относится анализ IP-адресов, используемых для доступа к криптовалютным платформам, отслеживание транзакций в блокчейне и выявление связей с другими участниками сети[425].

При допросе лица, подозреваемого в совершении мошеннических действий, связанных с использованием криптовалютных бирж и потенциально сопряженных с созданием и/или применением вредоносного программного обеспечения (ПО), особое внимание уделяется установлению уровня его компетенций в области программирования, а также опыта разработки и применения специализированного ПО, позволяющего совершать противоправные деяния в цифровой среде. В частности, необходимо выяснить, обладает ли допрашиваемый знаниями языков программирования высокого уровня, используемых для создания смарт-контрактов и автоматизированных торговых алгоритмов, которые впоследствии могут быть использованы для манипулирования рынком или хищения активов. Важно установить, имеет ли он опыт работы с криптографическими протоколами и методами обеспечения безопасности информации, а также знаком ли с архитектурой и принципами функционирования блокчейн-технологий.

Далее в ходе допроса необходимо детально выяснить обстоятельства, способствовавшие совершению преступления, включая факты нарушения регламентов доступа к учетным записям на криптобиржах, несанкционированного использования программных средств и/или аппаратного обеспечения, а также способы преодоления систем защиты информации.

---

[425] *Васюков, В. Ф.* Противодействие преступлениям в сфере незаконного оборота наркотиков, совершаемым с использованием информационно-телекоммуникационных технологий / В. Ф. Васюков, К. К. Клевцов, В. И. Малик. – Москва : Общество с ограниченной ответственностью "Издательство Прометей", 2023. – 468 с.

Например, если мошенничество было совершено с использованием фишинговых атак, следует установить, какие именно методы социальной инженерии были применены, какие уязвимости в системах безопасности были использованы и какие меры были предприняты для сокрытия следов преступления. Примером из практики может служить случай, когда злоумышленник, обладающий знаниями в области криптографии и опытом разработки вредоносного программного обеспечения, создал и распространил фишинговый сайт, имитирующий интерфейс популярной криптобиржи. В результате обмана пользователи вводили свои учетные данные на поддельном сайте, что позволило злоумышленнику получить доступ к их аккаунтам и вывести криптовалютные активы на свои кошельки.

Кроме того, при допросе обвиняемого крайне важно установить алгоритм функционирования использованного вредоносного программного обеспечения, а также характер его воздействия на информационные системы криптобирж и/или кошельки пользователей. Необходимо выяснить, какие типы данных были подвергнуты несанкционированному уничтожению, блокированию, модификации или копированию и какие конкретно последствия это повлекло за собой (например, нарушение работы торговой платформы, потеря активов пользователями). В случае использования эксплойтов[426] для взлома смарт-контрактов следует установить, какие именно уязвимости были использованы и каким образом злоумышленнику удалось обойти механизмы защиты. Примером из практики может служить случай, когда хакер, обнаружив уязвимость в смарт-контракте DeFi-протокола, смог вывести значительную сумму криптовалюты на свой кошелек, что привело к серьезным финансовым потерям для инвесторов. Важным аспектом является выяснение мер, которые могли бы быть наиболее эффективны для предотвращения подобных инцидентов в будущем, что может

[426] *Эксплойт* (англ. exploit, эксплуатировать) – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

включать рекомендации по улучшению безопасности программного обеспечения, усилению контроля доступа и обучению пользователей правилам безопасного поведения в цифровой среде.

Особое внимание следует уделить выяснению масштаба и серийности преступной деятельности. Даже если отдельные эпизоды мошенничества кажутся незначительными по объему похищенных средств, совокупный ущерб от действий злоумышленника может быть значительным. Установление серийности преступлений позволит более точно оценить тяжесть содеянного и выявить возможные связи с другими преступными группами[427].

В процессе допроса также целесообразно применять технические средства для демонстрации принципов работы использованного вредоносного ПО и визуализации алгоритмов его функционирования. Это позволит допрашиваемому лучше осознать последствия своих действий и может способствовать получению более полных и достоверных показаний.

При проведении *допроса потерпевшего* в рамках расследования мошеннических действий, совершенных с использованием криптовалюты, первостепенной задачей следствия является установление обстоятельств, потенциально способствующих идентификации субъекта преступной деятельности. Данный процесс предполагает комплексный анализ значимых данных, ориентированный на выявление причинно-следственных связей, позволяющих сузить круг вероятных подозреваемых.

В частности, отдельного внимания заслуживает установление факта предварительного знакомства между потерпевшим и предполагаемым злоумышленником. При подтверждении наличия такого знакомства необходимо детализировать его характер, включая определение продолжительности, интенсивности и контекста взаимодействия сторон. Ключевое значение приобретает выяснение обстоятельств знакомства, в том числе сведения о лицах,

---

[427] *Коломинов, В.В.* Расследование мошенничества в сфере компьютерной информации : научно-теоретическая основа и прикладные аспекты первоначального этапа : автореф. дис. … канд. юрид. наук / Коломинов Вячеслав Валентинович. – Краснодар, 2017. – 25 с.

присутствовавших при установлении первичного контакта, а также подробности о каналах коммуникации, используемых для последующего взаимодействия.

Например, в практике расследования случаев мошенничества с криптовалютой нередко встречаются ситуации, когда потерпевший и злоумышленник знакомятся в специализированных онлайн-сообществах, посвященных инвестициям в цифровые активы. В таких случаях установление никнеймов, IP-адресов и иных идентификационных данных, связанных с аккаунтом злоумышленника, может стать отправной точкой для дальнейших следственных действий. Другим распространенным сценарием является использование социальных сетей для установления доверительных отношений с потерпевшим. В данном случае детальный анализ профиля злоумышленника, его круга общения, а также содержания переписки с потерпевшим, может предоставить ценную информацию о личности преступника, его мотивах и способах совершения преступления.

В ряде случаев потерпевшие указывают на наличие посредников, содействовавших установлению контакта со злоумышленником. Например, потерпевший может быть введен в заблуждение лицом, позиционирующим себя как эксперт в области криптовалют, который рекомендует инвестировать средства в определенный проект, являющийся заведомо мошенническим. В таких ситуациях допрос посредника, а также исследование его связей и финансовых операций, может позволить выявить организаторов преступной схемы, а также установить роль каждого из участников.

Таким образом, подводя итог настоящего параграфа, стоит отметить следующее.

1. Современная криминалистическая наука, сталкиваясь с вызовами цифровой трансформации преступной деятельности, актуализирует необходимость интеграции традиционных методов расследования с инновационными технологическими подходами, что обусловлено ростом технологической оснащенности преступных элементов и ситуационным усложнением механизмов противоправных деяний.

2. Эффективность расследования преступлений, связанных с криптовалютой, напрямую коррелирует с уровнем системности криминалистической деятельности, предполагающей синтез организационного, тактического и технического обеспечения. Ключевая роль в данном контексте отводится осмотру, трансформирующемуся в условиях цифровой среды: его объектом становится не только физическое пространство, но и виртуальные платформы, блокчейн-транзакции и электронные устройства, что требует переосмысления традиционных принципов своевременности, полноты и планомерности.

3. Технологическая сложность криптопреступлений, характеризующихся анонимизацией транзакций и использованием децентрализованных систем, обусловливает необходимость привлечения специалистов в области блокчейн-аналитики и кибербезопасности, чьи знания позволяют «декодировать» цифровые следы и устанавливать причинно-следственные связи между транзакциями и лицами, причастными к преступной деятельности. При этом процесс осмотра электронных носителей информации, таких как смартфоны и компьютеры, демонстрирует возрастающую значимость протоколирования метаданных, анализа установленных приложений и реконструкции цифровых поведенческих закономерностей.

4. Особое методологическое значение приобретает дифференциация тактических подходов к допросу участников процесса. Если взаимодействие с подозреваемыми требует глубокого погружения в технические аспекты криптографических протоколов и методов обхода систем безопасности, то допрос потерпевших фокусируется на реконструкции коммуникативных каналов установления контакта с злоумышленниками, включая анализ социальных сетей и специализированных форумов. При этом выявление серийности преступлений и трансграничного характера операций подчеркивает необходимость гармонизации международных стандартов взаимодействия правоохранительных органов.

§ 3. Тактика проведения последующих следственных действий при расследовании преступлений, совершаемых в отношении и с использованием криптовалюты

Специфика проведения последующих следственных действий при расследовании рассматриваемых преступлений предопределена общей сущностью и задачами последующего этапа расследования, а также механизмом совершения данных посягательств. Типичным следственным действием, осуществляемым на последующем этапе расследования преступлений, совершаемых в отношении и с использованием криптовалют, является *обыск* по месту жительства лица или осуществления им незаконной деятельности.

Обыск представляет собой принудительное следственное действие, направленное на обнаружение и изъятие объектов, имеющих доказательственное значение для уголовного дела[428]. В контексте расследования рассматриваемых нами преступлений обыск приобретает особую значимость, обусловленную спецификой цифровых активов и их хранения. По верному замечанию Д.Э. Алехина, «основная сложность в делах, связанных с криптовалютами, заключается в необходимости понимания технических тонкостей работы с цифровыми активами и их защиты»[429].

При расследовании преступлений, связанных с криптовалютой, обыск проводится с целью обнаружения цифровых кошельков, аппаратных носителей, компьютеров и иных устройств, содержащих информацию о транзакциях, ключах доступа и иных данных, позволяющих установить причастность лица к совершению преступления, а также проследить движение криптовалютных активов.

Основанием проведения обыска могут стать данные, полученные в результате оперативно-розыскных мероприятий, исследования транзакций в

---

[428] *Гриненко, А. В.* Криминалистика : учебник / А. В. Гриненко, В. А. Дударев, С. С. Маевский. – Москва : Общество с ограниченной ответственностью "Проспект", 2025. – 432 с.

[429] *Алехин, Д. Э.* Особенности процессуальных действий по уголовным делам в сфере оборота цифровой валюты // Российская юстиция. – 2024. – № 7. – С. 30-38.

блокчейне, показаний свидетелей и потерпевших. Например, если в ходе расследования мошеннической схемы с использованием криптовалюты установлено, что подозреваемый использует определённый аппаратный кошелёк для хранения похищенных средств, то следователь вправе вынести постановление о проведении обыска по месту жительства подозреваемого с целью обнаружения и изъятия данного устройства.

Следует акцентировать внимание на значимости сведений, которые могут быть предоставлены подразделением финансовой разведки. Так, австралийско полицией был проведен обыск на основании разведданных, предоставленных подразделением финансовой разведки Австралии (AUSTRAC), которым были выявлены подозрительные транзакции через незарегистрированный криптовалютный банкомат, установленном в торговом центре Брейбрука. Анализ блокчейн-транзакций, проведенный в рамках оперативно-розыскных мероприятий, позволил установить связь между владельцами банкомата и незаконными операциями, что стало правовой основой для возбуждения уголовного дела по ст. 76A(5) Закона о борьбе с отмыванием денег и ст. 400.9 Уголовного кодекса Австралии[430].

В следственной практике встречаются ситуации, когда в ходе обыска обнаруживаются не только цифровые активы, но и документы, подтверждающие участие подозреваемого в незаконной деятельности, например переписка с соучастниками, договоры о предоставлении услуг по обналичиванию криптовалюты, а также электронные таблицы с информацией о транзакциях и доходах. Особую сложность представляет обыск, проводимый в отношении лиц, использующих методы анонимизации и сокрытия информации, такие как VPN, Tor и другие средства шифрования. В таких случаях следователю необходимо обладать специальными знаниями и навыками для выявления фактов использования таких методов.

---

[430] Man arrested as part of cryptocurrency investigation // AUSTRAC. – URL: https://www.austrac.gov.au/about-us/media-release/man-arrested-cryptocurrency-investigation (дата обращения: 15.02.2025).

Важным аспектом является обеспечение сохранности изъятых цифровых носителей и данных, а также предотвращение несанкционированного доступа к ним. В связи с этим целесообразно привлекать к участию в обыске специалистов в области исследования следов блокчейна, в том числе из специализированных организаций[431].

При проведении обыска ходе расследования преступлений, связанных с криптовалютой, подлежат изъятию не только объекты, непосредственно указывающие на совершённое деяние, но и предметы, документы, свидетельствующие о подготовке к преступлению или указывающие на потенциальные места хранения доказательственной информации, а также объекты, пригодные для сравнительных исследований. В частности, при наличии оснований полагать, что необходимо провести исследование цифровой подписи или идентификацию криптокошелька, возможно изъятие устройств и документов, содержащих образцы ключей, данные о транзакциях или иные релевантные идентификаторы[432].

Для обеспечения эффективности следственного действия и полноты изъятия потенциальных источников доказательств поисковая группа вправе вскрывать запертые помещения и хранилища, например, в целях обнаружения майнингового оборудования. Выбранный способ вскрытия, а также все обстоятельства его применения должны быть подробно отражены в протоколе обыска, чтобы обеспечить фиксацию процессуальных действий и защиту прав участников следственного действия.

---

[431] *Васюков, В. Ф.* Расследование дел о сбыте наркотиков с использованием мессенджеров и криптовалюты / В. Ф. Васюков // Уголовный процесс. – 2019. – № 9(177). – С. 44-49.

[432] Необходимо отметить, что в соответствии с поправками, внесенными в Положение о полномочиях на обыск и изъятие имущества Англии и Уэльса, сотрудники правоохранительных органов наделены полномочиями на проведение обыска не только с целью обнаружения и изъятия криптовалютных активов, но и для поиска объектов, которые, по обоснованному мнению субъектов обыска, могут содержать информацию, способствующую обнаружению таких активов. См.: CODE OF PRACTICE ISSUED UNDER SECTION 47S OF THE PROCEEDS OF CRIME ACT 2002. Search, Seizure and Detention of Property (England and Wales). April 2024. ISBN 978-1-5286-4655-0. – URL: https://www.gov.uk/government/publications/search-seizure-and-detention-of-property-england-and-wales/code-of-practice-issued-under-section-47s-of-the-proceeds-of-crime-act-2002-search-seizure-and-detention-of-property-england-and-wales-accessible (дата обращения: 30.03.2025).

Обыск как одно из наиболее ресурсозатратных и психологически напряжённых следственных действий требует от следователя высокой степени концентрации и уверенности в положительном исходе. Это особенно актуально при расследовании преступлений, связанных с криптовалютой, где специфика цифровых активов и методов их сокрытия предъявляет повышенные требования к подготовке и тактике проведения обыска. Подготовка к обыску в рамках «крипторасследований» включает два взаимосвязанных этапа: предварительный анализ и подготовку к поисковым действиям на месте. На этапе предварительного анализа следователю необходимо тщательно изучить материалы уголовного дела, включая данные о транзакциях в блокчейне, информацию о подозреваемых и их связях, а также специфические методы сокрытия криптоактивов.

Например, в случае расследования легализации преступных доходов с помощью криптовалютных миксеров анализ транзакций может выявить адреса кошельков, используемых подозреваемыми. Также важно собрать сведения об индивидуальных особенностях обыскиваемого лица, его технологической осведомлённости и возможных местах хранения криптографических ключей, аппаратных кошельков или seed-фраз. Например, при расследовании финансирования терроризма с помощью криптовалюты следователь должен учитывать возможность использования подозреваемыми стеганографии для сокрытия информации в цифровых изображениях или текстовых файлах.

Второй этап подготовки начинается с момента прибытия на место обыска и включает оценку обстановки, установление контроля над территорией и предварительный осмотр помещений. Целью этого этапа является предотвращение уничтожения или сокрытия улик. Например, практике известны случаи, когда подозреваемые пытались физически уничтожить аппаратные кошельки или зашифрованные USB-накопители, содержащие криптографические ключи[433]. В связи с этим перед началом активных поисковых

[433] *Старостенко, Н.И.* Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных

действий необходимо обеспечить блокировку доступа к сети Интернет, чтобы предотвратить удалённое уничтожение данных или перемещение криптоактивов.

Тщательная предварительная подготовка играет определяющую роль в успешном проведении обыска, особенно при расследовании преступлений, связанных с криптовалютой. Анализ собранной информации позволяет определить оптимальное время начала обыска, что критически важно, учитывая волатильность цифровых активов и возможность их быстрого перемещения. Например, данные о сетевой активности подозреваемого могут указывать на наиболее вероятное время его присутствия за компьютером и доступа к криптокошелькам. Кроме того, предварительный этап включает в себя решение вопросов тактико-технического обеспечения, таких как использование специализированного программного обеспечения для анализа блокчейна, обнаружения скрытых криптокошельков или восстановления удалённых данных. Определение оптимальной численности и персонального состава следственно-оперативной группы, включая специалистов в области компьютерной криминалистики и оперативных сотрудников, также является неотъемлемой частью подготовки. При этом распределение обязанностей, установление способов связи и взаимодействия между членами группы как на месте обыска, так и за его пределами обеспечивают скоординированные и эффективные действия.

Важным аспектом является разработка мер по охране места обыска, предотвращению утечки информации и обеспечению безопасного проникновения группы на объект, особенно при наличии признаков возможного противодействия со стороны обыскиваемых лиц. В связи с этим оперативно-розыскная информация, полученная до начала обыска, приобретает исключительное значение. Примером может служить информация о наличии у подозреваемого средств контрнаблюдения или попыток уничтожения цифровых следов.

технологий : дис. … канд. юрид. наук / Старостенко Нина Игоревна. – Краснодар, 2023. – 230 с.

Составление тактического плана проведения обыска является важнейшим элементом подготовки. Этот план должен содержать систематизированное описание последовательности действий, вспомогательные мероприятия по обеспечению эффективности поиска и прогнозируемые сценарии развития ситуации. Например, в плане может быть предусмотрено одновременное изъятие нескольких электронных устройств, чтобы предотвратить удалённое уничтожение данных. Также в плане должны быть учтены требования к фиксации изымаемых данных и обеспечению их целостности. Следует отметить, что объём подготовительных мероприятий зависит от конкретной следственной ситуации, однако стремление к их максимально полной реализации целесообразно в каждом случае, поскольку это напрямую влияет на общий результат.

Обобщая практику проведения обысков по изучаемой категории дел, отметим, что при их подготовке и осуществлении следователю необходимо особое внимание уделять установочным и ориентирующим данным о характере и признаках разыскиваемых цифровых активов, определяемые по их наименованию, количеству, размеру (объему данных), используемым криптографическим ключам, а также индивидуальным идентификаторам транзакций (хешам). Источником таких данных могут служить процессуальные документы, такие как протоколы допросов свидетелей и потерпевших, заключения экспертов в области блокчейн-технологий и криптографии, а также материалы, полученные в ходе оперативно-розыскных мероприятий, направленных на установление движения цифровых активов и выявление лиц, их контролирующих. Для визуализации и облегчения идентификации разыскиваемых криптоактивов можно использовать инструменты анализа блокчейна, позволяющие отслеживать транзакции и визуализировать сети взаимосвязанных адресов. В качестве примера можно привести использование программного обеспечения «Прозрачный блокчейн», позволяющего отслеживать движение криптовалюты, связанной с незаконной деятельностью, и идентифицировать связанные с ней сервисы и пользователей.

