V УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ

Научная статья
УДК 343.98
DOI: 10.47475/2411-0590-2024-11-4-576-586

Особенности противодействия расследованию преступлений, совершенных с использованием криптовалюты в Российской Федерации

Василий Владимирович Векленко[1], **Анна Михайловна Чихрадзе**[2]

[1] *Санкт-Петербургский государственный университет, Санкт-Петербург, Россия*
veklenkovv@yandex.ru
https://orcid.org/0000-0003-1373-6271

[2] *Санкт-Петербургский университет МВД РФ, Санкт-Петербург, Россия*
anna.chikhradze@mail.ru
https://orcid.org/0009-0000-0763-2228

Аннотация. Статья посвящена анализу проблем противодействия расследованию преступлений, совершенных с использованием криптовалюты. В работе освещаются теоретические положения противодействия, точки зрения исследователей разных лет относительно его основных общих признаков. Внимание уделяется ряду объективно существующих факторов, которые способствуют оказанию противодействия следствию по данной категории дел (децентрализованный характер криптовалютных операций, анонимность, неоднородность ее правового регулирования). Выделены кибервиктимологические характеристики жертв криптопреступлений, включающие низкую цифровую грамотность, доверчивость и недостаточную защиту данных. Совершение указанной группы преступлений сопровождается рядом особенностей ввиду особой сферы существования и оборота криптовалюты. Отсюда, нетрадиционное образование следовой картины, а также специфика форм и видов противодействия следствию. В работе предлагается рассматривать формы противодействия расследования преступлениям, совершенным с использованием криптовалют в ключе технической и юридической форм противодействия. Техническая форма противодействия предполагает использование специализированного программного обеспечения для сокрытия или уничтожения электронно-цифровых следов. В контексте рассмотрения юридических форм противодействия акцентируется внимание, в том числе на особенностях процессуальной фиксации обнаружения и изъятия электронно-цифровых следов для минимизации возможностей юридического противодействия расследованию преступлений, совершенных с использованием криптовалют. Работа подчеркивает значимость комплексного подхода к расследованию криптопреступлений для повышения эффективности следственных мероприятий.

Ключевые слова: противодействие расследованию, криптовалюты, блокчейн, жертва преступления, виктимизация, анонимность, децентрализация, техническое противодействие, юридическое противодействие, криптопреступления

Для цитирования: Векленко В. В., Чихрадзе А. М. Особенности противодействия расследованию преступлений, совершенных с использованием криптовалюты в Российской Федерации // Виктимология. 2024. Т. 11, № 4. С. 576–586. DOI: 10.47475/2411-0590-2024-11-4-576-586

Research article

Features of Countering the Investigation of Crimes Committed Using Cryptocurrency in the Russian Federation

Vasilij V. Veklenko[1], **Anna M. Chikhradze**[2]

[1] *St. Petersburg State University, Saint Petersburg, Russia*
veklenkovv@yandex.ru
https://orcid.org/0000-0003-1373-6271

[2] *Saint Petersburg University of the MIA of Russia, Saint Petersburg, Russia*
anna.chikhradze@mail.ru
https://orcid.org/0009-0000-0763-2228

Abstract. The article is devoted to the analysis of the problems of countering the investigation of crimes committed using cryptocurrency. The paper highlights the theoretical positions of counteraction, the points of view of researchers from different years regarding its main common features. Attention is paid to a number of objectively existing factors that contribute to countering the investigation of this category of cases (the decentralized nature of cryptocurrency transactions, anonymity, and the heterogeneity of its legal regulation). Cybervictimological characteristics of victims of cryptoprimes are highlighted, including low digital literacy, credulity and insufficient data protection. The commission of this group of crimes is accompanied by a number of features due to the special sphere of existence and turnover of cryptocurrency. Hence, the unconventional formation of the trace pattern, as well as the specifics of the forms and types of counteraction to the investigation. The paper proposes to consider the forms of countering the investigation of crimes committed using cryptocurrencies in the key of technical and legal forms of counteraction. The technical form of counteraction involves the use of specialized software to conceal or destroy electronic and digital traces. In the context of the consideration of legal forms of counteraction, attention is focused, among other things, on the features of the procedural fixation of the detection and seizure of electronic digital traces in order to minimize the possibilities of legal counteraction to the investigation of crimes committed using cryptocurrencies. The work highlights the importance of an integrated approach to the investigation of cryptocrimes in order to increase the effectiveness of investigative measures.