Информация о характере и признаках искомых криптоактивов позволяет выдвигать розыскные версии о наиболее вероятных местах их сокрытия или использования, принимая во внимание особенности функционирования блокчейн-технологий и криптографических протоколов. Следует учитывать обратную зависимость между сложностью доступа к цифровому активу (например, требованием наличия приватного ключа) и потенциальными способами его сокрытия: чем сложнее доступ, тем менее вероятно прямое сокрытие актива и тем более вероятно сокрытие информации, необходимой для доступа к нему (приватного ключа, seed-фразы и т.п.).

Важное значение имеет осведомлённость следователя психологической характеристике лиц, вовлечённых в криптопреступления, с учётом их личностных особенностей, профессиональных навыков в области информационных технологий, уровня интеллектуального развития, склонности к использованию анонимных сервисов и инструментов обеспечения конфиденциальности. Например, лицо, обладающее продвинутыми навыками в области криптографии, может использовать сложные методы сокрытия приватных ключей, такие как стеганография (сокрытие информации в цифровых изображениях или других файлах) либо мультисигнатурные кошельки, требующие подтверждения транзакции несколькими ключами.

Человек с более низким уровнем технической подготовки может хранить приватные ключи в незащищённых текстовых файлах или использовать упрощённые сервисы для хранения и обмена криптовалютами, что упрощает их обнаружение в ходе следственных действий. В качестве примера можно привести случай, когда подозреваемый в отмывании криптовалюты хранил приватные ключи в зашифрованном файле на своём компьютере, полагая, что это обеспечит достаточную защиту. Однако благодаря использованию методов криптоанализа и прочтению пароля следователям удалось расшифровать файл и получить доступ к криптоактивам.

Данные, полученные в ходе анализа цифровых следов и поведенческих факторов субъекта, позволяют выдвигать версии о вероятном местонахождении

и способах сокрытия активов, в том числе криптовалютных, представляющих особый интерес в контексте расследования.

Знание психологических особенностей обыскиваемого, включая членов его семьи и лиц, проживающих совместно, является важным элементом тактического планирования обыска. Прогнозирование возможного сопротивления или попыток уничтожения искомых активов, основанное на анализе поведенческих проявлений, позволяет следователю принять превентивные меры и оптимизировать процесс обыска.

Эти данные позволяют предположить возможное место хранения и способ сокрытия искомых объектов, что особенно актуально, если использовались малогабаритные предметы. Известен случай из практики, когда субъект, профессиональный водитель, использовал автомобильную камеру в качестве тайника: разрезав резину, он поместил внутрь оружие и боеприпасы, после чего аккуратно заклеил разрез и накачал камеру воздухом. Подготовленная таким образом камера была установлена на автомобиль, помещённый в гараж, что обеспечило эффективную маскировку. Знание поведенческих особенностей, психологических черт обыскиваемого, членов его семьи и других лиц, проживающих совместно, играет важную роль в прогнозировании вероятности оказания сопротивления следственным действиям или попыток уничтожить улики. В то же время опора на психологические знания о характере субъекта, его привычках и навыках позволяет следователю использовать рефлексивное мышление, то есть способность предвидеть и анализировать действия обыскиваемого для выработки оптимальной тактики проведения обыска[434].

Эти данные позволяют предположить возможное место хранения и способ сокрытия искомых объектов, что особенно актуально, если по оперативной информации, в помещении может находиться майнинговое оборудование, используемое в незаконной деятельности.

---

[434] *Коломинов, В. В.* Расследование мошенничества в сфере компьютерной информации : научно-теоретическая основа и прикладные аспекты первоначального этапа : автореф. дис. … канд. юрид. наук / Коломинов Вячеслав Валентинович. – Краснодар, 2017. – 25 с.

Ключевым индикатором наличия таких объектов служит аномальное потребление электроэнергии, несоответствующее заявленному назначению помещения. Например, в жилых зонах или малых коммерческих объектах подобная нагрузка может проявляться через установку трансформаторных подстанций, не типичных для данной инфраструктуры, а также через использование кабелей большого сечения, рассчитанных на токи в сотни ампер. Эти элементы часто маскируются под легальные коммуникации, однако их расположение вне технических коридоров или наличие следов кустарного монтажа позволяет идентифицировать нарушения.

Тепловыделение, сопутствующее работе майнингового оборудования, требует организации мощных систем охлаждения, что становится еще одним маркером. В отличие от стандартных вентиляционных решений, в таких случаях наблюдаются самодельные конструкции, промышленные вентиляторы или модифицированные климатические установки, чья производительность многократно превышает потребности помещения, которое планируется обыскать.

Например, в ходе обыска, проведённого правоохранительными органами Республики Казахстан, было изъято 1257 единиц оборудования для майнинга криптовалют (ASIC-майнеров), промышленные охлаждающие вентиляторы и трансформаторная подстанция. Установлено, что в период с 2022 по май 2024 года данное оборудование обеспечивало функционирование майнинговой фермы, замаскированной под центр обработки данных, потребляя электроэнергию в объёме, сопоставимом с месячным потреблением одного жилого района крупного города[435].

Тепловые «аномалии» могут фиксироваться с помощью термографического оборудования, выявляющего зоны повышенной температуры на фасадах зданий или вентиляционных выходах, что особенно актуально при анализе заброшенных объектов или подвалов, где естественная циркуляция

[435] Имущество на 900 млн тенге конфисковали у трех казахстанцев за незаконный майнинг – URL: https://clck.ru/3LWhnS (дата обращения: 05.03.2025).

воздуха отсутствует. Дополнительным фактором является акустический шум — характерное гудение, создаваемое работой ASIC-майнеров и систем охлаждения, которое часто маскируется звукоизоляционными материалами.

Злоумышленники активно используют фальшивые архитектурные элементы, такие как двойные стены, зашитые гипсокартоном ниши или искусственные перегородки. Поэтому особого внимания заслуживают объекты с противоречивыми характеристиками — например, гаражи с усиленными бетонными полами, рассчитанными на нагрузку от оборудования, или склады без логистической инфраструктуры, но с повышенной охраной.

Применительно к расследованию преступлений, связанных с использованием криптовалюты, эти принципы приобретают особую значимость. Сложность отслеживания транзакций и возможность сокрытия активов в децентрализованных системах требуют от следователя не только знания технических аспектов работы блокчейн-технологий, но и понимания психологии криптопреступников.

Рассмотрим пример из следственной практики. В ходе расследования уголовного дела об отмывании денежных средств, полученных в результате кибермошенничества, следователи столкнулись с необходимостью обнаружить криптовалютные активы, принадлежащие подозреваемому. Анализ поведения подозреваемого, собранный в ходе оперативно-розыскных мероприятий, указывал на его склонность к конспирации и использованию сложных схем для сокрытия доходов. Основываясь на этой информации, следователи предположили, что подозреваемый мог использовать аппаратные кошельки для хранения криптовалюты, причём не в традиционных местах, а в специально оборудованных тайниках. Было принято решение провести обыск в гараже, где в скрытом отсеке, замаскированном под вентиляционную систему, был обнаружен аппаратный кошелёк со значительным количеством криптовалюты.

Еще одним примером является расследование дела об «отмывании» средств, полученных в результате кибервымогательства, в ходе которого следователи столкнулись с ситуацией, когда подозреваемый отрицал владение

какими-либо криптовалютными активами. Проанализировав его социальные сети и обнаружив увлечение старинными монетами, следователи применили рефлексивное мышление. Они предположили, что подозреваемый мог использовать аналогию с коллекционированием монет для сокрытия цифровых активов. В результате обыска в его доме был обнаружен физический носитель, замаскированный под старинную монету, на котором хранился зашифрованный файл с ключами доступа к криптовалютному кошельку, содержащему значительную сумму в биткоинах.

Предварительные данные о месте проведения обыска, включая тип помещения (квартира, частный дом, дача и т. д.), его планировку и особенности, полученные предпочтительно негласным путём в ходе оперативно-розыскных мероприятий, играют критически важную роль в эффективном планировании следственных действий, особенно с учетом того, что расследуются преступления, связанные с криптовалютами.

Эти сведения позволяют следователю не только оценить целесообразность использования фактора внезапности при проведении обыска, но и спрогнозировать объём поисковых мероприятий, их последовательность и необходимые ресурсы. Например, если в помещении, где предположительно хранятся ключи доступа к криптоактивам, установлена сложная система видеонаблюдения или сигнализации, можно заранее спланировать действия по нейтрализации этих систем и предотвратить уничтожение или сокрытие цифровых доказательств.

Анализ особенностей объекта обыска, включая подходы к нему, возможные варианты проникновения, наличие средств связи, а также факторов, потенциально осложняющих проведение обыска (например, домашние животные или больные члены семьи), является необходимым этапом подготовки. На основе этого анализа определяется оптимальный состав группы, в которую входят не только оперативники, но и специализированные эксперты в области компьютерной криминалистики и технические специалисты, способные

оперативно идентифицировать и изъять цифровые носители информации, содержащие криптовалютные ключи и данные о транзакциях.

Кроме того, предварительные данные позволяют определить перечень необходимых научно-технических средств, включая специализированное программное обеспечение для анализа криптотранзакций, оборудование для создания криминалистических копий цифровых носителей, а также инструменты для «обхода» криптографической защиты данных. Например, в практике расследования случаев отмывания денежных средств с использованием криптовалют нередко встречаются случаи, когда преступники используют сложные методы шифрования и сокрытия данных на цифровых носителях. В таких ситуациях наличие специализированного программного обеспечения для расшифровки и восстановления удаленных файлов имеет исключительное значение для получения доказательств[436].

В качестве примера можно привести случай расследования деятельности организованной преступной группы, занимавшейся нелегальной торговлей наркотическими веществами через даркнет-маркетплейсы и использовавшей криптовалюту Биткоин для проведения расчетов. В ходе первоначального собирания информации было установлено, что подозреваемый использует несколько ноутбуков, смартфонов и аппаратных криптокошельков для хранения криптовалютных активов и ведения учета операций. При проведении обыска в квартире подозреваемого были оперативно изъяты все цифровые устройства, а эксперты-криминалисты, привлеченные к участию в следственном действии, обеспечили создание криминалистических копий жестких дисков и флеш-памяти устройств, что позволило обнаружить информацию о транзакциях, адресах криптокошельков и переписку с другими участниками преступной группы.

В контексте расследования преступлений, совершаемых в отношении криптовалют, тактические методы обыска и поиска улик требуют особого

---

[436] *Колычева, А. Н.* Отдельные аспекты противодействия использованию криптовалют в преступных целях / А. Н. Колычева, В. Ф. Васюков // Криминалистика: вчера, сегодня, завтра. – 2025. – № 1(33). – С. 89-101.

внимания к цифровой среде и специфике хранимых данных. Применяемый подход должен учитывать как физические, так и виртуальные объекты, связанные с транзакциями, владением и управлением цифровыми активами.

В первую очередь следователь проводит обзорное обследование, которое включает в себя оценку как физической, так и цифровой инфраструктуры. Подобная деятельность может включать в себя осмотр компьютеров, серверов, мобильных устройств, а также жестких дисков, USB-накопителей и SIM-карт[437]. Например, в деле о незаконном майнинге криптовалюты обзорное обследование может выявить наличие высокопроизводительного компьютерного оборудования и необычно высоких счетов за электроэнергию, что указывает на возможную деятельность, связанную с майнингом.

Важность обнаружения электронных носителей информации определяется в примере из практики, получившего отражение в исследовании И.А. Безенкова. Так, в 2023 г. в Москве было возбуждено уголовное дело по ст. 290 УК РФ в отношении должностного лица правоохранительного органа по факту получения им взятки в виде биткоинов от фигурантов уголовного дела за то, чтобы не допустить наложение ареста на всю принадлежащую им цифровую валюту, хранящуюся на изъятых у них электронных носителях информации. При обыВ результате обыска у обвиняемого был изъят ноутбук, при осмотре которого обнаружены пароли для доступа к криптокошелькам с хранящейся на них валютой в размере более 1 тыс. BTC (их стоимость эквивалентна почти 24 млн долл. США)[438].

Следующим шагом является определение границ поиска и разделение его на участки. В контексте криптовалютных расследований это может означать разделение пространства (например офиса, квартиры) на зоны, соответствующие различным аспектам владения или использования криптовалюты: рабочие зоны,

---

[437] Приговор Абаканского городского суда (Республика Хакасия) от 30 июля 2024 г. по уголовному делу № 1-257/2024 // СПС «КонсультантПлюс» (дата обращения: 30.03.2025).

[438] *Безенков, И.А.* Международный опыт противодействия коррупционным правонарушениям, совершаемым с использованием цифровой валюты / И.А. Безенков // Законность. – 2024. – № 4. – С. 44 - 48.

где могут храниться криптовалютные кошельки или ключи доступа; зоны, где могут храниться физические носители ключей (бумажные кошельки, аппаратные кошельки); зоны, где находятся устройства, используемые для совершения транзакций.

Наиболее вероятные места сокрытия цифровых следов включают в себя защищенные паролем устройства, зашифрованные файлы, аппаратные кошельки, а также онлайн-сервисы и облачные хранилища. Практическим примером может служить обнаружение скрытого раздела на жестком диске, содержащего зашифрованные криптовалютные кошельки, или обнаружение секретной фразы в записной книжке, которая дает доступ к криптовалютному кошельку.

Очередность обследования определяется логикой расследования и приоритетом обнаружения наиболее ценных улик. Так, если у лица, подозреваемого в совершении мошеннических действий, производится обыск, то приоритетно должны быть обследованы устройства, которые, вероятно, содержат ключи доступа к кошелькам, а затем производится анализ транзакций и связей с другими лицами. Способы поиска варьируются от традиционного осмотра до использования специализированного программного обеспечения для криминалистического анализа данных, расшифровки файлов и извлечения удаленной информации. В качестве примера можно привести использование инструментов для анализа блокчейна с целью определения движения криптовалюты и установления связи с подозреваемыми[439].

В процессе детального обследования следователь должен придерживаться выбранного плана, внося по мере необходимости коррективы. Важно уделять внимание местам общего пользования, где могут храниться общие для всех данные, такие как пароли, адреса кошельков или информация об учётных записях на биржах. Особое внимание уделяется устройствам, подключённым к сети Интернет, поскольку они могут содержать следы онлайн-активности,

[439] *Zakaria, H.* Enquête approfondie : traçage des transactions cryptographiques pour la sécurité des fonds / H. Zakaria. – 2024. – URL: https://hzlegal.ae/fr/enquête-perspicace-retraçant-les-transactions-cryptographiques-pour-la-sécurité-des-fonds/ (дата обращения: 30.03.2025).

связанной с криптовалютой. Например, анализ истории браузера может выявить посещения сайтов криптовалютных бирж или форумов[440].

При расследовании преступлений, связанных с криптовалютой, тактические приёмы проведения обыска приобретают особую значимость ввиду специфики хранения и сокрытия цифровых активов. Применение вербальной разведки в ходе обыска, заключающееся в объявлении о предстоящих этапах поисковых мероприятий и последующем анализе поведенческих реакций обыскиваемого и присутствующих лиц, представляется эффективным методом выявления потенциальных мест сокрытия информации. Словесный стимул, усиливая психологическое напряжение, способен спровоцировать релевантные реакции, такие как облегчение при ошибочном направлении поиска или усиление тревоги при приближении к искомым объектам. В практике известны случаи, когда лица, испытывающие сильное психологическое давление, услышав объявление о намерении обыскать определённую территорию, добровольно выдавали информацию о местонахождении скрытых криптовалютных ключей или устройств, содержащих критически важные данные.

При проведении обыска в помещении целесообразно придерживаться системного подхода, предполагающего последовательное обследование объектов в заданном направлении (например, по часовой стрелке), охватывающее как отдельные предметы, так и центральную часть помещения, стены и напольное покрытие, прежде чем переходить к обследованию других помещений. Выбор конкретной тактики поиска – сплошного последовательного обследования или выборочного – определяется с учетом совокупности факторов, включая имеющуюся информацию о возможном местонахождении искомых объектов, поведение обыскиваемого и особенности обстановки, и остаётся прерогативой следователя. Метод последовательного сплошного обследования наиболее эффективен в условиях информационной неопределённости относительно

---

[440] *Бастрыкин, А. И.* Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий / А. И. Бастрыкин // Вестник Российской правовой академии. – 2022. – № 4. – С. 88-94.

вероятного местонахождения цифровых активов, при проведении обыска в отсутствие обыскиваемого лица, а также в ситуациях, когда непроизвольные поведенческие реакции обыскиваемого не позволяют однозначно определить направление поисковых мероприятий. В данном случае следователь придерживается строго определённого направления, систематически осматривая все встречающиеся объекты и последовательно переходя от одного к другому, чтобы минимизировать риск упущения потенциальных мест хранения цифровых активов. Например, в одном деле о незаконном обороте криптовалюты следователь, применяя метод сплошного обследования, обнаружил USB-накопитель, замаскированный под обычный брелок для ключей, содержащий приватные ключи от криптовалютного кошелька с существенной суммой средств, что позволило привлечь обвиняемого к ответственности[441].

При проведении обыска в рамках расследования, связанного с криптовалютами, эффективным представляется применение выборочного метода. Данный подход подразумевает приоритетное обследование мест, в которых с наибольшей вероятностью могут быть сокрыты цифровые активы или информация, имеющая отношение к делу. Определение таких мест осуществляется следователем на основе комплексного анализа доступных данных, включая, помимо традиционных факторов, таких как результаты наблюдения за реакцией обыскиваемого и оперативно-розыскную информацию, сведения о специфических особенностях обращения с криптовалютами. Например, анализируются цифровые следы, оставленные при использовании анонимных браузеров (Tor, I2P[442]) или специализированных операционных

---

[441] *Бахтеев, Д.В.* Векторы цифрового развития криминалистики / Д. В. Бахтеев // Технологии XXI века в юриспруденции : Материалы Шестой всероссийской научно-практической конференции, Екатеринбург, 24 мая 2024 года. – Екатеринбург, 2024. – С. 13-17.

[442] I2P (Invisible Internet Project, с англ. – «Невидимый Интернет-проект») представляет собой децентрализованную анонимную сеть, разработанную для обеспечения конфиденциальности и устойчивости к цензуре посредством криптографически защищённых коммуникаций. В отличие от традиционных интернет-архитектур, где маршрутизация данных подчиняется жёсткой иерархии, I2P функционирует на принципах peer-to-peer (P2P) взаимодействия, при котором каждый узел одновременно выступает и как клиент, и как сервер, участвуя в передаче зашифрованных сообщений.

систем (Tails, Whonix), которые могут указывать на использование зашифрованных контейнеров или тайников на USB-накопителях для хранения приватных ключей. Важно учитывать поведенческие паттерны подозреваемого в цифровой среде: активное участие в форумах, посвященных кибербезопасности и анонимности, использование VPN-сервисов для сокрытия IP-адреса, что косвенно свидетельствует о повышенном внимании к вопросам конфиденциальности и, следовательно, о вероятности использования продвинутых методов сокрытия информации.

Проведение обыска в подобных условиях требует от следователя не только знания стандартных процедур, но и глубокого понимания принципов функционирования криптовалют, методов обеспечения анонимности и сокрытия информации в цифровой среде. Неудачи на начальном этапе поиска не должны приводить к отказу от дальнейших действий. Важно проявлять настойчивость и адаптировать тактику обыска к конкретной ситуации. К примеру, если имеются данные о том, что подозреваемый использовал так называемую стеганографию – метод сокрытия информации внутри цифровых изображений или аудиофайлов, – необходимо тщательно проанализировать мультимедийные файлы, хранящиеся на устройствах подозреваемого, с помощью специализированного программного обеспечения.

Основу анонимизации в данной системе составляет так называемый «чесночный маршрутизационный протокол» («garlic routing»), являющийся усовершенствованной версией луковой маршрутизации («onion routing»). Суть его заключается в том, что сообщения не просто инкапсулируются в последовательные слои шифрования, но и могут объединяться в «головки чеснока», что значительно затрудняет анализ трафика и повышает устойчивость к перехвату. Более того, передача данных осуществляется через цепочку промежуточных узлов, причём ни один из них не обладает полной информацией ни об отправителе, ни о получателе, ни даже о полном пути следования пакета.

Важнейшей особенностью I2P является поддержка скрытых сервисов («eepsites»), доступ к которым возможен только внутри сети, что исключает их индексацию традиционными поисковыми системами и блокировку на уровне интернет-провайдеров. Помимо этого, благодаря динамической адаптации топологии маршрутов и постоянному обновлению криптографических ключей, система демонстрирует высокую устойчивость к атакам. *Abdo, J.B.* Modeling the Invisible Internet / J.B. Abdo, L. Hossain // Complex Networks & Their Applications XII. COMPLEX NETWORKS 2023. Studies in Computational Intelligence, vol 1143. / ed. by H. Cherifi, L.M. Rocha, C. Cherifi, M. Donduran. – Cham: Springer, 2024. – DOI: https://doi.org/10.1007/978-3-031-53472-0_30

С тактической точки зрения обыск в помещении следует начинать с мест, где наиболее вероятно обнаружение искомых объектов, применяя современные научно-технические средства. Помимо традиционных инструментов, таких как металлоискатели, целесообразно использовать анализаторы радиочастот для обнаружения скрытых устройств хранения данных (например, модифицированных USB-накопителей с возможностью удалённого стирания информации). Если искомые объекты имеют небольшие размеры или могут быть разобраны на части, то поиск следует начинать с труднодоступных мест, таких как вентиляционные шахты, скрытые ниши в стенах или даже бытовая техника, модифицированная для сокрытия цифровых носителей.

Нередко для сокрытия криптовалютных активов преступники создают сложные тайники (как физические, так и цифровые). В качестве нетипичного примера можно привести случай, когда приватные ключи от криптовалютного кошелька были спрятаны в виде QR-кода, вытатуированного на теле одного из соучастников. Обнаружение такого тайника требует от следователей не только профессионализма, но и творческого подхода к проведению следственных действий, а также глубокого знания способов обеспечения безопасности и сокрытия информации, используемых в криптовалютной сфере[443].

При обследовании помещений необходимо обращать внимание на так называемые «негативные обстоятельства» – отклонения от ожидаемых характеристик объектов. Что касается напольных покрытий, то это могут быть признаки вскрытия плинтусов, деформации паркета или отсутствие естественного загрязнения между досками, свидетельствующие о недавнем демонтаже и повторной установке. Различия в цвете краски или повреждения шпаклевки также могут указывать на наличие скрытого доступа к тайнику под полом. Мебель также является распространенным местом для тайников. При обыске необходимо тщательно исследовать как видимые, так и скрытые

[443] *Гаспарян, Г.З.* Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : автореф. дис. … канд. юрид. наук / Гаспарян Гурген Зорикович. – Москва, 2020. – 30 с.

поверхности предметов мебели, включая внутренние полости, двойное дно и ножки. Мягкую мебель можно прощупать или проколоть тонкой иглой, чтобы выявить скрытые полости, а твёрдые поверхности следует исследовать так же, как и стены. Предметы интерьера, такие как картины, часы и иконы, также могут скрывать тайники за собой, поэтому необходимо обращать внимание на следы на стенах и состояние обоев или краски под ними. В рамках расследования также может потребоваться осмотр компьютерной и бытовой техники, средств связи и музыкальных инструментов, по возможности с их частичной разборкой.

Примером резонансного дела, иллюстрирующего важность тщательного расследования, является уже упоминавшееся нами дело «Шелковый путь», в ходе которого правоохранительные органы обнаружили значительное количество криптовалюты Биткоин, спрятанной на цифровых носителях в хорошо замаскированных тайниках в доме подозреваемого. В другом случае в ходе расследования отмывания денег с помощью криптовалюты обыск в доме подозреваемого позволил обнаружить физические кошельки (аппаратные кошельки) с криптовалютой, спрятанные в корпусе старого компьютера, который, на первый взгляд, не представлял никакой ценности.

В рамках расследования преступлений, связанных с криптовалютой, задача обнаружения скрытых цифровых активов является одной из наиболее сложных. Крипто-тайники, в отличие от традиционных способов сокрытия активов, характеризуются своей цифровой природой и способностью маскироваться в различных формах. Их обнаружение требует комплексного подхода, основанного на анализе цифровых следов, выявлении нетипичных моделей поведения и применении специализированных инструментов.

Локальные хранилища могут быть замаскированы под обычные файлы на жёстком диске компьютера, зашифрованы или скрыты внутри контейнеров стеганографии. Так, вместо банального шифрования кошелька VeraCrypt злоумышленники могут использовать специализированные инструменты для сокрытия контейнера внутри графического файла, распространяемого через общедоступные файлообменники. Для обнаружения таких тайников требуется

анализ файловой системы, поиск файлов аномальных размеров, проверка метаданных и использование методов криптоанализа. Негативные факторы здесь проявляются в несоответствии размера файла его содержимому, подозрительной активности процессов шифрования или дешифрования на компьютере, а также в нетипичном использовании ресурсов процессора и памяти.

Онлайн-хранилища представляют собой криптовалютные кошельки, зарегистрированные на подставных лиц или использующие анонимные сервисы. Обнаружение таких тайников требует анализа истории транзакций, выявления связей между различными кошельками и использования OSINT-инструментов для деанонимизации владельцев. Например, преступники могут использовать сервисы смешивания (криптомикшеры) для запутывания транзакций и сокрытия источника средств. Однако анализ шаблонов транзакций, объёмов средств и времени проведения операций может выявить закономерности, указывающие на использование подобных сервисов. Анализ онлайн-хранилищ предполагает мониторинг активности кошельков, анализ их связей с другими кошельками и выявление признаков «двойного дна». Например, использование нескольких уровней анонимизации или регистрацию кошельков на украденные персональные данные.

Виртуальные хранилища представляют собой использование смарт-контрактов для сокрытия криптовалюты. Смарт-контракты позволяют создавать сложные финансовые инструменты, которые могут быть использованы для маскировки транзакций и сокрытия владения активами. Например, преступники могут использовать децентрализованные биржи (DEX) для обмена криптовалюты на другие активы, а затем использовать смарт-контракты для создания токенов, обеспеченных этими активами. Обнаружение таких тайников требует анализа кода смарт-контрактов, выявления аномальной активности и использования специализированных инструментов для отслеживания транзакций в блокчейне.

Для эффективного выявления крипто-тайников необходимо сочетать традиционные методы расследования с современными технологиями анализа

данных и инструментами мониторинга открытых источников. Важно учитывать принцип пропорциональности при проведении обысков и изъятии цифровых устройств, ограничиваясь необходимым объемом данных для проведения расследования.

Тайники, в которых спрятаны следы, связанные с криптовалютой, потенциально могут находиться где угодно. В контексте расследования акцент часто смещается с традиционных физических хранилищ на цифровые, однако не стоит сбрасывать со счетов и «старые добрые» тайники.

Физические тайники под полом, особенно у стен или под мебелью, под коврами и ковролином, по-прежнему актуальны. Здесь можно обнаружить не только наличные, полученные в результате обмена криптовалюты, но и физические носители с важной информацией: бумажные «холодные кошельки» с приватными ключами, флеш-накопители с зашифрованными файлами, содержащими сведения о транзакциях, схемы обналичивания и т.п. Их можно выявить, обратив внимание на следующие обстоятельства: признаки вскрытия на плинтусах (например, свежие сколы краски, микроцарапины); вмятины на паркете или отсутствие «пазовой грязи» между паркетными досками (указывает на недавний подъём досок); доски, состоящие из нескольких частей (маскировка люка); дополнительные крепления ламината, покачивание или прогибание панелей, различия в оттенках краски отдельных частей пола, повреждения шпаклевки.

Мебель также является популярным местом для тайников. В крипторасследованиях это может быть актуально для хранения ноутбуков с «чистой» операционной системой, предназначенных исключительно для работы с криптовалютами, отдельных жёстких дисков или даже специализированных устройств для генерации и хранения приватных ключей (например, Trezor или Ledger Nano S). При обыске нужно тщательно изучить внешние и скрытые части предметов мебели (включая поверхности, обращённые к стене, полу, потолку, внутренние части, ножки), а также наличие скрытых полостей и двойного дна. Картины, настенные часы и другие предметы, висящие на стенах, могут

скрывать за собой не только потайные ниши, но и, например, магнитные крепления для флеш-накопителей. Следы под этими предметами, состояние обоев или краски – важные индикаторы.

Особое внимание следует уделять компьютерной и бытовой технике, средствам связи, музыкальным инструментам. Здесь можно найти скрытые разделы на жёстких дисках с зашифрованными данными о криптоактивах, модифицированные прошивки роутеров, перенаправляющие трафик для сокрытия истинного IP-адреса при работе с криптовалютными биржами, а также встроенные в технику устройства для майнинга (хотя это и маловероятно в условиях жилой квартиры, но исключать такую возможность нельзя).

Поиск мелких и плоских предметов, таких как USB-накопители, SD-карты или бумажные носители с сид-фразами и приватными ключами, требует тщательного осмотра книг, альбомов и журналов. Следует не только перелистывать страницы, но и измерять толщину обложек, анализировать состояние переплета, поскольку тайники могут быть искусно замаскированы.

Обыски в помещениях юридических лиц представляют собой отдельную категорию сложности. Из-за большого количества лиц, имеющих доступ к таким помещениям, существует повышенный риск утраты или уничтожения искомых объектов. При осмотре служебных кабинетов особое внимание уделяется столам, сейфам и шкафам. Несмотря на то, что устройство сложных тайников в офисных помещениях менее распространено, следует учитывать возможность наличия потайных сейфов или искусно замаскированных хранилищ.

В ходе поиска документации, связанной с криптовалютными транзакциями, необходимо тщательно осматривать мусорные корзины, контейнеры для бумаг и устройства для уничтожения документов. Даже обрывки уничтоженных документов могут быть восстановлены и содержать ценную информацию. Если в кабинете работают несколько сотрудников, то целесообразно предложить им в присутствии следователя самостоятельно проверить свои рабочие места, что может способствовать обнаружению искомых объектов и создать атмосферу сотрудничества.

Процедура обыска, регламентированная уголовно-процессуальным законодательством, требует детальной фиксации всех процессуальных действий и их результатов в протоколе. Данный протокол по сути является легитимизирующим документом, удостоверяющим законность проведенных мероприятий и допустимость собранных доказательств. При расследовании преступлений, связанных с криптовалютой, протокол приобретает особую важность, поскольку специфические объекты поиска – цифровые активы, криптографические ключи, данные о транзакциях – требуют максимально точного описания для последующей идентификации и анализа[444].

В протоколе обыска необходимо четко указывать место обнаружения цифровых следов, будь то конкретный жесткий диск компьютера, USB-накопитель, мобильное устройство или облачное хранилище. Обстоятельства обнаружения, такие как открытый доступ к криптокошельку на экране компьютера или наличие зашифрованных файлов, также подлежат обязательной фиксации. Важно указать, были объекты выданы добровольно или изъяты принудительно, поскольку это может повлиять на оценку добросовестности действий лица, у которого проводится обыск.

Перечисление изымаемых цифровых активов требует особой тщательности. Необходимо по возможности идентифицировать конкретный вид криптовалюты, количество изъятых монет, адреса криптокошельков, к которым они относятся, а также хеш-суммы ключевых файлов (например, файлов wallet.dat, содержащих приватные ключи).

Протоколирование обстоятельств обыска имеет первостепенное значение для обеспечения допустимости полученных доказательств и соблюдения процессуальных гарантий. Если в ходе обыска предпринимаются попытки скрыть или уничтожить подлежащие изъятию предметы, документы или цифровые активы, это должно быть тщательно зафиксировано в протоколе с

---

[444] Преступления в сфере высоких технологий и информационной безопасности / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина. – Москва : Общество с ограниченной ответственностью "Издательство Прометей", 2023. – 1086 с.

указанием конкретных действий, предпринятых лицами, у которых проводился обыск, а также мер, принятых следственной группой для пресечения таких действий. Например, попытка физического уничтожения криптокошелька путём разбивания устройства или удаления программного обеспечения, либо сокрытие аппаратного кошелька в труднодоступном месте, должны быть подробно описаны. Протокол должен отражать не только факт противодействия, но и методы, использованные для его преодоления, включая применение технических средств или принудительных мер. При этом должен строго соблюдаться принцип соразмерности, запрещено причинение неоправданного ущерба.

Негативные обстоятельства, возникшие в ходе обыска, такие как необходимость принудительного вскрытия хранилищ (сейфов, заблокированных компьютеров, зашифрованных носителей информации), требуют подробного описания. Следует указать причины, обосновывающие применение данной меры, методы вскрытия, использованные инструменты и полученные результаты. Например, если для доступа к зашифрованному жесткому диску потребовалось привлечение специалиста по криптографии и применение специализированного программного обеспечения, это должно быть отражено в протоколе с указанием используемого программного обеспечения и времени, затраченного на процедуру. Важно зафиксировать, оказывал ли обыскиваемый сопротивление, и если да, то какие меры были приняты для обеспечения проведения обыска.

Использование научно-технических средств при проведении обыска, таких как сканирование сети на предмет обнаружения скрытых устройств, извлечение данных с поврежденных носителей информации или анализ трафика для выявления криптотранзакций, должно быть отражено в протоколе с указанием типа используемого оборудования, программного обеспечения, целей применения и полученных результатов. Например, применение криминалистического программного обеспечения для создания образа жесткого диска, содержащего криптокошелек, должно быть подробно задокументировано, включая хэш-суммы для обеспечения целостности данных.

В протоколе необходимо указать, предоставлял ли обыскиваемый доступ к своим аккаунтам, сообщал ли пароли и коды доступа к криптокошелькам или, наоборот, отказывался от сотрудничества. Отказ от предоставления информации может быть расценен судом как косвенное доказательство вины (так называемые улики поведения) и учтен при вынесении приговора, хотя сам по себе не является достаточным основанием для признания лица виновным.

В практике расследования преступлений, связанных с криптовалютой, нередки случаи, когда подозреваемые пытаются уничтожить или скрыть следы своей деятельности, осознавая юридические последствия обнаружения криптоактивов. Например, в одном из дел о финансировании терроризма подозреваемый пытался удалить приложение криптокошелька со своего смартфона во время обыска, однако следователь смог восстановить данные с помощью привлеченных специалистов, что послужило важным доказательством его причастности к преступной деятельности. В другом случае подозреваемый в отмывании денег спрятал аппаратный криптокошелёк в тайнике в стене, но тот был обнаружен с помощью нелинейного локатора. Эти примеры подчёркивают важность тщательного протоколирования всех обстоятельств обыска для обеспечения полноты и достоверности собранных доказательств[445].

При расследовании преступлений, совершаемых в отношении и с использованием криптовалюты, особое значение приобретают *заключения специалиста в области аналитики сетей блокчейн.* Это обусловлено прежде всего спецификой цифровых активов и транзакций, неразрывно связанных с информационно-коммуникационными технологиями. Исследование с использованием специализированных программного обеспечения в данном случае выступает ключевым инструментом для установления обстоятельств modus operandi преступления, идентификации вовлеченных лиц и, что крайне важно, обнаружения, фиксации и анализа цифровых следов на электронных

---

[445] *Шаевич, А.А.* Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений : дис. … канд. юрид. наук / Шаевич Антон Александрович. – Иркутск, 2007. – 195 с.

устройствах, обнаруженных при проведении оперативно-розыскных мероприятий и следственных действий.

Применение специалистом в ходе исследования определенных методов позволяет проанализировать широкий спектр цифровых следов, оставленных криптопреступниками. К таким методам, в частности, относятся: анализ блокчейн-транзакций с использованием специализированного программного обеспечения; идентификация IP-адресов и других сетевых данных, связанных с криптокошельками и торговыми платформами; восстановление удаленной или зашифрованной информации с жестких дисков, USB-накопителей и других носителей данных. Кроме того, исследование специалиста включает в себя анализ программного обеспечения, используемого для создания и распространения вредоносных программ, фишинговых страниц и программ для майнинга криптовалют.

В рамках указанной деятельности выделяются следующие ключевые направления, имеющие значение при расследовании рассматриваемой группы преступлений.

1. Исследование информации на электронных носителях. Данное направление предполагает применение специализированных методов и инструментов (например, EnCase, FTK Imager) для создания бит-копий накопителей, восстановления удалённых или повреждённых файлов, анализа файловых систем и извлечения скрытых данных, включая временные файлы, кэшированные записи и метаданные. Особое внимание уделяется выявлению следов пользовательской активности: истории браузера, журналов мессенджеров, электронных писем, а также файлов, защищённых шифрованием, для дешифрации которых могут использоваться методы перебора («brute force») или извлечения ключей из оперативной памяти.

2. Анализ программного обеспечения. Он включает в себя проверку установленных приложений на предмет наличия вредоносного кода, выявление несанкционированных модификаций системных файлов или признаков использования инструментов анонимизации. Также в ходе анализа исследуется

соответствие ПО лицензионным соглашениям, анализируются логи работы программ для установления временны́х рамок их эксплуатации. В случае кибератак проводится «реверс-инжиниринг» вредоносных образцов с использованием дизассемблеров (IDA Pro, Ghidra) для определения функционала и векторов проникновения.

3. Идентификация аппаратных компонентов. Она направлена на установление уникальных характеристик устройств, таких как серийные номера материнских плат, MAC-адреса сетевых карт, идентификаторы жёстких дисков или IMEI мобильных устройств. Эти данные позволяют связать устройство с конкретными событиями (например, участие в DDoS-атаке через идентификацию роутера) или доказать его принадлежность определённому лицу через сопоставление с регистрационными записями производителей либо операторов связи.

4. Компьютерно-сетевая экспертиза. Включает в себя анализ сетевого трафика, журналов и прокси-серверов, DNS-запросов, а также данных пакетной передачи для реконструкции событий в цифровой среде. Эксперты выявляют факты несанкционированного доступа, отслеживают маршруты утечки данных, определяют IP-адреса участников атак и идентифицируют инструменты их проведения, используя, например, сетевые сканеры. Важным аспектом является исследование следов взаимодействия с облачными файлами и расшифровка трафика через извлечение сессионных ключей.

6. Исследование криптовалютных транзакций с использованием специализированных аналитических инструментов. Указанные инструменты представляют собой программные комплексы, разработанные для обработки и анализа больших объемов данных из блокчейнов различных криптовалют. Они предоставляют широкий спектр функций, которые помогают в расследовании криптопреступлений, оценке рисков и соблюдении нормативных требований.