Keywords: counteraction to investigation, cryptocurrencies, blockchain, victimization, victimization, anonymity, decentralization, technical counteraction, legal counteraction, cryptocrime

For citation: Veklenko VV, Chikhradze AM. Features of countering the investigation of crimes committed using cryptocurrency in the Russian Federation. *Viktimologiya* [Victimology]. 2024;11(4):576-586. (In Russ.) DOI: 10.47475/2411-0590-2024-11-4-576-586

Введение

Криптовалюта представляет собой децентрализованный цифровой актив, основанный на блокчейн-технологии, использование которого в механизме совершения преступления ставит новые задачи перед правоприменителями не только в сфере противодействия преступлениям, совершаемым с использованием криптовалюты, но и требует анализа с позиции кибервиктимологии. Специфические особенности криптовалют — анонимность, децентрализация, сложность отслеживания и отсутствие сегодня системности правового регулирования — создают уникальные вызовы для расследования преступлений, усложняя процесс доказывания, проведения следственных действий, увеличивая возможности оказания противодействия следствию. Эти факторы также требуют особых подходов к профилактической работе.

Особое внимание в данном исследовании уделено противодействию расследованию преступлений, совершенных с использованием криптовалюты. Теоретическая и прикладная необходимость осмысления проблем сокрытия следов преступлений детерминировала активизацию внимания ученых в отношении проблем противодействия расследованию как общей теории, начиная с 70-х годов [2, с. 49; 3, с. 160]. В отношении же частных криминалистических методик тема исследования продолжает оставаться актуальной и сегодня, поскольку в науке и практике отмечаются системные качественные изменения преступности (в том числе в сторону ее цифровизации, процент раскрываемости которой крайне мал[1]) с положительной динамикой роста из года в год [15, с. 90]. Все это влечет за собой необходимость модернизации мер противодействия следствию.

В данной статье, опираясь на работы отечественных ученых и новейшие исследования в области кибервиктимологии, авторы рассматривают специфические аспекты противодействия расследованию преступлений, совершаемых с использованием криптовалют, а также виктимологические характеристики жертв этих преступлений, выявленные на основе анализа следственной и судебной практики в Санкт-Петербурге за период 2021–2023 гг.

Материал и методы

При написании статьи произведен анализ специальной литературы, посвященной вопросам особенностей расследования преступлений, совершенных с использованием криптовалюты, противодействия расследованию этой категории преступлений, а также материалов следственной и судебной практики в том числе с целью выявления особых характеристик жертв указанных преступлений, которые способствуют не только совершению криптопреступлений, но и укрепляют желание и уверенность лица в необходимости оказания противодействия следствию. Свои работы указанным вопросам в разные годы посвятили российские ученые Т. В. Аверьянова, Р. С. Белкин, А. А. Бибиков, А. В. Волобуев, А. Ю. Головин, С. Ю. Журавлев, А. М. Кустов, Е. О. Москвин, Г. К. Синилов, О. Б. Стулин, Н. П. Яблоков и др.

В качестве специальных исследовательских методов использованы: диалектический и формально-логический методы, логико-семантический, системный анализ.

Результаты исследования и обсуждение

Проведенный в данной работе анализ научных источников позволяет утверждать, что вопросу противодействия расследования преступлений уделяется значительное внимание в науке. Однако, единого мнения на счет того, что же понимается под противодействием при расследовании преступлений сегодня, нет. Не ставя перед собой цель приводить все определения, которые даны в научной литературе, перед исследованием особенностей противодействия преступлений, совершенным с использованием криптовалюты, выделим несколько подходов разных лет в интерпретации общегопонятия противодействия расследования преступлению, а также рассмотрим его основные характеристики.