При расследовании преступлений, совершаемых в отношении и с использованием криптовалюты, чаще всего наиболее эффективным методом

выявления противоправной активности в инфраструктуре криптовалют является кластеризация криптовалютных адресов.

Кластеризация криптовалютных адресов – это аналитический подход, позволяющий объединять адреса блокчейна в группы, предположительно контролируемые одним фигурантом. Основой для такой группировки служат шаблоны транзакций, метаданные и структурные особенности публичного реестра. Например, если несколько адресов используются совместно в одной транзакции, в отдельных юрисдикциях называемой «эвристикой совместного расходования», то их относят к одному кластеру, поскольку высока вероятность, что все они принадлежат одному владельцу[446].

О подобной ситуации в своей работе упоминает В.А. Перов. По мнению правоведа «…как правило, участником блокчейн-сети используется большое количество криптовалютных адресов (кошельков). Для осуществления транзакции лицо должно иметь ключи от всех кошельков, с которых осуществляется данная транзакция. Таким образом, можно прийти к выводу о том, что все криптокошельки указанного кластера принадлежат одному и тому же лицу… Фиксация следов подобного рода не только подтверждает проведенную криптовалютную транзакцию, но и позволяет установить точное время ее осуществления, что в сочетании с информацией об IP-адресе используемого компьютерного устройства и данными биллинга может позволить определить владельца определенного криптокошелька»[447].

Рассматриваемый метод принято разделять на два ключевых направления, каждое из которых решает специфические экспертные задачи. Первый тип, называемый «*выявлением кластеров владения»,* осуществляется для идентификации групп адресов, контролируемых единым субъектом - будь то физическое лицо, организация или сервис. Подобный подход лежит в основе

---

[446] *Гаврилин, Ю.В.* Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств : учебное пособие / Ю.В. Гаврилин, И.С. Бедеров. – Москва : Академия управления МВД России, 2022. – 76 с.

[447] *Перов В. А.* Доказательственное значение электронных следов при расследовании преступлений с использованием блокчейн-технологий // Российский следователь. – 2021. – № 4. – С. 38-40.

большинства профессиональных инструментов, где адреса бирж формируются в единые кластеры на основе анализа совместного расходования средств, выявления адресов сдачи или привязки к KYC-данным. Такая группировка позволяет не только отследить совокупный объем транзакций, но и выявить закономерности поведения (например, определить, какая доля средств удерживается на кошельках, а какая регулярно выводится на сторонние платформы). Если в ходе обыска обнаружен адрес подозреваемого, то кластеризация владения помогает выявить все связанные с ним кошельки, выстроить хронологию истории переводов и оценить общий финансовый след, что важно для доказательства систематичности противоправной деятельности[448].

Однако исследование нередко фокусируется исключительно на трассировке потоков средств, упуская из виду аналитический потенциал метаданных. Например, частота транзакций, временны́е интервалы между операциями или преобладание входящих/исходящих переводов могут указывать на роль субъекта в криминальной схеме: является он организатором, посредником или конечным бенефициаром. Кластер, связанный с биржей, может демонстрировать высокую ликвидность и короткие циклы удержания средств, тогда как кошельки киберпреступников часто характеризуются длительными периодами бездействия, за которыми следуют крупные переводы через миксеры.

Второй тип – *«операционные кластеры»* – служит для группировки адресов по их функциональной роли в криптосистеме, независимо от владельца. Например, кластеры микширования, децентрализованных бирж или ransomware-операций помогают экспертам классифицировать транзакции по типу активности. Это особенно полезно при расследовании сложных схем, где средства последовательно перемещаются через цепочки сервисов: от криптобиржи к микшеру, а затем на кошельки дропов[449]. Операционная

---

[448] *Xu, S.* Blockchain-based secure data sharing with overlapping clustering and searchable encryption / S. Xu, S. Dong, L. Wang, M.J. Mihaljević, S. Zhang, W. Shao, Q. Wang // Computer Standards & Interfaces. – 2025. – Vol. 93. – P. 103-979.

[449] *Koshy, T.* A survey on cryptocurrency mixers / T. Koshy, S. Koshy // Journal of King Saud University - Computer and Information Sciences. – 2021. – Vol. 33(7). – P. 826–842.

кластеризация позволяет быстро идентифицировать точки входа и вывода, даже если преступники используют сотни адресов для маскировки.

Оба подхода могут взаимодополнять друг друга: кластеры владения раскрывают «кто», а операционные кластеры – «как» и «зачем». Например, если подозреваемый взаимодействует с адресом, входящим в операционный кластер миксера, это свидетельствует о попытке маскировки следов, а связь его персонального кластера с биржевыми адресами – о канале легализации противоправных средств. Тем не менее эффективность кластеризации ограничена такими факторами, как использование приватных монет, автоматическая генерация адресов кошельками типа Electrum или умышленное дробление транзакций через peel chains. Кроме того, ошибки в эвристиках (например, ложное объединение адресов сдачи нескольких пользователей в P2P-сделках) требуют ручной верификации данных.

Дополняет этот метод *эвристика общего вывода*, которая фокусируется на выходных данных транзакций. Если средства отправляются на несколько адресов, один из которых уже ассоциирован с известным кластером, остальные адреса-получатели также могут быть отнесены к этому кластеру. Предполагается, что отправитель, контролируя исходные адреса, может управлять и целевыми адресами, особенно в случаях транзакций с множественными выходами.

Важную роль играет *эвристика смены адреса*, основанная на анализе адресов, создаваемых кошельками для возврата неизрасходованных средств. Такие адреса идентифицируются по ряду признаков, например, по отсутствию последующей активности или связи с ранее использованными адресами. Например, если транзакция с адреса A отправляет 0.5 BTC на адрес B, а 0.3 BTC возвращается на новый адрес C, то C с высокой вероятностью является адресом сдачи, контролируемым владельцем A.

Для выявления сложных взаимосвязей применяется анализ *транзакционных графов,* где «узлы» представляют адреса, а «рёбра» –

транзакции между ними[450]. Кластеры формируются на основе плотности связей: группы адресов, многократно взаимодействующих друг с другом, объединяются в единые структуры. Этот метод особенно эффективен для выявления сетевых схем, таких как микширование средств через цепочки промежуточных кошельков.

Повысить точность кластеризации позволяет интеграция данных из сторонних источников – специализированных сервисов и баз, связывающих адреса с реальными субъектами. Например, биржевые адреса, идентифицированные через KYC-данные, или адреса миксеров, внесённые в чёрные списки регуляторов, служат опорными точками для расширения кластеров. Компании Chainalysis или Elliptic агрегируют такие данные, что позволяет обогатить анализ контекстом: принадлежностью к определённым сервисам, связью с киберпреступными группами или участием в санкционированных операциях.

Системное применение этих методов обеспечивает реконструкцию финансовых потоков в блокчейне, выявление скрытых связей между участниками и установление причастности субъектов к противоправной деятельности. Например, кластеризация может раскрыть схему отмывания средств, где адреса-«воронки» связаны с микшерами, а затем с биржами, или идентифицировать кошельки ransomware-группы через анализ транзакций с жертвами. Однако эффективность методики зависит от корректности эвристических допущений, качества сторонних данных и способности минимизировать ложные срабатывания, вызванные автоматической генерацией адресов или использованием инструментов повышения конфиденциальности, таких как CoinJoin. Следовательно, можно сделать вывод о том, что кластеризация остаётся неотъемлемым инструментом деконструкции

[450] *Weber, M.* Untangling Bitcoin: Exploring the Structure of the Bitcoin Transaction Graph / M. Weber, D. D. Gramlich, F. Streitz, R. State // Security and Communication Networks. – 2019. – 648 p.

псевдоанонимности блокчейна, сочетающим техническую аналитику с контекстуальной интерпретацией данных.

Итак, суммируя все изложенное выше, можно прийти к следующим выводам.

1. Тактика проведения обысков приобретает выраженную междисциплинарную направленность. Подготовительный этап предполагает изучения данных: 1) транзакционного анализа для идентификации целевых кошельков; 2) психологических профилей подозреваемых, что позволяет определить вероятные методы сокрытия информации; 3) архитектурные особенностей помещений. При этом ключевое значение приобретает прогнозирование усложнения ситуации, когда техническая осведомленность подозреваемого прямо коррелирует со сложностью применяемых им методов конспирации.

2. Аналитические методы исследования криптотранзакций выступают системообразующим элементом доказывания. Кластеризация адресов, реализуемая через «анализ графов транзакций» и «эвристик смены выходов», позволяет реконструировать криптовалютные «переводы» даже при использовании миксеров. Однако эффективность этих методов ограничена технологиями повышения конфиденциальности, что актуализирует необходимость развития прогностических моделей, основанных на машинном обучении для выявления подозрительных транзакций.

3. Выявлена прямая зависимость между качеством подготовки следственно-оперативной группы и результативностью обысков. Привлечение специалистов по блокчейн-аналитике на этапе планирования позволяет оптимизировать поисковую стратегию, минимизируя риски утраты данных вследствие срабатывания шифрующих механизмов.

ЗАКЛЮЧЕНИЕ

В результате исследования вопросов раскрытия и расследования преступлений, совершаемых в отношении и с использованием криптовалюты, на основе изучения российского и зарубежного опыта, были обоснованы следующие выводы.

1. Криминалистически значимая информация, получаемая из криптовалютной среды, представляет собой специфическую категорию данных, характеризующих механизм совершения таких преступлений и особенности их отражения в цифровой среде. Данная категория информации обладает комплексом общих и уникальных атрибутов, определяющих ее качество и, как следствие, доказательственное значение в условиях высокой степени анонимности и трансграничности криптовалютных транзакций. Между тем свойства и характеристики криминалистически значимой информации подлежат тщательной оценке с учетом специфики криптографических методов защиты данных и особенностей функционирования блокчейн-технологий.

2. Сочетание специализированных знаний и передового аналитического инструментария может обеспечить проведение соответствующего комплексного анализа закономерностей, образующихся при функционировании взаимосвязанных элементов: криптокошельков, адресов, данных, полученных с криптобирж, и информации о платформах, используемых для осуществления транзакций. Соответственно, расследование преступлений, связанных с криптовалютой, требует постоянного развития специализированных инструментов для анализа блокчейна, деанонимизации транзакций, выявления преступных схем, реализуемых с использованием технологии блокчейн.

3. Криптопреступления, обладая высокой степенью технологической и организационной сложности, требуют системного подхода к их классификации, базирующейся на операционно-функциональных критериях, выявленных через эмпирический анализ следственной практики, и криминалистически значимых признаков. Подобное разделение позволяет не только структурировать

разнородные проявления цифровой преступности, но и выявить закономерности, связанные с технической реализацией противоправных деяний, их транснациональным характером и взаимодействием с инфраструктурой блокчейн-сетей.

4. Мошеннические схемы адаптируются к цифровой среде, преступники используют доверие пользователей к инновациям, деяния приобретают комбинированные формы, сочетающие психологическое манипулирование с техническими инструментами. Децентрализованные платформы и анонимные криптовалюты формируют системные риски для глобальной финансовой безопасности.

5. Обучение сотрудников правоохранительных органов является обязательным элементом системы подготовки. Без подготовки специалистов, владеющих методами получения криминалистически значимой информации, даже совершенные инструменты анализа останутся невостребованными. Программы обучения должны включать анализ кейсов, что соответствует принципу интерактивного обучения, где резонансные случаи криптопреступлений становятся основой для разработки алгоритмов действий[451].

6. Комплексный анализ закономерностей, формирующихся во взаимодействии словообразующих элементов криптовалютных транзакций (криптокошельков, криптографических адресов, данных криптобирж, сведений о платформах), требует интеграции специализированных знаний и передового аналитического инструментария для эффективного расследования преступлений, связанных с криптовалютой, и обусловливает необходимость постоянного развития специализированных инструментов для анализа блокчейна, деанонимизации транзакций и выявления преступных схем, реализуемых с использованием технологии распределенного реестра.

---

[451] Опрос практических сотрудников показал, что подавляющее большинство респондентов (90%) считают необходимым специальное обучение для работы с информацией из блокчейна, что свидетельствует о потребности в повышении квалификации специалистов в этой области. См.: Приложение 1.

7. Технологическая эволюция криптоиндустрии диктует необходимость непрерывного развития криминалистической науки, ориентированного на прогнозирование вновь возникающих рисков. Появление DeFi-платформ, смарт-контрактов и AI-инструментов в руках злоумышленников требует опережающего криминалистического осмысления уязвимостей, разработки превентивных мер и обучения сотрудников правоохранительных органов работе с инновационными аналитическими системами, такими как «Прозрачный блокчейн».

9. Деятельность организованных преступных групп охватывает множество юрисдикций, что обусловливает необходимость международного сотрудничества. Злоумышленники внедряют искусственный интеллект для оптимизации фишинга, анализа уязвимостей и прогнозирования поведения жертв, что создаёт новые вызовы для правоохранительных органов, требующих ответного технологического развития.

10. Использование криптомиксеров для сокрытия происхождения криптоактивов эффективно выявляется анализом трафика, метаданных транзакций и информации о серверах микширования, что позволяет идентифицировать связанные адреса и объемы транзакций. При этом обнаружение упоминаний криптомиксеров в связи с отмыванием средств от кибервымогательства может стать начальным звеном в отслеживании транзакций причастных лиц.

11. Особое значение приобретает правильное оформление протокола следственного действия, обеспечивающее процессуальную легитимность обнаружения, фиксации и изъятия цифровых следов в условиях применения технических средств. Значимыми инструментами проведения экспертных исследований выступает кластеризация криптовалютных адресов, позволяющая деконструировать псевдоанонимность блокчейна через эвристики совместного расходования и транзакционные графы. Однако ограничения методов, такие как автоматическая генерация адресов или использование миксеров, актуализируют

необходимость дополнения кластеризации данных, полученных от поставщиков услуг виртуальных активов.

13. Эффективность обыска напрямую зависит от этапа предварительной подготовки, включающей анализ транзакций в блокчейне, прогнозирование поведения подозреваемого и моделирование вероятных мест сокрытия данных, что подтверждается примерами из следственной практики, демонстрирующими обнаружение криптоактивов в нетривиальных тайниках (модифицированные устройства, QR-коды на физических носителях).

14. Особое значение для обеспечения процессуальной легитимности изъятия цифровых следов приобретает тщательное протоколирование, включающее в себя детализацию метаданных и фиксацию возможных действий / противодействия со стороны подозреваемых. Применение научно-технических средств, таких как криминалистические инструменты для создания бит-копий и анализаторы сетевого трафика, становится обязательным условием сохранения целостности доказательств.

15. Ключевым инструментом исследования специалиста, где объектом выступают элементы криптовалютной инфраструктуры, является кластеризация криптовалютных адресов, позволяющая деконструировать псевдоанонимность блокчейна посредством установления совместного расходования и анализа транзакционных графов. Однако ограничения существующих методов, обусловленные, например, автоматической генерацией адресов или использованием миксеров, актуализируют необходимость дополнения кластеризации контекстуальными данными, получаемыми от регулируемых криптобирж и из международных баз данных, что подчеркивает важность межведомственного и международного сотрудничества.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Международно-правовые документы

1. Всеобщая декларация прав человека от 10 декабря 1948 г. // Российская газета. 1995. № 67.

2. Конвенция об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности от 08.11.1990 // Бюллетень международных договоров Российской Федерации. 2003. № 3. С. 14-46.

3. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам, заключенная 22 января 1993 г. // Собрание законодательства Российской Федерации. 1995. № 17. Ст. 1472.

4. Конвенция Организации Объединенных Наций против транснациональной организованной преступности от 15.12.2000 г. // Собрание законодательства Российской Федерации. 2004. № 40. Ст. 3882.

5. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационнокоммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (Принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 г.) // https://www.un.org/ru/documents/treaty/A-RES-79-243

6. Протокол о порядке передачи наркотических средств, психотропных веществ и их прекурсоров, огнестрельного оружия, его основных частей, боеприпасов, взрывчатых веществ и взрывных устройств, являющихся вещественными доказательствами по уголовным делам, от 11 октября 2017 // Единый реестр правовых актов и других документов СНГ // https://cis.minsk.by/

7. Протокол о порядке передачи наркотических средств, психотропных веществ и их прекурсоров, огнестрельного оружия, его основных частей, боеприпасов, взрывчатых веществ и взрывных устройств, являющихся вещественными доказательствами по уголовным делам от 11 октября 2017 г. //

Единый реестр правовых актов и других документов СНГ [Электронный ресурс]. URL: http://cis.minsk.by/

8. Соглашение о сотрудничестве между Генеральной прокуратурой Российской Федерации и Верховной народной прокуратурой Лаосской Народно-Демократической Республики (Заключено в г. Владивостоке 04.09.2024).

9. Соглашение о сотрудничестве между Генеральной прокуратурой Российской Федерации и Центральной прокуратурой Корейской Народно-Демократической Республики (Заключено в г. Пхеньяне 22.07.2024).

10. Постановление № 54-11 Межпарламентской Ассамблеи государств - участников СНГ «О Глоссарии терминов, используемых органами внутренних дел (полицией) государств - участников Содружества Независимых Государств, по вопросам противодействия преступлениям, совершаемым посредством блокчейн-технологий и криптовалют» (Принято в г. Самарканде 28.10.2022).

Нормативные правовые акты и официальные документы

11. Конституция Российской Федерации: [принята Всенар. Голосованием 12 дек. 1993 г., с изменениями, одобренными в ходе общероссийского голосования 01.07.2020] // Собрание законодательства РФ. 2014. №31. Ст. 4398.

12. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации. 2021. № 27 (Часть II). Ст. 5351.

13. Уголовный кодекс Российской Федерации (последняя редакция): Федеральный закон от 13 июня 1996 г. № 63-ФЗ // РГ. 1996, 18 июня.

14. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ (последняя редакция) // Собрание законодательства РФ. 2001. № 52. Ст. 1.

15. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Собрание законодательства Российской Федерации. 2001. №33. Ст. 3418.

16. Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 № 144-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

17. Федеральный закон «О полиции» от 7 февраля 2011 № 3-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

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

19. Regulation (EU) 2023/1114 of the European Parliament and of the Council of May 31, 2023 on markets in crypto-assets and amending Directives 2009/65/EC, (EU) 2019/1937 // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114.

20. Code Of Practice Issued Under Section 47s Of The Proceeds Of Crime Act 2002. Search, Seizure and Detention of Property (England and Wales). April 2024. ISBN 978-1-5286-4655-0.

Судебные решения и правоприменительная практика

21. Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) «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» // Бюллетень Верховного Суда Российской Федерации. 2015. № 9.

22. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // Бюллетень Верховного Суда Российской Федерации. 2023. № 3. С. 3-8.

23. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации по делу № 88-УДП23-7-К8 / Банк судебных документов // URL: https://vsrf.ru/lk/practice/stor_pdf/2314260

24. Постановление Девятого арбитражного апелляционного суда от 15.05.2018 № 09АП16416/2018 по делу № А40-124668/2017.

25. Постановление Яковлевского районного суда (Белгородская область) от 4 июня 2019 г. по делу № 1-85/2019.

26. Приговор Абаканский городской суд (Республика Хакасия) от 30 июля 2024 г. по делу № 1-257/2024.

27. Приговор Абаканского городского суда (Республика Хакасия) от 30 июля 2024 г. по делу № 1-257/2024.

28. Приговор Абаканского городского суда (Республика Хакасия) № 1-203/2024 от 5 июля 2024 г. по делу № 1-203/2024.

29. Приговор Благовещенского городского суда (Амурская область) от 2 февраля 2024 г. по делу № 1-1371/2023.

30. Приговор Дзержинского районного суда г. Волгограда № 1-643/2023 от 28 ноября 2023 г. по делу № 1-643/2023.

31. Приговор Дзержинского районного суда г. Перми (Пермский край) от 11 марта 2021 г. по делу № 1-67/2021.

32. Приговор Ивдельского городского суда (Свердловская область) от 16 июля 2024 г. по делу № 1-60/2024.

33. Приговор Кировского районного суда г. Саратова от 9 июля 2024 г. по делу № 1-294/2024.

34. Приговор Кировского районного суда г. Ростова-на-Дону от 26 января 2024 г. по делу № 1-157/2023.

35. Приговор Кировского районного суда г. Саратова от 10 марта 2021 г. по делу № 1-274/2020.

36. Приговор Королёвского городского суда (Московская область) от 16 января 2024 г. по делу № 1-46/2024.

37. Приговор Ленинского районного суда г. Оренбурга от 09.07.2019 по делу № 1-346/2019.

38. Приговор Ленинского районного суда г. Уфы (Республика Башкортостан) от 5 июля 2024 г. по делу № 1-135/2024.

39. Приговор Московского областного суда № 2-106/2024 от 26 августа 2024 г. по делу № 2-106/2024.

40. Приговор Московского районного суда г. Твери (Тверская область) от 6 февраля 2024 г. по делу № 1-337/2023.

41. Приговор Мотовилихинского районного суда г. Перми от 19 декабря 2023 г. по делу № 1-500/2023.

42. Приговор Новокузнецкого районного суда № 1-95/2023 от 28 ноября 2023 г. по делу № 1-95/2023.

43. Приговор Новомосковского городского суда от 29 июля 2024 г. по делу № 1-174/2024.

44. Приговор Новотроицкого городского суда (Оренбургская область) от 9 июля 2024 г. по делу № 1-228/2024.

45. Приговор Октябрьского районного суда г. Мурманска от 13 сентября 2023 г. по делу № 1-453/2022.

46. Приговор Петрозаводского городского суда (Республика Карелия) № 1-865/2024 от 29 июля 2024 г. по делу № 1-865/2024.

47. Приговор Петропавловск-Камчатского городского суда (Камчатский край) от 18 июля 2024 г. по делу № 1-535/2024.

48. Приговор Петропавловского-Камчатского городского суда № 1-272/2021 от 13 июля 2021 г. по делу № 1-272/2021.

49. Приговор Промышленного районного суда г. Курска № 1-121/2024 от 20 августа 2024 г. по делу № 1-121/2024.

50. Приговор Промышленного районного суда г. Курска от 20 августа 2024 г. по делу № 1-121/2024.

51. Приговор Свердловского районного суда г. Костромы от 15 июля 2024 г. по делу № 1-166/2024.

52. Приговор Томского областного суда (Томская область) от 14 февраля 2024 г. по делу № 2-23/2023.

53. Приговор Ханты-Мансийского районного суда № 1-263/2020 от 24 июля 2020 г. по делу № 1-263/2020.

54. Приговор Химкинского городского суда (Московская область)№ 1-738/2023 от 9 ноября 2023 г. по делу № 1-738/2023.

55. Приговор Чебоксарского районного суда (Чувашская Республика) от 10 июля 2024 г. по делу № 1-85/2024.

56. Приговор Череповецкого городского суда (Вологодская область) от 17 июля 2024 г. по делу № 1-637/2024.

57. Приговор Шуйского городского суда (Ивановская область) от 7 декабря 2023 г. по делу № 1-60/2023.

58. Приговор Щелковского городского суда (Московская область) от 16 июля 2024 г. по делу № 1-450/2024.

Отчеты ООН, ФАТФ, иные руководства и рекомендации международных и зарубежных правоохранительных органов

59. Лучшие дела, расследованные членами Группы «Эгмонт». Дела, при расследовании которых осуществлялся финансовый анализ (2014-2020 годы) // www.egmontgroup.org

60. Отчет ФАТФ. Возврат преступных доходов из-за рубежа через задействование межведомственных сетей по возврату активов // https://mumcfm.ru/mediateka/international/fatf/otcet-fatf-vozvrat-prestupnyx-doxodov-iz-za-rubeza-cerez-zadeistvovanie-mezvedomstvennyx-setei-po-vozvratu-aktivov

61. Типологический проект ЕАГ. – 2022. – URL: https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_rus.pdf

62. Anlagebetrug: Ein andauerndes Phänomen mit hohen Schadenssummen // https://lka.polizei.nrw/artikel/anlagebetrug-ein-andauerndes-phaenomen-mit-hohen-schadenssummen

63. Association of Certified Anti-Money Laundering Specialists, 2023 // https://www.moneylaundering.com/news/ cryptocurrency-research-firms-vastly-underestimate-illicitpayments-critics-claim

64. Australian Competition and Consumer Commission. Romance baiting scams on the rise [Electronic resource]. – 2021. – URL: https://www.accc.gov.au/media-release/romance-baiting-scams-on-the-rise

65. Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat // United Nations Office on Drugs and Crime (UNODC). – 2024 // https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf

66. Crypto Assets and CBDCs in Latin America and the Caribbean: Opportunities and Risks. Available from: https://www.researchgate.net/publication/368869923_Crypto_Assets_and_CBDCs_in_Latin_America_and_the_Caribbean_Opportunities_and_Risks [accessed Mar 16 2025].

67. Dating and romance scams - don't let them break your heart or wallet // https://www.police.nsw.gov.au/crime/frauds_and_scams/fraud_categories/dating_and_romance_scams

68. Drugs and the darknet Perspectives for enforcement, research and policy European Monitoring Centre for Drugs and Drug Addiction, 2017. Praça Europa 1, Cais do Sodré, 1249–289 Lisbon, Portugal / https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf

69. FATF. Countering Ransomware Financing [Electronic resource]. – Paris, 2023. // FATF. – URL: http://www.fatf-gafi.org/publications/Methodsandtrends/countering-ransomware-financing.htm

70. Guidance for a Risk-Based Approach for Money or Value Transfer Services // FATF. – Paris. - 2016. – URL: www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html

71. Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets //

https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guide-on-relevant-aspects-and-appropriate-steps-for-the-investigation-identification-seizure-and-confiscation-of-virtual-assets.pdf

72. Illicit Financial Flows from Cyber-Enabled Fraud / FATF – Interpol - Egmont Group // FATF. – Paris, France. – 2023. – URL: www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyberenabled-fraud.html.

73. International operation closes down Piilopuoti dark web marketplace // https://www.europol.europa.eu/media-press/newsroom/news/international-operation-closes-down-piilopuoti-dark-web-marketplace

74. International Organization for Standardization. Blockchain and Distributed Ledger Technologies-Vocabulary. – 2020. – URL: https://www.iso.org/obp/ui/en/#iso:std:iso:22739:ed-1:v1:en (дата обращения: 05.08.2024).

75. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF. – Paris, France. 2025 // URL: www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

76. Married couple arrested alleged conspiracy // https://www.justice.gov/opa/pr/married-couple-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

77. Official announcement issued by the Wenzhou People's Procuratorate, 29 November 2021 // https:// www.12309. gov.cn/12309/gj/zj/wzs/zdajxx/202111/.shtml.

78. Operation Cryptosweep // https://www.nasaa.org/policy/enforcement/operation-cryptosweep/

79. Polizia Postale. Report annuale 2024. Aggiornamento 21/12/2024 [Electronic resource] // Sophos News. – URL: https://news.sophos.com/en-us/2023/08/02/sha-zhu-pan-scam-uses-ai-chat-to-target-iphone-and-android-users

80. Principles for information exchange between financial intelligence units approved by the heads of fius july 2013 // Egmont Group. – URL:

https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf

81. Risk of money laundering and the financing of terrorism through crypto assets. – 2024. https://www.fedpol.admin.ch/fedpol/en/home/aktuell/mm.msg-id-

82. Taiwan Police Department PoC. 台灣警政署165防騙網111/7/18-111/7/24 民眾通報假投資(博弈)詐騙網站 // Public Notice / https://165.npa.gov.tw/lineId

83. The changing nature of crime and criminal investigations // Police Executive Research Forum (PERF). – 2018. – P. 51.

84. Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security // https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security

85. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape // United Nations Office on Drugs and Crime (UNODC). – Southeast Asia and the Pacific. – 2024.

86. United Nations Human Rights. Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response. – 2023 // URL: https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

87. UNODC opens the first cryptocurrency analysis laboratory in Southeast Asia // https://www.unodc.org/roseap/en/malaysia/2022/05/cryptocurrency-analysis-laboratory/story.html

88. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. – Paris, France. 2021 // URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

89. Virtual Currencies: Key Definitions and Potential AML/CFT Risks [Электронный ресурс] : [доклад]. – June 2014. – [S. l.]: FATF, [2014]. – URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Монографии, учебники, учебные пособия

90. Бекетнова, Ю. М. Модели и типологии отмывания преступных доходов / Ю. М. Бекетнова. – Москва : Общество с ограниченной ответственностью "Русайнс", 2020. – 84 с.

91. Белкин, Р. С. Курс криминалистики: в 3 т. Т. 2: Частные криминалистические теории. М., 1997.

92. Васюков, В. Ф. Противодействие преступлениям в сфере незаконного оборота наркотиков, совершаемым с использованием информационно-телекоммуникационных технологий / В. Ф. Васюков, К. К. Клевцов, В. И. Малик. – Москва: Общество с ограниченной ответственностью "Издательство Прометей", 2023. – 468 с.

93. Волеводз, А.Г. Компьютерная информация, как объект криминалистического следоведения // Криминалистическая техника: Учебник / Отв. ред. И.М. Балашов, рук. колл. С.В. Маликов. М.: ООО Издательство «Юрлитинформ», 2008. - 381 с.

94. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО «Издательство «Юрлитинформ», 2001.

95. Волеводз, А. Г. Криптовалюта и цифровые финансовые активы как предмет и способ преступного посягательства / А. Г. Волеводз // Цифровое право : Учебник. – Москва : ООО Издательский дом "Юрлитинформ", 2024. – С. 589-599.

96. Гаврилин, Ю. В. Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств : учебное пособие / Ю.В. Гаврилин, И.С. Бедеров. – Москва : Академия управления МВД России, 2022. – 76 с.

97. Глотов, В. И. Криптобезопасность криптовалют / В. И. Глотов, Д. М. Михайлов. – Москва : Российский экономический университет имени Г.В. Плеханова, 2019. – 116 с.

98. Горбунова, К. А. Тактика производства следственных действий при расследовании преступлений в сфере компьютерной информации / К. А. Горбунова, А. С. Киселев. – Москва: Общество с ограниченной ответственностью «Проспект», 2023. – 88 с.

99. Гриненко, А. В. Криминалистика : учебник / А. В. Гриненко, В. А. Дударев, С. С. Маевский. – Москва : Общество с ограниченной ответственностью "Проспект", 2025. – 432 с.

100. Гриненко, А. В. Противодействие легализации (отмыванию) доходов, полученных преступным путем: уголовно-правовые, уголовно-процессуальные и криминалистические аспекты / А. В. Гриненко, А. В. Коляда, С. Н. Хорьяков; Московский государственный институт международных отношений (университет) министерства иностранных дел Российской Федерации. – Москва : Общество с ограниченной ответственностью "Проспект", 2022. – 184 с.

101. Информационные технологии в уголовно-правовой сфере: монография / под ред. А.И. Бастрыкина, А.Н. Савенкова. — М.: ЮНИТИ-ДАНА, 2023. — 279 с.

102. Колычева, А. Н. Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие / А. Н. Колычева, В. Ф. Васюков. – Москва : Общество с ограниченной ответственностью "Проспект", 2025. – 200 с.

103. Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» / В. С. Овчинский, О. А. Вагин, Б. Я. Гаврилов [и др.]. – Москва : Издательский Дом «Инфра-М», 2022. – 488 с.

104. Комов, А.В. Использование компьютерных (цифровых) следов при выявлении, раскрытии и расследовании преступлений. М.: 2025. – 293 с.

105. Мещеряков, В. А. Теоретические основы механизма следообразования в цифровой криминалистике / В. А. Мещеряков. – Москва: Общество с ограниченной ответственностью "Проспект", 2022. – 176 с.

106. Оперативно-розыскная деятельность: Научно-практический комментарий (постатейный) к Федеральному закону / А. И. Бастрыкин, В. М.

Егоршин, С. И. Захарцев [и др.]. – Москва : Издательство "Юрлитинформ", 2020. – 280 с.

107. Преступления в сфере высоких технологий и информационной безопасности / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина. – Москва : Общество с ограниченной ответственностью "Издательство Прометей", 2023. – 1086 с.

108. Противодействие криптовалютным преступлениям в зарубежных странах / В. Ф. Васюков, А. Г. Волеводз, К. К. Клевцов [и др.]. – Москва : ООО Издательский дом "Юрлитинформ", 2025. – 504 с.

109. Теория оперативно-розыскной деятельности: Краткие учебные курсы юридических наук / О. А. Вагин, К. К. Горяинов, А. В. Земскова [и др.]. – 5-е издание, переработанное. – Москва : Издательский Дом "Инфра-М", 2021. – 352 с.

110. Сидоренко, Э. Л. Криптовалюта и будущее цифровых финансов / Э. Л. Сидоренко. – Москва : МГИМО МИД России, 2023. – 36 с.

111. Смушкин, А. Б. Криминалистические аспекты использования киберпространства и обеспечения кибербезопасности / А. Б. Смушкин. – Москва : Общество с ограниченной ответственностью "Русайнс", 2024. – 196 с.

112. Стельмах, В. Ю. Производство следственных действий, направленных на получение и использование компьютерной информации / В. Ю. Стельмах, О. М. Ефремова, В. Ф. Васюков. – Москва: Общество с ограниченной ответственностью "Проспект", 2021. – 480 с.

113. Сущенко, С. А. Недопустимость доказательств в уголовном процессе Российской Федерации и государств англо-американской и романо-германской правовых семей : Учебное пособие / С. А. Сущенко, В. Ф. Васюков, А. Г. Волеводз. – Москва : Общество с ограниченной ответственностью "Издательство Прометей", 2022. – 466 с.

114. Тисен, О. Н. Противодействие финансированию терроризма и диверсий, совершаемых с использованием криптовалют : Серия: Библиотека криминалиста / О. Н. Тисен. – Москва : Издательский дом «Юрлитинформ», 2025. – 248 с.

115. Фомичев А.В. Использование возможностей Федеральной службы по финансовому мониторингу в ходе предварительного расследования: Методическое пособие / под ред. Д.А. Кунева; под общ. ред. А.В. Лавренко. М., 2016.

116. Чернавский Д.С. Синергетика и информация. Динамическая теория информации. М.: УРСС. ЛЕНАНД. 2017. – 304 с.

117. Bonanni, E. Tecniche investigative / E. Bonanni, G. Pettenati, F. Garoia, V. Paolillo. – 2010.

118. Kruisbergen, E.W. Combating organized crime A study on undercover policing and the followthe-money strategy / E.W. Kruisbergen. – 2017. – URL: https://www.Ew-Kruisbergen-2/publication/312197822_

119. Kruisbergen, E.W. When Other Methods Fail…: Infiltrating Organized Crime Groups in the Netherlands / E.W. Kruisbergen // Contemporary Organized Crime. Studies of Organized Crime, vol 18. / ed. by H. Nelen, D. Siegel. – Cham: Springer, 2021. – DOI: https://doi.org/10.1007/978-3-030-56592-3_15

120. Nakayama, H. Criminal Psychology in Japan / H. Nakayama. – Tokyo : University of Tokyo Press, 2015.

121. Przewłoka E., Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej (Eng. Methodology of basic actions carried out by a police officer and related to the crime of "theft" of virtual currency), Bydgoszcz 2023.

122. Toezichtsrapport Automated OSINT: tools en bronnen voor openbronnenonderzoek CTIVD nr. 74. 2021. – URL: https://www.ctivd.nl/onderzoeken/aivd-mivd-onderzoek-automated-osint/

123. Zakaria, H. Enquête approfondie : traçage des transactions cryptographiques pour la sécurité des fonds / H. Zakaria. – 2024. – URL: https://hzlegal.ae/fr/enquête-perspicace-retraçant-les-transactions-cryptographiques-pour-la-sécurité-des-fonds/

Научные статьи

124. Агарков, А. В. Оперативно-розыскное мероприятие «исследование предметов и документов»: содержание понятия / А. В. Агарков // Оперативно-розыскное противодействие наркопреступности : Материалы Всероссийского научно-практического семинара, Красноярск, 8 апреля 2022 г. – Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2022. – С. 53-56.

125. Ализаде, В. А. Неприменение ст. 174.1 Уголовного кодекса РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов / В. А. Ализаде, А. Г. Волеводз // Наркоконтроль. – 2018. – № 1. – С. 5-13.

126. Ализаде, В. А. Судебная практика применения ст. 174¹ УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты / В. А. Ализаде, А. Г. Волеводз // Наркоконтроль. – 2017. – № 4. – С. 8-14.

127. Астафьев Ю.В. Методологические основы соотношения оперативно-розыскной и доказательственной информации в расследовании преступлений // Вестник ВГУ. Серия Право. 2007. №1.

128. Бастрыкин, А. И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий / А. И. Бастрыкин // Вестник Российской правовой академии. – 2022. – № 4. – С. 88-94.

129. Батраченко, Д. А. Некоторые вопросы получения оперативно значимой и криминалистической информации из облачных хранилищ / Д. А. Батраченко, В. Ф. Васюков // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2025. – № 1 (69). – С . 98–107.

130. Бахтеев, Д.В. Векторы цифрового развития криминалистики / Д. В. Бахтеев // Технологии XXI века в юриспруденции : Материалы Шестой всероссийской научно-практической конференции, Екатеринбург, 24 мая 2024 года. – Екатеринбург, 2024. – С. 13-17.

131. Безенков, И. А. Международный опыт противодействия коррупционным правонарушениям, совершаемым с использованием цифровой валюты / И.А. Безенков // Законность. – 2024. – № 4. – С. 44 - 48.

132. Бульбачева, А. А. Актуальные проблемы осмотра места происшествия / А. А. Бульбачева // Труды Академии управления МВД России. – 2015. – № 2(34). – С. 97-100.

133. Васюков, В. Ф. К вопросу о сущности следов преступлений, совершаемых в сфере информационно-коммуникационных технологий // Право и образование. – 2016. – № 8. – С. 112-118.

134. Васюков, В. Ф. Расследование дел о сбыте наркотиков с использованием мессенджеров и криптовалюты / В. Ф. Васюков // Уголовный процесс. – 2019. – № 9(177). – С. 44-49.