[1] В Генпрокуратуре заявили о низкой раскрываемости киберпреступлений в России // РИА Новости. URL: https://ria-ru.turbopages.org/turbo/ria.ru/s/20241010/kiberprestuplenie-1977431676.html (дата обращения: 23.10.2024).

Р.С. Белкин определял, что под противодействием расследованию преступлений необходимо понимать умышленную деятельность с целью воспрепятствования решению задач расследования и, в конечном счете, установлению истины по делу [10, с. 59]. По мнению В.Н. Карагодина, «противодействие предварительному расследованию — это умышленные действия (система действий), направленные на воспрепятствование установления объективной истины по делу, достижению других целей предварительного расследования» [7, с. 39]. А.Ю. Головин под противодействием расследованию понимает умышленную деятельность (сложную систему действий, бездействия) преступников и связанных с ними лиц, препятствующую работе правоохранительных органов по раскрытию и расследованию конкретных преступлений [5, с. 147].

В силу отмеченного ранее многообразия мнений авторов относительно содержательного определения «противодействие расследованию преступлений» видится целесообразным также рассмотреть исследуемое понятие через его основные общие признаки, на которых ученые в разное время акцентировали свое внимание:

1. Противодействие расследованию преступления может осуществляться как в активной форме, так и пассивной (С.Ю. Журавлев) [6, с. 9–10].

2. Противодействие расследованию преступлений совершается умышленно (И.А. Климов, Г.К. Синилов) [9, с. 22].

3. Действия, составляющие содержание противодействия расследованию преступлений, не обязательно являются противоправными (В.Н. Карагодин) [8, с. 26].

4. Противодействие расследованию преступлений может осуществляться как самим подозреваемым/обвиняемым, так и третьими лицами (О.Б. Стулин) [14, с. 26].

5. Цель противодействия расследованию — уклонение от уголовной ответственности либо ее существенное смягчение (О.Б. Стулин, А.Ф. Волобуев, Е.О. Москвин) [4, с. 42; 12, с. 140].

6. Цель противодействия расследованию — дезорганизация работы органов следствия (А.М. Кустов) [11, с. 54].

Отметив с содержательной точки зрения в общих чертах характерные признаки и особенности противодействия расследованию преступлений, рассмотрим их через призму частной методики в части видов и форм противодействия преступлениям, совершенным с использованием криптовалют. Количество подобных совершенных преступлений находится в положительной динамике, что подтверждается статистическими данными, в том числе и отчетами международных организаций[1]. В свою очередь, расследование преступлений, совершаемых с использованием криптовалют имеет свои характерные особенности, которые выделяют их, обуславливая сложности обнаружения, фиксации и изъятия криминалистически значимой информации, перевод ее в поле доказательств, а также наличие ряда объективно-субъективных факторов, которые способствуют и укрепляют желание оказывать противодействие следствию.

Стоит отметить, что факторы, способствующие оказанию противодействия расследованию преступлений, совершенных с использованием криптовалют находятся в правовом поле, то есть не носят противозаконного характера. Однако, само их объективное существование в силу специфики криптовалюты, механизма ее обращения и условий платформ, привлекает лиц для осуществления противоправных действий, а в будущем создают для следствия объективные трудности в установлении обстоятельств, подлежащих доказыванию.

К подобным факторам следует относить:

1. Децентрализацию и анонимность криптовалютных транзакций. Децентрализация как фактор, способствующий оказанию виновным противодействия при расследовании криптопреступлений, подразумевает, что в механизм функционирования распределенных реестров данных и обращения криптовалюты не включено такое звено, как единый контролирующий

[1] См.: 2023 Crypto Crime Mid-year Update: Crime Down 65% Overall, But Ransomware Headed for Huge Year Thanks to Return of Big Game Hunting // Chainalysis. URL: https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/ (дата обращения: 23.10.2024).

орган либо его суррогаты. Контроль внутри распределенных реестров осуществляют сами пользователи, что существенно затрудняет получение криминалистически знаний информации в рамках оперативно-розыскных мероприятий и предварительного расследования.