135. Васюков, В. Ф. Использование криптовалюты в преступных целях: некоторые вопросы противодействия / В.И. Ерохов, В.Ф. Васюков // Современная наука. – 2020. – № 2. – С. 5-6.

136. Васюков, В. Ф. К вопросу о получении оперативно значимой информации из открытых источников информации сети «Интернет» / В. Ф. Васюков, А. Ю. Афанасьев // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2024. – № 1(65). – С. 79-86.

137. Васюков, В. Ф. Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют / В.Ф. Васюков, А.Н. Старжинская // Российское право: образование, практика, наука. – 2024. – № 4. – С. 68-78.

138. Векленко, В. В. Особенности противодействия расследованию преступлений, совершенных с использованием криптовалюты в Российской Федерации / В. В. Векленко, А. М. Чихрадзе // Виктимология. – 2024. – Т. 11, № 4. – С. 576-586.

139. Вехов, В. Б. Отдельные аспекты следственного осмотра некоторых электронных устройств / В. Б. Вехов, А. Б. Смушкин // Вестник Саратовской государственной юридической академии. – 2024. – № 4(159). – С. 230-236.

140. Волеводз, А. Г. Розыск, арест и обеспечение конфискации за рубежом денежных средств и имущества, нажитых преступным путем (вопросы организации и методики) / А.Г. Волеводз // Российский следователь. – 1999. – №2. – С. 40-50.

141. Волеводз, А. Г. К вопросу об учете потребностей противодействия отмыванию денег и финансированию терроризма при формировании правовых основ оборота криптовалюты в Российской Федерации / А. Г. Волеводз // Правовое поле современной экономики. – 2016. – № 3. – С. 135-145.

142. Волеводз, А. Г. Международное сотрудничество в сфере уголовного судопроизводства по делам о преступлениях, совершенных с использованием криптовалюты: постановка проблемы / А. Г. Волеводз // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования: Сборник материалов Международной научно-практической конференции. К 300-летию российской полиции, Орёл, 18–19 октября 2018 г. / Под редакцией Е.Б. Гришина. – Орёл, 2018. – С. 66-75.

143. Волеводз, А. Г. Особенности криптовалюты в системе денежных инструментов как определяющие факторы правовой регламентации ее оборота / А. Г. Волеводз, В. А. Кутырин // Электронная валюта в свете современных правовых и экономических вызовов : сборник материалов Международной научно-практической конференции, Москва, 2 июня 2016 г. – Москва: Издательство "Юрлитинформ", 2016. – С. 292-308.

144. Волеводз, А. Г. Оценка криптовалюты как предмета преступления, предусмотренного ст. 174.1 УК РФ / А. Г. Волеводз // Уголовное право: стратегия развития в XXI веке : Материалы XV Международной научно-практической конференции, Москва, 25–26 января 2018 г. – Москва: РГ-Пресс, 2018. – С. 597-603.

145. Волеводз, А. Г. Международно-правовое регулирование возврата преступных активов в рамках БРИКС: современное состояние и перспективы / А. Г. Волеводз // Актуальные проблемы международного сотрудничества в борьбе с преступностью : Сборник научных трудов Международной научно-практической

конференции, Москва, 16 ноября 2023 года. – Москва: Московский университет МВД РФ им. В.Я. Кикотя, 2023. – С. 18-24.

146. Волеводз, А. Г. Следы преступлений в сфере компьютерной информации / А.Г. Волеводз // Российский следователь. – 2001. – № 7. – С. 2–11.

147. Володикова, И. В. Отдельные аспекты механизма образования цифровых следов при совершении дистанционных мошенничеств / И.В. Володикова // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 1 (98). – С. 97–103.

148. Гаврилин, Ю. В. Развитие методов цифровой криминалистики: пределы допустимости / Ю. В. Гаврилин // Уголовный процесс и криминалистика: теория, практика, дидактика: Сборник материалов VII Всероссийской научно-практической конференции, Рязань, 16 декабря 2021 г. – Рязань: Академия права и управления Федеральной службы исполнения наказаний, 2022. – С. 69-75.

149. Гаврилов, Б.Я. К вопросу о совершенствовании уголовной политики противодействия преступности в условиях информатизации общества: искусственный интеллект в уголовном судопроизводстве / Б. Я. Гаврилов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2025. – № 1 (69). – С. 262-265.

150. Головин, А. Ю. Задачи криминалистики в сфере противодействия криптопреступности / А. Ю. Головин, Е. В. Головина // Санкт-Петербургский международный криминалистический форум: Материалы международной научно-практической конференции, Санкт-Петербург, 10–11 июня 2024 г. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2024. – С. 119-126.

151. Горяинов К. К. Некоторые вопросы оперативно-розыскной практики в борьбе с коррупционными проявлениями в США и Великобритании / К.К. Горяинов // Современное состояние и актуальные проблемы противодействия коррупции в органах и учреждениях УИС. Сборник материалов круглого стола. 2019. – С. 55-60.

152. Грибунов, О. П. Криптовалюта и иные виртуальные активы как феномен современной преступности: проблемы раскрытия, расследования и предупреждения / О. П. Грибунов, С. И. Усачев, Е. А. Усачева // Российский следователь. – 2024. – № 4. – С. 7-12.

153. Гриненко, А. В. Взаимодействие уголовно-процессуальной и криминалистической наук: труды профессора Р.С. Белкина и современность / А. В. Гриненко // Вестник криминалистики. – 2022. – № 3(83). – С. 11-14.

154. Давыдова Ю. Б. Модель информационно-аналитической системы анализа данных при расследовании компьютерных преступлений // Сборник статей III Международной научно-практической конференции: в 2 ч.. Пенза, 2022. С. 19-24.

155. Дамирчиев, Э. И. Международный и зарубежный опыт криминализации противоправных деяний, связанных с использованием информационно-коммуникационных технологий / Э. И. Дамирчиев // Мировой судья. – 2024. – № 7. – С. 9-14.

156. Дамирчиев, Э. И. Социальные сети как источник оперативно значимой информации при выявлении и раскрытии преступлений / Э. И. Дамирчиев, А. А. Комоско, В. Ф. Васюков // Современное общество и право. – 2024. – № 3(70). – С. 72-78.

157. Дамирчиев, Э. И. Некоторые вопросы противодействия дистанционным мошенничествам в Китае / Э. И. Дамирчиев, В.Ф. Васюков // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 2 (99). – С. 161-166.

158. Долгиева, М. М. Криптовалютная наркоторговля в России и за рубежом / М.М. Долгиева // Вестник Воронежского института МВД России. – 2018. – № 4. – С. 177-182.

159. Дорошков, В.В. Уголовно-правовая политика Российского государства в современную эпоху / В. В. Дорошков // Мировой судья. – 2024. – № 5. – С. 2-8.

160. Дронова, О.Б. Интеграция данных экспертно-криминалистических и оперативных учетов как способ повышения уровня информационного обеспечения раскрытия и расследования преступлений / О.Б. Дронова, Б.П. Смагоринский // Юридическая наука и правоохранительная практика. – 2024. – № 2 (68). – С. 51–58.

161. Захарцев, С. И. Кибермафия как угроза нормальному человеческому существованию: рецензия-размышление по поводу монографии «Мировые тенденции и международное противодействие» / С.И. Захарцев, В.П. Сальников // Юрист-Правоведъ. – 2022. – № 3 (102). – С. 215–220.

162. Захарцев, С. И. Оперативно-розыскные мероприятия: вопросы правового регулирования / С. И. Захарцев, И. Н. Кондрат, В. П. Сальников // Мониторинг правоприменения. – 2024. – № 3(52). – С. 54-60.

163. Золин, И. Ю. Легализация (отмывание) наркодоходов: использование цифровой валюты / И. Ю. Золин, С. И. Земцова // Научный компонент. – 2023. – № 4(20). – С. 5-14.

164. Зуев, С.В. IT-следователь в цифровой среде уголовного судопроизводства / С.В. Зуев А.И. Зазулин // Правопорядок: история, теория, практика.– 2024. – № 2 (41). – С. 48-54.

165. Иванов, И. И. Особенности предупреждения преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий / И.И. Иванов, И.Н. Кондрат // Мировой судья. – 2024. – № 12. – С. 2–9.

166. Исаков, Р. В. О противодействии легализации (отмыванию) наркодоходов с использованием финансовых активов (криптовалют) / Р. В. Исаков, Д. В. Теткин, А. М. Попов // Вестник Воронежского института МВД России. – 2021. – № 2. – С. 267-271.

167. Карепанов, Н. В. Особенности технологии агрегирования, исследования и использования электронно-цифровых следов преступления / Н. В. Карепанов // Технологии XXI века в юриспруденции: Материалы четвёртой международной научно-практической конференции, Екатеринбург, 20 мая 2022

г. – Екатеринбург: «Уральский государственный юридический университет», 2022. – С. 86-104.

168. Карымсаков, Р. Ш. Вопросы прав и обязанностей органов, осуществляющих оперативно-розыскную деятельность в рамках борьбы с преступлениями, связанными с использованием криптовалют / Р. Ш. Карымсаков, Д. Ж. Молдакулова // Вестник науки. – 2025. – Т. 4, № 1(82). – С. 293-303.

169. Колычева, А. Н. Отдельные аспекты противодействия использованию криптовалют в преступных целях / А. Н. Колычева, В. Ф. Васюков // Криминалистика: вчера, сегодня, завтра. – 2025. – № 1(33). – С. 89-101.

170. Комков, В. В. Этапы актуальных атак посредством фишинговых писем / В. В. Комков // Журнал высоких гуманитарных технологий. – 2024. – № 3(6). – С. 39-46.

171. Кунев, Д. А. Международно-правовые стандарты противодействия криминальному обороту криптовалют и иных виртуальных активов / Д. А. Кунев // Вестник Университета прокуратуры Российской Федерации. – 2022. – № 1(87). – С. 146-151.

172. Кустов, А. М. К вопросу о «цифровой» криминалистике / А. М. Кустов // Цифровые технологии в юриспруденции: генезис и перспективы : Материалы I Международной межвузовской научно-практической конференции, Москва, 28 февраля 2020 г. – Москва: Красноярский государственный аграрный университет, 2020. – С. 90-94.

173. Кушниренко, С. П. Оборот криптовалют в механизме совершения преступлений / С. П. Кушниренко, А. Г. Харатишвили // Криминалистъ. – 2022. – № 3(40). – С. 77-83.

174. Ладов, В. А. О понятии информации в контексте современных исследований по проблемам семантики и искусственного интеллекта / В. А. Ладов // Вестник Томского государственного университета. Философия. Социология. Политология. – 2013. – № 4(24). – С. 26-32.

175. Литвишко, П.А. Юрисдикционные и международно-правовые аспекты обеспечительных и конфискационных мер в отношении виртуальных активов / П.А. Литвишко // Законность. – 2021. – № 3. – С. 10–11.

176. Лубин, А. Ф. О версионном анализе исходной информации при расследовании преступлений / А. Ф. Лубин // Казанские уголовно-процессуальные и криминалистические чтения: Материалы Международной научно-практической конференции. В 2-х частях, Казань, 28 апреля 2022 г. / Том Часть 1. – Казань: Общество с ограниченной ответственностью "ЮрЭксПрактик", 2022. – С. 173-182.

177. Лузгин, И. И. Актуальные вопросы использования цифровых технологий при производстве осмотра места происшествия / И. И. Лузгин // Пенитенциарная система, государство и общество: проблемы взаимодействия: материалы Международной научно-практической конференции, Псков, 15 октября 2021 г. – Псков: Псковский филиал Академии ФСИН России, 2022. – С. 168-172.

178. Маркарян, Э. С. Особенности получения данных о механизме следообразования при расследовании преступлений, совершенных с использованием криптовалют / Э. С. Маркарян // Библиотека криминалиста. Научный журнал. – 2017. – № 4(33). – С. 176-187.

179. Маркарян, Э. С. Специфика проведения следственного осмотра при расследовании преступлений, совершенных с использованием криптовалют / Э. С. Маркарян // Актуальные проблемы российского права. – 2018. – № 6(91). – С. 146-152.

180. Матренин, М. О. Информационные следы в сети интернет и последствия их оставления / М. О. Матренин // Инновации и научно-техническое творчество молодежи : Материалы Российской научно-технической конференции, Новосибирск, 20–21 апреля 2022 г. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. – С. 615-619.

181. Машков, С. А. «Большие данные» и криминалистика: возможности и перспективы / С.А. Машков // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 2(44). – С. 78-86.

182. Меретуков, Г. М. Осмотр места происшествия как источник криминалистически значимой информации / Г. М. Меретуков // Год науки и технологий 2021 : Сборник тезисов по материалам Всероссийской научно-практической конференции, Краснодар, 9–12 февраля 2021 г. / Отв. за выпуск А.Г. Кощаев. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2021. – С. 223-239.

183. Мещеряков, В. А. Следы цифрового века / В. А. Мещеряков // Вопросы экспертной практики. – 2019. – № 1. – С. 423-426.

184. Мосин, И. В. Детерминанты преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий / И. В. Мосин // Вестник Уральского юридического института МВД России. – 2024. – № 2(42). – С. 79-84.

185. Мурадян, С. В. Актуальные проблемы противодействия деятельности криптовалютных пирамид / С. В. Мурадян // Имущественные отношения в Российской Федерации. – 2024. – № 2(269). – С. 93-104.

186. Озеров, И. Н. Цифровые следы преступлений как инструмент раскрытия и расследования коррупционных преступлений / И. Н. Озеров, А. М. Журбенко, К. И. Озеров // Актуальные проблемы борьбы с коррупцией: Материалы всероссийской научно-практической конференции, Москва, 27 октября 2023 г. – Москва: Московская академия следственного комитета, 2024. – С. 96-100.

187. Ордоков, М. Х. Совершение мошеннических действий в сети интернет / М. Х. Ордоков // Право и управление. – 2024. – № 6. – С. 330-333.

188. Осипенко, А. Л. Информационное воздействие на криминальную среду в условиях цифровизации / А. Л. Осипенко // Вестник Краснодарского университета МВД России. – 2024. – № 4(66). – С. 6-14.

189. Пермякова К.С. Криптографические методы защиты информации // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики. Материалы XI Международной научно-практической очно-заочной конференции. Екатеринбург, 2024. С. 29-32.

190. Перов, В. А. О криминалистической методике выявления преступлений, совершаемых с использованием криптовалюты, и расследовании соответствующих уголовных дел // Российский следователь. – 2020. – № 12. – С. 10-13.

191. Перов, В. А. Доказательственное значение электронных следов при расследовании преступлений с использованием блокчейн-технологий / В. А. Перов // Российский следователь. – 2021. – № 4. – С. 38-40.

192. Перов, В. А. Способы совершения, выявления и особенности квалификации преступлений, совершаемых с использованием отдельных видов криптовалют (на примере криптовалюты Zcash) / В.А. Перов // Российский следователь. – 2024. – № 9. – С. 51–54.

193. Подшибякин, А. С. Правовое и криминалистическое обеспечение оперативно-розыскной деятельности: Сборник составлен из статей, опубликованных профессором А.С. Подшибякиным в 1983-2010 г.г. в научных и в специальных изданиях / А. С. Подшибякин. – Москва, 2010. – 352 с.

194. Подшибякин, А. С. Современная криминалистика и ее развитие / А. С. Подшибякин // Криминалистика и судебно-экспертная деятельность в условиях современности: Материалы Международной научно-практической конференции: в 2-х томах, Краснодарский университет МВД России, 26 апреля 2013 г. / Том I. – Краснодарский университет МВД России, 2013. – С. 3-15.

195. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С. В. Иванцов, Э. Л. Сидоренко, Б. А. Спасенников [и др.] // Всероссийский криминологический журнал. – 2019. – Т. 13, № 1. – С. 85-93.

196. Родионов, В. С. К вопросу о разработке понятия «цифровой след» в российской и зарубежной криминалистике / В. С. Родионов // Университетские

правовые диалоги «право цифровой среды»: материалы Международной научно-практической конференции, Челябинск, 27–28 марта 2020 г. – Челябинск: Издательский центр ЮУрГУ, 2020. – С. 243-247.

197. Россинская, Е. Р. Система теории цифровизации судебно-экспертной деятельности / Е. Р. Россинская // Теория и практика судебной экспертизы. – 2024. – Т. 19, № 3. – С. 20-32.

198. Россинская, Е. Р. Теория информационно-компьютерного обеспечения судебно-экспертной деятельности как новая частная теория судебной экспертологии // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 2. – С. 27-40

199. Русман, Г. С. Первоначальный этап расследования преступлений, связанных с использованием криптовалюты / Г. С. Русман // Smart Law for Smart Industry : сборник научных статей / Под ред. Е. В. Титовой, Т. П. Подшивалова; Южно-Уральский государственный университет юридический институт. – Москва : РГ-Пресс, 2020. – С. 191-195.

200. Русскевич Е. А., Малыгин И. И. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики. 2021. N 3. С. 106 - 125.

201. Русскевич, Е. А. Преступления, связанные с обращением криптовалют: особенности квалификации / Е.А. Русскевич, И.И. Малыгин // Право. Журнал Высшей школы экономики. – 2021. – № 3. – С. 106–125.

202. Сажаев, А. М., Мишуточкин, А. Л. Значение электронно-цифровых следов в тактике допроса свидетелей и потерпевших // Расследование преступлений: проблемы и пути их решения. – 2022. – № 3 (37). – С. 142-149.

203. Свидетельство о государственной регистрации программы для ЭВМ № 2023664920 Российская Федерация. Прозрачный блокчейн. Государственный модуль : № 2023663888 : заявл. 04.07.2023 : опубл. 10.07.2023 ; заявитель Федеральная служба по финансовому мониторингу.

204. Семенчук, В. В. Вопросы информационного обеспечения выявления и раскрытия преступлений, совершаемых с использованием криптовалют / В. В. Семенчук // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 81-86.

205. Сергеев, С. М. Возможности ОРМ «Наведение справок» при проверке сообщения о преступлении экономической направленности / С. М. Сергеев // Криминалистика: вчера, сегодня, завтра. – 2022. – № 4(24). – С. 161-167.

206. Сидоренко, Э. Л. Defi-преступность: состояние, тенденции и криминологические модели / Э. Л. Сидоренко // Russian Journal of Economics and Law. – 2023. – Т. 17, № 2. – С. 327-341.

207. Сидоренко, Э. Л. Даркнет и наркопреступность: криминологические вызовы и актуальные уголовно-правовые вопросы / Э. Л. Сидоренко // Наркоконтроль. – 2023. – № 2. – С. 9-15.

208. Сидоренко, Э. Л. Криминологические риски оборота криптовалюты и проблемы ее правовой идентификации / Э. Л. Сидоренко // Библиотека криминалиста. Научный журнал. – 2016. – № 3(26). – С. 148-154.

209. Сидоренко, Э. Л. Криптовалюта как новый юридический феномен // Общество и право. – 2016. – № 3 (57). – С. 193-197.

210. Сидоренко, Э. Л. Криптопреступность как новое криминологическое явление / Э. Л. Сидоренко // Общество и право. – 2018. – № 2(64). – С. 15-21.

211. Сидоренко, Э. Л. Легализация преступных доходов с использованием DeFi: типовые схемы и индикаторы риска / Э. Л. Сидоренко // Russian Journal of Economics and Law. – 2023. – Т. 17, № 4. – С. 822-836;

212. Скобелин, С. Ю. Об использовании специальных знаний при исследовании смартфонов / С. Ю. Скобелин // Судебные экспертизы в уголовном процессе: теория и практика : Материалы II Всероссийской научно-практической конференции, Москва, 19 октября 2023 г. – Москва: Московская академия следственного комитета, 2024. – С. 187-191.

213. Смирнов, В. М. Проблемы противодействия преступности в сфере информационно-телекоммуникационных технологий и обеспечения

информационной безопасности / В. М. Смирнов, Д. С. Селезнев // Криминологический журнал. – 2024. – № 2. – С. 295-298.

214. Сотников, К. И. Потенциал современной криминалистики и показатели раскрытия преступлений / К. И. Сотников // Актуальные проблемы раскрытия и расследования преступлений : сборник материалов Международной научно-практической конференции, Екатеринбург, 29 сентября 2023 г. – Екатеринбург: Уральский юридический институт Министерства внутренних дел Российской Федерации, 2023. – С. 104-110.

215. Степаненко, Д. А., Гармышев, Я. В. Криптовалюты как предмет и средство совершения преступлений: проблемы квалификации и расследования / Д. А. Степаненко, Я. В. Гармышев // Российский следователь. – 2025. – № 1. – С. 32-35.

216. Степаненко, Д. А. Цифровизация как фактор и условие развития современной криминалистики / Д. А. Степаненко, А. А. Митрофанова // Российский следователь. – 2023. – № 4. – С. 16-22.

217. Судницын, А. Б. Отдельные возможности получения и использования сведений об операциях с криптовалютой при раскрытии и расследовании преступлений / А. Б. Судницын, В. В. Молоков // Вестник Восточно-Сибирского института МВД России. – 2019. – № 2(89). – С. 213-221.

218. Тисен, О. Н. Использование результатов деятельности Росфинмониторинга в уголовном судопроизводстве / О. Н. Тисен, А. В. Гриненко // Всероссийский криминологический журнал. – 2022. – Т. 16, № 4. – С. 492-504.

219. Тисен, О. Н. Использование сервиса отслеживания криптовалютных транзакций «Прозрачный блокчейн – 2» при выявлении и расследовании преступлений, совершенных с использованием криптовалют / О. Н. Тисен // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : Сборник научных трудов, Москва, 30 марта 2023 г. / Сост. А.В. Константинов. – Москва: Московский университет

Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 195-200.

220. Тисен, О. Н. Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют / О. Н. Тисен // Уголовное право. – 2024. – № 3(163). – С. 69-80.

221. Тисен, О. Н. Установление владельцев криптокошельков, обнаружение и изъятие приватных ключей при расследовании уголовных дел / О. Н. Тисен // Уголовный процесс. – 2024. – № 1(229). – С. 78-83.

222. Титов, А.А. Некоторые вопросы обнаружения и исследования компьютерной информации при раскрытии и расследовании преступлений / А.А. Титов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2022. – № 3(37). – С. 39-48.

223. Титов, А. А. Понятие, признаки и правовая природа цифровых финансовых активов: уголовно-правовой аспект / А. А. Титов // Пролог: журнал о праве. – 2022. –№ 4(36). – С. 105-113.

224. Титов, А. А. Процессуальные и тактические проблемы изъятия электронных носителей и копирования информации при расследовании преступлений с использованием криптовалюты / А. А. Титов, В. Ф. Васюков // Российский следователь. – 2023. – № 2. – С. 23-27.

225. Титов, А. А. Отдельные особенности рассмотрения сообщений (заявлений) о преступлениях, совершенных с использованием криптовалют / А.А. Титов // Вестник Академии Следственного комитета Российской Федерации. – 2023. – № 2. – С. 121-128.

226. Титов, А. А. Отдельные аспекты выявления и раскрытия криптомошенничеств в Индии / А.А. Титов // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 3 (98). – С. 279-283.

227. Титов, А. А. Использование криптовалют в преступных целях: методы выявления и противодействия / А.А. Титов // Современное общество и право. – 2024. – № 4. – С. 138-146.

228. Ульянова, М. А. Тактика получения и анализа информации, передаваемой в сетях связи с использованием технологии оконечного шифрования, при расследовании преступлений террористического характера / М. А. Ульянова // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : Сборник статей Международной научно-практической конференции, Москва, 18 мая 2018 г. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2018. – С. 296-299.

229. Фельдман, В. В. Blockchain и криптовалюты / В. В. Фельдман // Оперативно-розыскное противодействие наркопреступности : Всероссийский научно-практический семинар, Красноярск, 9 апреля 2021 г. – Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2021. – С. 46-50.

230. Хамидуллин, Р. С. Криминалистическое обеспечение противодействия незаконному обороту наркотических средств и психотропных веществ, осуществляемому в криптовалюте с использованием технологий «blockchain» / Р. С. Хамидуллин // Технологии XXI века в юриспруденции : Материалы четвёртой международной научно-практической конференции, Екатеринбург, 20 мая 2022 г. / отв. редактор: Д.В. Бахтеев. – Екатеринбург, 2022. – С. 52-58.

231. Центров, Е.Е. Теоретико-практический анализ соотношения понятий криминалистическая характеристика и классификация преступлений / Е. Е. Центров // Санкт-Петербургский международный криминалистический форум: Материалы международной научно-практической конференции, Санкт-Петербург, 10–11 июня 2024 г. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2024. – С. 537-542.

232. Черданцев, А. Ю. Практические проблемы получения, анализа и последующей правильной интерпретации полученной цифровой

криминалистически значимой информации / А. Ю. Черданцев // Эксперт-криминалист. – 2022. – № 4. – С. 26-29.

233. Шампаров, А. В. Механизм следообразования информации о соединениях между абонентами и (или) абонентскими устройствами / А. В. Шампаров // Вестник Удмуртского университета. Серия Экономика и право. – 2014. – № 4. – С. 202-207.

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

235. Шумилов, А. Ю. Совершенствование законодательного регулирования оперативно-розыскной деятельности таможенных органов / А. Ю. Шумилов // Регулирование внешнеэкономической деятельности и эволюция таможенной политики России: Тезисы докладов международной научно-практической конференции (22-23 октября 1996 г.): в 2 частях, Москва, 22–23 октября 1996 г. / Российская таможенная академия; председатель редколлегии Н.М. Блинов. Часть 2. – Москва: Российская таможенная академия, 1996. – С. 34-37.

236. Яблоков, Н.П. К вопросу о криминалистическом мышлении // Правовые проблемы укрепления российской государственности. Томск, 2012. С. 156-159.

237. Abdo, J.B. Modeling the Invisible Internet / J.B. Abdo, L. Hossain // Complex Networks & Their Applications XII. COMPLEX NETWORKS 2023. Studies in Computational Intelligence, vol 1143. / ed. by H. Cherifi, L.M. Rocha, C. Cherifi, M. Donduran. – Cham: Springer, 2024. – DOI: https://doi.org/10.1007/978-3-031-53472-0_30

238. Agarwal, U. Blockchain and crypto forensics: Investigating crypto frauds / U. Agarwal, V. Rishiwal, S. Tanwar, M. Yadav // International Journal of Network Management. – 2023. – Vol. 34. – DOI: https://doi.org/10.1002/nem.2255

239. Akartuna, E. A. A Holistic Network Analysis of the Money Laundering Threat Landscape: Assessing Criminal Typologies, Resilience and Implications for Disruption / E. A. Akartuna, S. D. Johnson, A. Thornton // Journal of Quantitative Criminology. – 2024. – DOI: 10.1007/s10940-024-09594-3.

240. Almaqableh, L. An investigative study of links between terrorist attacks and cryptocurrency markets / L. Almaqableh, K. Reddy, V. Pereira, V. Ramiah, D. Wallace, J.F. Veron // Journal of Business Research. – 2022. – Vol. 147. – P. 177-188.

241. Almaqableh, L. Is it possible to establish the link between drug busts and the cryptocurrency market? Yes, we can / L. Almaqableh, D. Wallace, V. Pereira, V. Ramiah, G. Wood, J.F. Veron, I. Moosa, A. Watson // International Journal of Information Management. – 2022. – DOI: 10.1016/j.ijinfomgt.2022.102488

242. Alrawi, O. Forecasting malware capabilities from cyber attack memory images / O. Alrawi et al. // USENIX Security. – 2021. – P. 3523–3540.

243. Abate, C. Online-Durchsuchung, Quellen-Telekommunikationsüberwachung und die Tücke im Detail: Einfluss rechtlicher und technischer Entwicklungen auf verdeckte Online-Ermittlungen zur Gewährleistung der Inneren Sicherheit / C. Abate // Datenschutz und Datensicherheit. – 2011. – Heft 2. – S. 122–125.

244. Baravalle, A. Dark Web Markets: Turning the Lights on AlphaBay / A. Baravalle, S. Lee // 19th International Conference, Dubai, United Arab Emirates, November 12-15, 2018, Proceedings, Part II. – 2018. – DOI: 10.1007/978-3-030-02925-8_35.

245. Barczentewicz, M. Crypto-Asset Market Abuse Under EU MiCA / M. Barczentewicz, A. de Gândara Gomes // European Journal of Risk Regulation. – 2024. – P. 1-18. – DOI: 10.1017/err.2024.80.

246. Bartos, P. Bitcoin Transaction Graph Analysis for Law Enforcement Purposes / P. Bartos, J. Feliks // Security and Safety Challenges for Smart Cities: Proceedings of the 15th International Conference on Cyber Warfare and Security (ICCWS 2020). – Academic Conferences and Publishing International, 2020.

247. Basynya, E. A. Bitcoin Transaction Analysis System / E. A. Basynya, N. Karapetyants, M. Karapetyants // Program and Computer Software. – 2024. – Vol. 50 (Suppl. 2). – P. S104–S112. – DOI: 10.1134/S0361768824700488.

248. Baum, C. A framework for universally composable publicly verifiable cryptographic protocols [Electronic resource] / C. Baum, B. David, R. Dowsley // Cryptology ePrint Archive, Report 2020/207. – 2020. – URL: https://eprint.iacr.org/2020/207

249. Bayer, D. Improving the Efficiency and Reliability of Digital Time-Stamping / Dave Bayer, Stuart Haber, W. Scott Stornetta. - 1992. - Vol. 2. - P. 329–334.

250. Bhardwaj, A. Keyloggers: silent cyber security weapons / A. Bhardwaj, S. Goundar // Network Security. – 2020. – P. 14–19.

251. Bhatia, N. A detailed review of blockchain and cryptocurrency / N. Bhatia, S. Bansal, S. Desai // CoRR. 2023 // https://arxiv.org/abs/2303.06008

252. Böhme, R. Bitcoin: Economics, technology, and governance / R. Böhme, N. Christin, B. Edelman, T. Moore // Journal of Economic Perspectives. – 2015. – Vol. 29, No. 2. – P. 213–238.

253. Brill, A. Cryptocurrencies: the next generation of terroristfinancing? / A. Brill, L. Keene // Defense Against Terrorism Review. – 2014. – Vol. 6, no. 1. – P. 7–30. Opitek, P. Selected aspects of crime involving virtual currencies / P. Opitek, A. Butor-Keler, K. Kanclerz // Terroryzm – studia, analizy, prewencja. – 2023. – P. 325–376.

254. Calafos, M. W. Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency / M. W. Calafos, G. Dimitoglou // Principles and Practice of Blockchains / ed. K. Daimi [и др.]. – Cham : Springer, 2023. – DOI: 10.1007/978-3-031-10507-4_12.

255. Chasinov, N. Mobile Advertising ID (MAID) Guide. 2024. – URL: https://www.teknicks.com/blog/capture-mobile-advertising-ids-maids/

256. Chen, W. Phishing scam detection on Ethereum: Towards financial security for blockchain ecosystem / W. Chen, X. Guo, Z. Chen, Z. Zheng, Y. Lu // IJCAI. – 2020. – P. 4506–4512.

257. Choi, W. Fractional non-fungible tokens: Overview, evaluation, marketplaces, and challenges / W. Choi, J. Woo, J.W. Hong // Int. J. Netw. Manag. – 2024. – Vol. 34. – P. e2260..

258. Choi, Y. Messenger phishing modus operandi in South Korea / Y. Choi, S. Choi // Journal of Korean Public Police and Security Studies. – 2021. – Vol. 18 (3). – P. 241–258.

259. Conti, M. Blockchain-Based Distributed and Secure Digital Forensic Investigation Systems / M. Conti, G. Kumar, C. Lal, R. Saha // Blockchains. Advances in Information Security. – Cham : Springer, 2024. – Vol. 105. – DOI: https://doi.org/10.1007/978-3-031-32146-7_11

260. Cross, C. Romance baiting, cryptorom and ‘pig butchering’: an evolutionary step in romance fraud // Current Issues in Criminal Justice. – 2024. – Vol. 36, No. 3. – P. 334-346.

261. Dhage, S. Crypto exchange Bybit confirms hack as over $1.4 billion worth of ETH leaves wallets / S. Dhage // The Block. – 2025. – February 21. – URL: https://www.theblock.co/post/342667/crypto-exchange-bybit-hacked-as-over-1-billion-worth-of-eth-leaves-wallets

262. El-Kadi, R. M. Criminal Counteraction to Encrypted Digital Currencies and Artificial Intelligence Crimes: An Analytical Study in Egyptian and Comparative Legislation / R. M. El-Kadi // Journal of Shariah and Law. - 2022. - No. 89, Article 6. - URL: https://scholarworks.uaeu.ac.ae/sharia_and_law/vol2022/iss89/6

263. Furneaux, N. There’s No Such Thing as Crypto Crime: An Investigative Handbook / N. Furneaux // URL: https://Theres-Such-Thing-Crypto-Crime/dp/1394164823

264. Ghani, M.T.A. An exploratory inquiry on the decision process of Ponzi scheme investor’s: A qualitative case study approach / M.T.A. Ghani, B.A. Halim,

S.A.A. Rahman // International Journal of Management. – 2020. – Vol. 11 (12). – P. 220-236.

265. Gomes, L.F. Direito penal estratégico / L.F. Gomes, R. Cervini. – 4. ed. – São Paulo : Revista dos Tribunais, 2008. – 656 p.

266. Grinenko, A. Comparative Legal Analysis of the Use of Electronic Format of Criminal Cases and the Procedure under the Code of Criminal Procedure of the Russian Federation / D. Ivanov, A. Grinenko, P. Fadeev [et al.] // Jurnal Cita Hukum. – 2024. – Vol. 12, No. 2. – P. 309-320. – DOI 10.15408/jch.v12i2.39691.

267. Gutiérrez-Agüero, I. et al. Burnable pseudo-identity: A non-binding anonymous identity method for ethereum // IEEE Access. – 2021. – T. 9. – P. 108912-108923.

268. Hang, S. T. Bitcoin History and Purpose / S. T. Zhang // The Potential and Limitations of Bitcoin and Ethereum. – Cham : Palgrave Macmillan, 2024. – DOI: 10.1007/978-3-031-56783-4_1.

269. Halder, D. Legal Challenges to Cryptocurrency and its Guardian-Less Victims in India: A Critical Victimological Analysis / D. Halder, A. A. Saiyed // International Annals of Criminology. – 2022. – Vol. 60, No. 1. – P. 79-98. – DOI: 10.1017/cri.2022.6.

270. Hou, Y. A survey on digital forensics in Internet of Things / Y. Hou, J. Li, J. Yu, W. Shi // IEEE Internet of Things Journal. – 2020. – Vol. 7, No. 1. – P. 1-15.

271. Irwin, A. The use of crypto-currencies in funding violentjihad / A. Irwin, G. Milad // Journal of Money Laundering Control. – 2018. – Vol. 19, iss. 4. – P. 407–425.

272. Jones, M. Book Review: Tracers in the dark: The global hunt for the crime lords of cryptocurrency / M. Jones // International Journal of Cybersecurity Intelligence & Cybercrime. – 2024. – Vol. 7, No. 1. – DOI: https://doi.org/10.52306/2578-3289.1161.

273. Jung, J. A study on pan-governmental and legislative controls related to cryptocurrency crime -Focusing on the amendments to the specific financial information act / J. Jung // The Journal of Police Science. – 2021. – Vol. 21 (1). – P. 61–89.

274. Kfir, I. Cryptocurrencies, national security, crime and terrorism / I. Kfir // Comparative Strategy. – 2020. – Vol. 39:2. – P. 113-127. – P. 119.

275. Khan, S. Network forensics: review, taxonomy, and open challenges / S. Khan, A. Gani, A.W.A. Wahab [и др.] // Journal of Network and Computer Applications. – 2016. – Vol. 66. – P. 214–235.

276. Kim, J. H. A Study on the Application of Digital Forensic Investigation for Cryptocurrency Crime / J. H. Kim, C. S. Park // Journal of Digital Forensics, Security and Law. – 2019. – Vol. 14, No. 2. – P. 45-62.

277. Koshy, T. A survey on cryptocurrency mixers / T. Koshy, S. Koshy // Journal of King Saud University - Computer and Information Sciences. – 2021. – Vol. 33(7). – P. 826–842.

278. Krause, D. The $1.4 Billion Bybit Hack: Cybersecurity Failures and the Risks of Cryptocurrency Deregulation / D. Krause. – 2025. https://ssrn.com/abstract=5150171

279. Kshetri, N. CryptoRAN: a review on cryptojacking and ransomware attacks wrt banking industry - threats, challenges, & problems / N. Kshetri, M.M. Rahman, S.A. Sayeed, I. Sultana // CoRR. 2023.

280. Lachtar, N. A cross-stack approach towards defending against cryptojacking / N. Lachtar, A.A. Elkhail, A. Bacha, H. Malik // IEEE Computer Architecture Letters. – 2020. – Vol. 19(2). – P. 126–129.

281. Lakshmanan, R. Bybit Confirms Record-Breaking $1.46 Billion Crypto Heist in Sophisticated Cold Wallet Attack/ R. Lakshmanan // The Hacker News. – 2025, February 22. – URL: https://thehackernews.com/2025/02/bybit-confirms-record-breaking-146.html

282. Larkin, C. Criminality and cryptocurrencies: Enforcement and policy responses - Part I / C. Larkin, N. Pearce, N. Shannon // Understanding Cryptocurrency Fraud / ed. S. Corbet. – (Batten-Corbet-Lucey Handbooks in Alternative Investments; vol. 2). – Germany: De Gruyter, 2021. – P. 121-131.

283. Lee, K. Recent criminal law issues on cryptocurrency / K. Lee, C. Bae // Northeast Asian Law Journal. – 2023. – Vol. 16 (4). – P. 191–217.

284. Levi, M. Understanding the laundering of organized crime money / M. Levi, M. Soudijn // Crime and Justice. – 2020. – Vol. 49. – P. 579–631. – DOI: 10.1086/708047.

285. Li, W. Digital Forensics and Cybercrime in China / W. Li, Y. Zhang // Proceedings of the International Conference on Cybercrime and Digital Forensics. – Beijing : Tsinghua University Press, 2020. – P. 123-135.