Под анонимностью необходимо понимать, что в распределенном реестре данных скрыты персональные данные пользователей, а идентификация пользователя возможна исключительно по номеру криптокошелька либо хэша транзакции (если они в открытом доступе. Для анонимных криптовалют и эти данные скрыты). Как справедливо отмечается в криминологических исследованиях, анонимность криптовалютных операций снижает ощущение риска быть обнаруженным, поощряя при этом преступное поведение [16, с. 31].

2. Бессистемность в правовом регулировании. Отсутствие единого законодательного подхода к нормативному определению статуса и функционирования криптовалют как в национальном, так и международном законодательстве создает некие правовые вакуумы, которые используются лицами в их противоправной деятельности, и создают ряд трудностей для правоохранителей в части получения криминалистически значимой информации в ходе следствия. Криптоиндустрия развивается настолько динамично, что появляются различные новые инструменты ее рынка(децентрализованные биржи, DeFi-платформы), которые не совсем вписываются в правовое регулирование финансового рынка, что влечет за собой появление неких «лазеек», которые укрепляют уверенность лица в необходимости оказания противодействия следствию.

Переходя к формам противодействия расследованию преступлений, совершенных с использованием криптовалют, необходимо отметить целесообразность их исследования не столько в традиционных формах противодействия — активной и пассивной, а учитывая особенности сферы совершения преступлений — в ключе технического и юридического противодействия.

Техническое противодействие расследованию преступлений с использованием криптовалют непосредственно связано с использованием современных высоких технологий и специализированных инструментов, которые позволяют в значительной мере затруднять процесс получения криминалистически значимой информации следствием:

— использование высокотехнологичных средств сокрытия персональных данных. Наличие электронно-цифровых следов не всегда гарантирует возможность установление конкретного лица, оставившего их. Такие современные цифровые инструменты как VPN (виртуальные частные сети), TOR (анонимные сети) позволяют сокрыть реальное местоположение, деятельность лица в сети Интернет, персональные данные, что существенно затрудняет идентификацию лица и отслеживание его активности;

— использование специальных сервисов и инструментов для маскировки транзакций, которые в ряде случаев заложены в виде смарт-контракта в распределенном реестре данных. Подобными сервисами являются так называемые «миксеры криптовалют». Они представляют собой онлайн-сервисы, которые дробят транзакцию и смешивают ее с транзакциями других пользователей блокчейн-технологии.

Использование таких инструментов значительно усложняет отслеживание транзакций и вызывает необходимость прибегать в блокчейн-анализу, в том числе используя метод анализа «входа-выхода» (input-output analysis). Он предполагает выявление связи между источниками средств, адресами криптокошельков отправителя и получателя, которые принимают участие в совершении транзакции для определения движения криптовалюты между ними и, соответственно, установления связей.

Каждая транзакция в системе блокчейн отличается от традиционной сделки тем, что имеет несколько входов — источников средств, а также несколько выходов, указывающих на адреса получателей. Отслеживание входов позволяет установить источники получения средств на адрес кошелька отправителя, в свою очередь, отслеживание выходов — движение криптовалюты до конечного ее получателя. Метод анализа «входа-выхода» позволяет связать

адреса криптокошельков, которые участвуют в транзакциях, объединять их в кластеры с целью выявления общих паттернов и одних и тех же участников нескольких сделок. Именно описанный метод целесообразно использовать для выявления отмывания денежных средств в блокчейн-системе, мошенничества, финансирования терроризма и др.

Однако нельзя с уверенностью утверждать, что использование лицом подобных продуктов обусловлено необходимостью скрыть сведения о транзакциях, поскольку это может быть лишь одним из обязательных условий функционирования платформы:

1. *Использование анонимных криптовалют*. Созданные с целью полной анонимности криптовалюты (например, Monero) используют технологии скрытых адресов и кольцевых подписей (ring signatures). Кольцевые подписи являются криптографическим методом, который возводит анонимность на новый уровень — никто, включая получателя криптовалюты не может установить адрес отправителя. Под кольцом в данном случае понимается совокупность публичных ключей, лишь один из которых — отправитель криптовалюты;