286. Lin, D. Towards Understanding Crypto Money Laundering in Web3 Through the Lenses of Ethereum Heists / D. Lin, J. Wu, Q. Fu, Y. Yu, K. Lin, Z. Zheng, S. Yang // Proceedings of the ACM SIGMETRICS Conference 2023 (SIGMETRICS'23), June 19–23, 2023, Orlando, Florida, USA. – New York, NY, USA: ACM, 2023. – P. 21

287. Ly, K. M. Coining Bitcoin's 'legal-bits': Examining the regulatory framework for Bitcoin and virtual currencies / K. M. Ly // Harvard Journal of Law and Technology. – 2014. – Vol. 27, No. 2. – P. 587–608.

288. Medina, M. Inteligencia de fuente abierta / M. Medina // Basel Institute of Governance, Quick Guide Series. – 2020. – No. 17. – June.

289. Mezquita, Y. Cryptocurrencies, systematic literature review on their current context and challenges / Y. Mezquita, M. Plaza-Hernández, M. Abbasi, J. Prieto // International Congress on Blockchain and Applications. – 2023. – Vol. 595. – P. 162-172.

290. 论刑事涉案虚拟货币处置2024 年 11 月 第 46 卷 第 6 期// Modern Law Science – URL: https://qks.swupl.edu.cn/docs//2024-12/eba75d539970461.pdf

291. Mukherjee, S. Cryptocurrency Ponzi schemes / S. Mukherjee, C. Larkin, S. Corbet // Understanding Cryptocurrency Fraud: THe Challenges and Headwinds to Regulate Digital Currencies. – 2021. – Vol. 2. – P. 111.

292. Nazzari, M. From payday to payoff: Exploring the money laundering strategies of cybercriminals / M. Nazzari // Trends in Organized Crime. – 2023. – DOI: 10.1007/s12117-023-09505-w.

293. Neumann, P. Don't follow the money: The problem with the war on terrorist financing / P. Neumann // Foreign Affairs. – 2017. – Vol. 96 (4). – P. 93-102.

294. Nimalendran, M. Informational Efficiency of Cryptocurrency Markets / M. Nimalendran, P. Pathak, M. Petryk, L. Qiu // Journal of Financial and Quantitative Analysis. – 2024. – P. 1-30.

295. Opiatek, P. Cryptocurrencies in the aspects of police investigative activities / P. Opiatek // Przegląd Policyjny. – 2017. – № 2. – P. 138–158.

296. Oranburg, S. C. Cryptocurrency Regulation / S. C. Oranburg // A History of Financial Technology and Regulation: From American Incorporation to Cryptocurrency and Crowdfunding. – Cambridge: Cambridge University Press, 2022. – P. 129-152.

297. Pastor-Galindo, J. The not yet exploited goldmine of OSINT: opportunities, open challenges and future trends / J. Pastor-Galindo, P. Nespoli, F.G. Mármol, G.M. Pérez // IEEE Access. – 2020. – Vol. 8. – P. 10282–10304.; Hayes, D.R. Open-source intelligence for risk assessment / D.R. Hayes, F. Cappa // Business Horizons. – 2018. – Vol. 61, № 5. – P. 689–697.

298. Prado-Romero, M.A. Discovering Bitcoin Mixing Using Anomaly Detection / M.A. Prado-Romero, C. Doerr, A. Gago-Alonso // Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications. CIARP 2017. Lecture Notes in Computer Science, vol 10657 / ed. by M. Mendoza, S. Velastín. – Cham: Springer, 2018. – DOI: https://doi.org/10.1007/978-3-319-75193-1_64

299. Qureshi, S.U. Systematic review of deep learning solutions for malware detection and forensic analysis in IoT / S.U. Qureshi, J. He, S. Tunio, N. Zhu, A. Nazir, A. Wajahat, F. Ullah, A. Wadud // Journal of King Saud University - Computer and Information Sciences. – 2024. – Vol. 36, Issue 8. – P. 102164.

300. Raud, T.H. Combating money laundering using cryptocurrencies: a comparative analytical study / T. H. A. Raud // Journal of the Center for Rule of Law and Anti-Corruption. - 2024. - № 1.

301. Riley, J. The Current Status of Cryptocurrency Regulation in China and Its Effect around the World / J. Riley // China and WTO Review. – 2021. – Vol. 7. – P. 135-152.

302. Scharfman, J. Cryptocurrency Ponzi, Pyramid, and MLM Schemes: Part 1 / J. Scharfman // The Cryptocurrency and Digital Asset Fraud Casebook . – Cham: Palgrave Macmillan, 2023. – DOI: https://doi.org/10.1007/978-3-031-23679-2_3

303. Scharfman, J. Introduction to Cryptocurrency and Digital Asset Fraud and Crime / J. Scharfman // The Cryptocurrency and Digital Asset Fraud Casebook. – Cham : Palgrave Macmillan, 2023. – DOI: 10.1007/978-3-031-23679-2_1.

304. Shafee, S. Evaluation of LLM-based chatbots for OSINT-based Cyber Threat Awareness / S. Shafee, A. Bessani, P.M. Ferreira // Expert Systems with Applications. – 2025. – Vol. 261. – P. 125509.

305. Shaik, C. Securing cryptocurrency wallet seed phrasedigitally with blind key encryption / C. Shaik // International Journal on Cryptography and Information Security (IJCIS). – 2020. – Vol. 10. - No. 4.

306. Sharad Mangrulkar, R. Bitcoin / R. Sharad Mangrulkar, P. Vijay Chavan // Blockchain Essentials. – Berkeley, CA : Apress, 2024. – DOI: 10.1007/978-1-4842-9975-3_3.

307. صدقر, وفاء. دور العملات الافتراضية المشفرة في جريمة غسل الأموال وتمويل الإرهاب // مجلة البحوث الفقهية والقانونية. ٢٠٢٤. ٤٦. ١٤٠٥-١٥٠٣.

308. Sharma, A. Simulating data breaches: Synthetic datasets for depicting personally identifiable information through scenario-based breaches / A. Sharma, M. Bantan // Data in Brief. – 2025. – Vol. 58. – 111207.

309. Stathakopoulou, C. Adding Fairness to Order: Preventing Front-Running Attacks in BFT Protocols using TEEs / C. Stathakopoulou, S. Rüsch, M. Brandenburger, M. Vukolic // 2021 40th International Symposium on Reliable Distributed Systems (SRDS). – 2021. – P. 34-45.

310. Sun, T. A Formal Verification Framework for Security Issues of Blockchain Smart Contracts / T. Sun, W. Yu // Electronics. – 2020. – Vol. 9. – P. 255. – DOI: 10.3390/electronics9020255.

311. Sun, Z. An analysis on the characteristics of “Pig-Butchering Scam” and anti-fraud strategy / Z. Sun, L. Yu // Journal of Jiangsu Police Institute. – 2022. – Vol. 2. – P. 86–92.

312. Suratkar, S. Cryptocurrency Wallet: A Review / S. Suratkar, M. Shirole, S. Bhirud // 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 2020. – P. 1-7.

313. Toulas, B. Millions of GitHub repos likely vulnerable to RepoJacking, researchers say / B. Toulas. – 2023. – URL: https://www.bleepingcomputer.com/news/security/millions-of-github-repos-likely-vulnerable-to-repojacking-researchers-say/

314. Trozze, A. Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering / A. Trozze, T. Davies, B. Kleinberg // Forensic Science International: Digital Investigation. – 2023. – Vol. 46. – 301575. –DOI: https://doi.org/10.1016/j.fsidi.2023.301575.

315. Varun, V.M. Prospects and Models of Combating Cryptocurrency Crimes. The India-EU Dialogue as a Perspect // URL: https://eucrim.eu/articles/prospects-and-models-of-combating-cryptocurrency-crimes/

316. Wang, F. Persuasive schemes for financial exploitation in online romance scam: an Anatomy on Sha Zhu pan (杀猪盘) in China / F. Wang, X. Zhou // Vict Offenders. – 2023. – Vol. 18(5). – P. 915–942.

317. Wang, F. Victim-offender overlap: the identity transformations experienced by trafficked Chinese workers escaping from pig-butchering scam syndicate / F. Wang // Trends Organ Crim. - 2024. – DOI: https://doi.org/10.1007/s12117-024-09525-5

318. Wang, H. M. Cryptocurrency is new vogue: a reflection on money laundering prevention / H. M. Wang, M. L. Hsieh // Security Journal. – 2024. – Vol. 37. – P. 25–46.

319. Wang, M. Lightweight and manageable digital evidence preservation system on Bitcoin / M. Wang, Q. Wu, B. Qin [и др.] // Journal of Computer Science and Technology. – 2018. – Vol. 33. – P. 568–586. – DOI: 10.1007/s11390-018-1841-4.

320. Weber, M. Untangling Bitcoin: Exploring the Structure of the Bitcoin Transaction Graph / M. Weber, D. D. Gramlich, F. Streitz, R. State // Security and Communication Networks. – 2019.

321. Wood, G. Advancing egalitarianism / G. Wood, A. Buchanan // Handbook of Digital Currency. – Cambridge: Academic Press, 2015. – P. 385–402.

322. Wronka, C. Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight / C. Wronka // J Bank Regul. – 2024. – Vol. 25. – P. 84–93. – DOI: 10.1057/s41261-023-00217-8.

323. Xiao, N. A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things / N. Xiao, Z. Wang, X. Sun, J. Miao // Alex. Eng. J. – 2024. – Vol. 86. – P. 631–643..

324. Xie, Z. «Why did I fall for it?» Exploring internet fraud susceptibility in the pig butchering scam / Z. Xie, Z. Duan // Secur J. – 2025. – Vol. 38, 9. – DOI: https://doi.org/10.1057/s41284-024-00457-x

325. Xu, S. Blockchain-based secure data sharing with overlapping clustering and searchable encryption / S. Xu, S. Dong, L. Wang, M.J. Mihaljević, S. Zhang, W. Shao, Q. Wang // Computer Standards & Interfaces. – 2025. – Vol. 93. – P. 103979.

326. Yamin, M.M. Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security / M.M. Yamin, M. Ullah, H. Ullah, B. Katt, M. Hijji, K. Muhammad // Mathematics. – 2022. – Vol. 10, No. 12. – P. 2054.

327. Zhang, Q. Auditable and dynamic access control scheme with behavior and identity tracing / Q. Zhang, L. Yuan, T. Xie, H. Chen // Computer Networks. – 2024. – T. 251. – P. 110623.

328. Zheng, B. Identifying the vulnerabilities of Bitcoin anonymous mechanism based on address clustering / B. Zheng, L. Zhu, M. Shen [и др.] // Science China Information Sciences. – 2020. – Vol. 63, 132101. – DOI: 10.1007/s11432-019-9900-9.

Диссертации и авторефераты диссертаций

329. Астахова, Е.А. Криминалистическая классификация транснациональных преступлений и ее использование в расследовании: диссертация на соискание ученой степени кандидата юридических наук / Астахова Екатерина Алексеевна, 2023. – 215 с.

330. Бабакова, М.А. Проблемы розыска при расследовании преступлений в сфере высоких технологий : дис. … канд. юрид. наук / Бабакова Мария Алексеевна. – Саратов, 2010. – 268 с.

331. Васильева О.А. Организационно-тактические основы проверки криминалистически значимой информации при расследовании преступлений: дис. … канд. юрид. наук. Калининград, 2022. – 199 с.

332. Гаврилин, Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики : теоретические, организационно-тактические и методические основы : автореф. дис. … д-ра юрид. наук / Гаврилин Юрий Викторович. – Москва, 2010. – 55 с.

333. Гаспарян, Г.З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : дис. … канд. юрид. наук / Гаспарян Гурген Зорикович. – 2021. – 300 с.

334. Гаспарян, Г.З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : автореф. дис. … канд. юрид. наук / Гаспарян Гурген Зорикович. – Москва, 2020. – 30 с.

335. Долгиева, М. М. Теоретические основания уголовной политики в сфере оборота криптовалюты: дис. … д-ра юрид. наук / Долгиева Мадина Муссаевна. – Москва, 2023. – 474 с.

336. Коломинов, В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : автореф. дис. … канд. юрид. наук / Коломинов Вячеслав Валентинович. – Краснодар, 2017. – 25 с.

337. Коновалов, С.И. Теоретико-методологические основы криминалистики (Современное состояние и проблемы развития): дис. … д-ра юрид. наук / Коновалов Станислав Иванович. – Волгоград, 2001. – 269 с.

338. Мазуров, И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий : автореф. дис. … канд. юрид. наук / Мазуров Игорь Евгеньевич. – Ростов-на-Дону, 2017. – 24 с.

339. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис…д-ра юрид. наук. - Воронеж, 2001. – 39 с.

340. Образцов В.А. Проблемы совершенствования научных основ методики расследования преступлений: автореф. дис. ... канд. юрид. наук. М., 1985.

341. Перов, В.А. Квалификация преступлений, совершаемых с использованием криптовалюты: дис. … канд. юрид. наук / Перов Валерий Александрович. – 2023. – 261 с.

342. Перов, В.А. Квалификация преступлений, совершаемых с использованием криптовалюты : автореф. дис. … канд. юрид. наук / Перов Валерий Александрович. – Москва, 2023. – 25 с.

343. Старостенко, Н.И. Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий : дис. … канд. юрид. наук / Старостенко Нина Игоревна. – Краснодар, 2023. – 230 с.

344. Шаевич, А.А. Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений : дис. … канд. юрид. наук / Шаевич Антон Александрович. – Иркутск, 2007. – 195 с.

345. Шуклин, А. Е. Особенности принятия информационных и тактических решений в сложных следственных ситуациях : дис. … канд. юрид. наук / Шуклин Александр Евгеньевич. – Екатеринбург, 2012. – 211 с.

Электронные ресурсы

346. Официальный сайт Верховного Суда Российской Федерации [Электронный ресурс] Режим доступа: http://www.vsrf.ru

347. Официальный сайт Судебного департамента при Верховном Суде Российской Федерации [Электронный ресурс] Режим доступа: http://www.cdep.ru

348. Официальный сайт МВД РФ [Электронный ресурс] Режим доступа: https://мвд.рф

349. Официальный сайт Следственного комитета Российской Федерации [Электронный ресурс] Режим доступа: http://sledcom.ru.

350. Судебные и нормативные акты РФ - портал [Электронный ресурс] Режим доступа: http://sudact.ru

351. Параграф-WWW - информационно-правовая система [Электронный ресурс] Режим доступа: http://online.zakon.kz

352. Справочно-правовая система «КонсультантПлюс».

353. Справочно-правовая система «Гарант».

Приложение №1

РЕЗУЛЬТАТЫ АНКЕТИРОВАНИЯ

В ходе диссертационного исследования по теме «Раскрытие и расследование преступлений, совершаемых в отношении и с использованием криптовалюты» было опрошено 274 респондента, из которых 199 сотрудника следственных подразделений и 46 сотрудников, уполномоченных осуществлять оперативно-розыскную деятельность

1. Должность, которую Вы занимаете			
1.	Следователь, старший следователь МВД России	153	56%
2.	Оперуполномоченный, старший оперуполнолномоченный, оперуполномоченный по особо важным делам	75	28%
3.	Следователь, старший следователь, следователь по особо важным делам СК России	46	17%
2. Стаж работы			
1.	До 1 года	48	17%
2.	От 1 до 3 лет	94	34%
3.	От 3 до 5 лет	62	23%
4.	От 5 до 10 лет	36	14%
5.	Более 10 лет	34	12%
3. Считаете ли Вы криптовалютную среду значимым источником криминалистически значимой информации при расследовании преступлений?			
1.	Да, безусловно	233	85%
2.	Скорее да, чем нет	33	12 %
3	Скорее нет, чем да	5	2 %
4.	Нет, не считаю	3	1 %
4. Как часто Вы используете информацию из блокчейна при расследовании преступлений?			
1.	Почти всегда	55	20%
2.	Часто	123	45%
3.	Иногда	69	25 %
4.	Редко	22	8 %
5.	Никогда	5	2%
5. Какие виды информации из блокчейна вы считаете наиболее полезными для расследования?			

1.	История транзакций	192	70%
2.	Адреса кошельков	164	60%
3.	Временны´е метки транзакций	123	45%
4.	Суммы транзакций	151	55%
5.	Другое	14	5%
6. Считаете ли Вы, что необходимо специальное обучение для работы с информацией из блокчейна?			
1.	Да, обязательно	247	90%
2.	Желательно	22	8%
3.	Не обязательно	5	2%
7. Какие элементы инфраструктуры криптовалюты наиболее часто используются преступниками?			
1.	Криптокошельки	206	75%
2.	Миксеры криптовалют	110	40%
3.	P2P-платформы	82	30%
4.	Криптобиржи	178	65%
8. Какие следы чаще всего остаются после совершения преступлений, связанных с криптовалютой?			
1.	Записи о транзакциях в блокчейне	178	65%
2.	IP-адреса	110	40%
3.	Данные о регистрации на криптобиржах	37	50%
4.	Переписка в мессенджерах	96	35%
9. Считаете ли Вы, что необходима разработка новых методов, адаптированных под криптовалютную среду?			
1.	Да	260	95%
2.	Нет	14	5%
10. Как Вы считаете, необходимо ли усилить международное сотрудничество в борьбе с криптовалютной преступностью?			
1.	Да	269	98%
2.	Нет	5	2%
11. Считаете ли Вы, что для успешного раскрытия криптовалютных преступлений необходимо привлекать специалистов в области IT и блокчейн-технологий?			
1.	Да	26	95%

		0	
2.	Нет	14	5%
12. Какие проблемы возникают при получении информации от криптобирж?			
1.	Долгое время ожидания ответа	137	50%
2.	Отказ в предоставлении информации	55	20%
3.	Неполнота предоставляемой информации	82	30%
13. Какие сложности возникают при раскрытии и расследовании криптопреступлений?			
1.	Сложность установления личности злоумышленника	164	60%
2.	Сложность доказывания умысла	110	40%
3.	Сложность доказывания причинно-следственной связи	82	30%
14. Какие основные риски вы видите при привлечении подозреваемого к осмотру места происшествия в делах, связанных с криптоактивами?			
1.	Сокрытие или уничтожение цифровых следов	233	85%
2.	Несанкционированный доступ к криптоактивам	205	75%
3.	Использование участия для противодействия расследованию	178	65%
4.	Рисков не вижу	6	2%
5.	Другое	63	23%
15. В каких случаях, по Вашему мнению, целесообразно привлекать подозреваемого к осмотру места происшествия в делах, связанных с криптовалютой?			
1.	Для установления местонахождения виртуальных активов	192	70%
2.	Для получения кодов доступа к криптокошелькам	164	60%
3.	Для идентификации криптокошельков и транзакций	110	40%
4.	Всегда целесообразно	68	25%
5.	Никогда не целесообразно	14	5%
16. Как часто при анализе профилей пользователей в крипто-приложениях вам удается идентифицировать реальные имена, привязанные абонентские номера или адреса электронной почты, несмотря на использование псевдонимов?			
1.	Всегда	8	3%
2.	Часто	82	30%
3.	Иногда	47	17%
4.	Редко	137	50%