2. *Уничтожение цифровых следов*. Указанная форма противодействия является ключевым методом, использующимся лицами и предусматривает их уничтожение в том числе и с помощью специального программного обеспечения:

a) удаление логов серверов, то есть файлов, в которых записывается и содержится информация о всей работе системы (данные о входах, выходах, IP-адресах, времени доступа и действиях пользователей). Стоит отметить, что в целях противодействия логи могут быть как удалены, так и изменены;

b) уничтожение данных на устройстве — после завершения необходимых операций лица могут уничтожить имеющиеся на устройстве электронно-цифровые следы физически путем уничтожения самого устройства. Также уничтожение возможно с помощью специального программного обеспечения, которое стирает данные с жёсткого диска, с невозможностью ее восстановления (wiping software), в том числе вследствие того, что программы для стирания данных многократно перезаписывают данные на носителе;

c) шифрование данных посредством использования специального программного обеспечения. Для получения информации, зашифрованной указанным способом необходимы специальные ключи. В противном случае она является недоступной для чтения (ознакомления, копирования).

Стоит отметить, что использование технических форм противодействия расследования преступлений, совершенных с использованием криптовалют, создает серьезные препятствия для следствия, поскольку даже при наличии необходимых правовых инструментов доступ к криминалистически значимой информации может быть физически невозможен, в том числе из-за полного или частичного ее уничтожения.

Противодействие расследованию преступлений, совершенных с использованием криптовалют на юридическом уровне заключатся в использовании стратегии противодействия следствию законными способами, а также используя состояние законодательства в этой сфере. В контексте противодействия исследуемой группе преступлений эта форма противодействия приобретает особую актуальность ввиду двух ее аспектов.

Один из них упоминался ранее — неоднозначность правового положения криптовалюты. Сегодня на законодательном уровне правовое положение криптовалюты как цифровой валюты установлено в Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[1]. Она не признана денежным средством либо его суррогатом, и использовать ее именно в качестве платежного средства запрещено законом (хотя 5 сентября 2024 года в России открылся криптовалютный

[1] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31.07.2020 № 259-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 23.10.2024).

банк[1]). В то же время лица вправе ею владеть на праве собственности.

Столкнувшись с криптовалютой и сферой ее функционирования, следствие быстро адаптировалось в применении существующих норм уголовно-процессуального законодательства в части особенностей производства отдельных следственных действий. Например, осмотр предметов и документов имеет ряд существенных отличий как собственно в проведении самого осмотра и в обнаружения доказательственной информации, так и в процессуальном оформлении его результатов в части фиксации в протоколе следственного действия.

Фиксация электронно-цифровых следов при расследовании преступлений, связанных с использованием криптовалют, производится в рамках осмотра предметов и документов по правилам ст. 166 УПК РФ[2]. К необходимым с точки зрения фиксации сведениям необходимо относить:

1) адрес криптокошелька — идентификатор, необходимый для осуществления операций в распределённых реестрах данных. Именно адрес криптокошелька позволит отследить движение криптовалюты в рамках совершения транзакции и кошельки отправителя/получателя;

2) историю транзакций. Если мы говорим об открытом распределённом реестре данных, то он содержит сведения о каждой транзакции, которая была проведена. Таким образом, к сведениям, относящимся к истории транзакции, которые необходимо зафиксировать в протоколе, следует отнести: хэш транзакции (ее номер), время проведения транзакции; сумму перевода; адреса отправителей и получателей; комментарии, если они были добавлены к транзакции. В ключе установления времени совершения транзакции необходимо отметить, что ее совершение может занять определенное время, поскольку транзакционные блоки выстаиваются в цепочку после их подтверждения и осуществляются в последовательности (чем больше заявлена комиссия по транзакции, там больше вероятность быстрого ее завершения). Именно поэтому мнения относительно «быстроты» совершения криптовалютной сделки не совсем верны и целесообразно отмечать в протоколе осмотра как изменялся баланс криптокошелька в интересующий следствие период времени [13, с. 367]. Также следует отметить, что если криптокошелёк в своей активности использует платформы со смарт-контрактами, как, например, Ethereum, фиксация информации о них необходима, поскольку позволит воспроизвести структуру совершённых сделок;

3) данные о балансе криптокошелька и их изменениях в интересующие следствие сроки;

4) приватные и публичные ключи. Для пользования возможностями распределённых реестров данных необходимы ключи: приватный — для удостоверения совершения транзакции, т. е. её подписи, публичный — позволяет принимать криптовалюту. Установление ключей позволяет удостовериться в возможности контроля над криптокошельком, поэтому их отражение в протоколе следственного действия является обязательным (при их наличии).

В целях полноты и правильности фиксации необходимо обязательное привлечение специалистов, обладающих знаниями, умениями и навыками в сфере компьютерной информации, её защиты и управления электронными документами. Также целесообразно использовать такую новейшую криминалистическую технику для извлечения криминалистически значимой информации, как, например, Мобильный криминалист «Эксперт плюс», его аналитические инструменты, PC-3000 Portable PRO.

Игнорирование отображения в протоколе следственного действия указанных аспектов порождает юридический аспект противодействия расследованию преступлений, совершенных с использованием криптовалюты. Он выражается в возможности злоупотребления обжалованием действий и решений относительно

[1] В РФ открылся первый криптовалютный банк «Валютный экспресс» // Телеграм-канал «Во///дь» : **[РКН: иностранный владелец ресурса нарушает закон РФ]**. URL: https://t.me/indeec_1937/18695 (дата обращения: 23.10.2024).

[2] Уголовно-процессуальный кодекс Российской Федерации : от 18.12.2001 № 174-ФЗ ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 23.10.2024).

производства следственных действий, связанных, например, с обнаружением и извлечением криминалистически значимой информации о транзакциях. Как следствие, например, в рамках ст. 125 УПК РФ возможно досрочное ознакомление с материалами уголовного дела и разработка дальнейшей линии противодействия следствию.

Также считаем необходимым обратить особое внимание на виктимологическую характеристику жертв от указанной группы преступлений. Их специфические признаки выделены вследствие анализа материалов следственной и судебной практики по г. Санкт-Петербургу за период 2021–2023 гг. Так, кибервиктимологические аспекты криптопреступлений включают в себя ряд факторов, которые, по нашему мнению, не только способствуют дальнейшему росту совершения исследуемой группы преступлений, но и дополнительно укрепляют уверенность лица в целесообразности оказания мер противодействия их расследованию:

1. *Недостаточная цифровая грамотность*. Анализ материалов следственной и судебной практики позволяет отметить, что жертвы криптопреступлений часто обладают достаточно ограниченными (фрагментарными) знаниями о криптовалюте, сфере ее функционирования и оборота, механизме работы распределенных реестров данных. Высокая степень доверия к децентрализованным валютам без единого центра правового регулирования и воздействия увеличивает их кибервиктимизацию;

2. *Склонность к инвестициям с высокими рисками*. Жертвы криптопреступлений, особенно мошенничества, участвуют в сомнительных «инвестиционных» проектах с использованием криптовалют с целью быстрого увеличения своих доходов. Однако, отсутствие необходимых знаний о блокчейн-технологиях, видах криптовалют, только лишь повышают степень их виктимизации (в таких случаях жертвы отдают свои средства, покупая так называемые скамы — токены, не представляющие никакой ценности). На этот фактор указывается и в криминологической науке: «некоторые жертвы мошенничества могут быть привлечены обещаниями легкого заработка, выгодных сделок или удовлетворения иных потребностей. Обещания богатства, успеха или иного благополучия может заставить их довериться и сотрудничать с мошенником» [1 с. 325];

3. *Доверчивость, недостаточная проверка контрагентов*. Жертвы нередко вступают в сделки с незнакомыми лицами или организациями без проведения должной проверки их надежности. Отсутствие критического подхода к выбору партнеров по сделкам с криптовалютами повышает риск виктимизации;

4. *Использование ненадежных платформ и сервисов*. Обращение к малоизвестным или не проверенным биржам, обменникам, криптокошелькам значительно повышает уровень угрозы безопасности финансовых активов;

5. *Отсутствие мер по защите персональных данных*. Жертвы криптопреступлений часто не уделяют достаточного внимания защите своих персональных данных, что повышает возможность получения указанных сведений, как с помощью технологических решений, так и средств социальной инженерии.

Заключение

Проведенное исследование позволяет сделать следующие выводы. Специфика форм противодействия следствию обусловлены технологической спецификой функционирования и оборота криптовалют, осуществления транзакций, а также особенностями образования следовой картины.

В представленной научной работе предложено рассматривать противодействие расследованию преступлений, совершенных с использованием криптовалют по двум направлениями — техническому и юридическому.

Технические формы противодействия включают в себя использование специального программного обеспечения, которое значительно затрудняет обнаружение, фиксацию и изъятия криминалистически значимой информации. К ним необходимо отнести: использование виртуальных частных сетей (VPN), анонимных сетей (TOR), миксеров криптовалют, шифрования, использование анонимных криптовалют,

уничтожение электронно-цифровых следов (как с помощью специального ПО, так и физически).

Использование юридической формы противодействия обусловлено неоднозначностью правового положения криптовалюты, особые требования к сведениям, подлежащим фиксации в протоколах следственных действий, злоупотребление обжалованием действий и решений относительно производства отдельных следственных действий, направленных на поиск и фиксацию электронно-цифровых следов о преступлениях, совершенных с использованием криптовалют. Таким образом, для повышения эффективности расследования криптопреступлений требуется комплексный подход, включающий как технологические меры, так и совершенствование правовых механизмов, что позволит оперативно реагировать на вызовы цифровой преступности.

Кроме того, в статье выделены кибервиктимологические характеристики жертв криптопреступлений, такие как доверчивость, отсутствие мер по защите персональных данных и склонность к рисковым инвестициям. Эти характеристики усиливают виктимизацию и требуют внедрения превентивных мер для снижения риска преступлений, направленных на пользователей криптовалютных платформ.

Список источников

1. Белодед Д. Р. Некоторые психологические особенности жертв преступлений, совершаемых с использованием цифровых технологий // Виктимология. 2023. Т. 10, № 3. С. 320–334. DOI: https://doi.org/10.47475/2411-0590-2023-10-3-320-334

2. Бибиков А. А. Противодействие расследованию преступлений как объект изучения криминалистики // Известия Тульского государственного университета. Экономические и юридические науки. 2017. № 2-2. С. 49–58.

3. Веренич И. В. Исторический аспект и сущность учения о преодолении противодействия расследованию преступлений // Genesis: исторические исследования. 2019. № 12. С. 159–165. DOI: https://doi.org/10.25136/2409-868X.2019.12.31774

4. Волобуев А. Ф. Противодействие расследованию экономических преступлений и его преодоление // Государство и право. 2002. № 4. С. 42–47.

5. Головин А. Ю. Криминалистическая систематика : монография. Москва : ЛексЭст, 2002. 305 с.

6. Журавлев С. Ю. Противодействие деятельности по раскрытию и расследованию преступлений и тактика его преодоления : дис. … канд. юрид. наук : 12.00.09. Нижний Новгород, 1992. 201 с.

7. Карагодин В. Н. Основы криминалистического учения о преодолении противодействия предварительному расследованию : дис. … д-ра юрид. наук : 12.00.09. Екатеринбург, 1992. 388 с.

8. Карагодин В. Н. Преодоление противодействия предварительному расследованию. Свердловск : Изд-во Урал. ун-та, 1992. 175 с.

9. Климов И. А., Синилов Г. К. Противодействие криминальной среды как объект и предмет исследования ОРД // Организованное противодействие расследованию преступлений и меры по его нейтрализации : материалы науч.-практ. конференции, г. Руза — г. Москва. Москва, 1997. С. 22–25.

10. Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования : учеб. для высш. и сред. учеб. заведений МВД России / Т. В. Аверьянова Р. С. Белкин А. И. Бородулин [и др.] ; под ред. Т. В. Аверьяновой, Р. С. Белкина ; Акад. МВД России. Москва : Новый юрист, 1997. 398 с.

11. Кустов А. М. Механизм преступления и противодействие его расследованию : учеб. пособие. Ставрополь : Изд-во Ставроп. ун-та, 1997. 131 с.

12. Москвин Е. О. Противодействие предварительному расследованию: понятие и классификация // Воронежские криминалистические чтения. Вып. 3. Воронеж, 2002. С. 137–145.

13. Пастернак С. Н. Проблемы противодействия международной преступности, связанной с оборотом криптовалюты // Право и государство: теория и практика. 2023. № 6 (222). С. 367–369. DOI: https://doi.org/10.47643/1815-1337_2023_6_367

14. Стулин О. Б. Как препятствовать противодействию расследованию // Законность. 2000. № 2. С. 26–27.

15. Чернышева Ю. А. Права человека в условиях цифровизации общества // Психология и право. 2019. Т. 9, № 4. С. 90–102. DOI: https://doi.org/10.17759/psylaw.2019090407

16. Stalans L. J., Donner C. M. Explaining Why Cybercrime Occurs: Criminological and Psychological Theories. In: Jahankhani, H. (eds) Cyber Criminology. Advanced Sciences and Technologies for Security Applications. Springer, 2018. Cham. P. 25–45. DOI: https://doi.org/10.1007/978-3-319-97181-0_2

References

1. Beloded DR. Some psychological characteristics of victims of crimes committed using digital technologies // Victimology. 2023. Vol. 10, No. 3. Pp. 320-334. (In Russ.) DOI: https://doi.org/10.47475/2411-0590-2023-10-3-320-334

2. Bibikov AA. Counteraction to crime investigation as an object of study in forensic science. *Bulletin of Tula State University. Economic and legal sciences*. 2017;(2-2):49-58. (In Russ.)

3. Verenich IV. Historical aspect and essence of the doctrine of overcoming counteraction to crime investigation. *Genesis: historical research*. 2019;(12):159-165. (In Russ.) DOI: https://doi.org/10.25136/2409-868X.2019.12.31774

4. Volobuev AF. Counteraction to the investigation of economic crimes and its overcoming. *State and Law*. 2002;(4):42-47. (In Russ.)

5. Golovin AYu. *Forensic taxonomy*: [monograph]. Moscow: LexEst, 2002. 305 p. (In Russ.)

6. Zhuravlev SYu. *Counteraction to activities on disclosure and investigation of crimes and tactics of its overcoming* : [dissertation]. Nizhny Novgorod, 1992. 201 p. (In Russ.)

7. Karagodin VN. *Fundamentals of the forensic doctrine on overcoming resistance to preliminary investigation*: [dissertation]. Yekaterinburg, 1992. 388 p. (In Russ.)

8. Karagodin VN. *Overcoming resistance to preliminary*. Sverdlovsk: Publishing house of the Ural. University, 1992. 175 p. (In Russ.)

9. Klimov IA, Sinilov GK. Counteraction of the criminal environment as an object and subject of research of operational search activities. *Organized counteraction to the investigation of crimes and measures to neutralize it* : materials of the scientific and practical conference. Ruza-Moscow, 1997:22-25. (In Russ.)

10. *Forensic support of the activities of the criminal police and preliminary investigation bodies* : [Textbook for higher and secondary]. Ed. of the Ministry of Internal Affairs of Russia / Averianova TV, Belkin RS, Borodulin AI. et al.; Under the editorship of Averianova TV, Belkin RS. Moscow: Novy Yurist, 1997. 398 p. (In Russ.)

11. Kustov AM. *The mechanism of crime and counteraction to its investigation*: [Textbook]. Stavropol, 1997. 131 p. (In Russ.)

12. Moskvin EO. Counteraction to preliminary investigation: concept and classification. *Voronezh forensic readings*. Issue 3. Voronezh, 2002:137-145. (In Russ.)

13. Pasternak SN. Problems of counteracting international crime related to cryptocurrency circulation. *Law and state: theory and practice*. 2023;(6):367-369. (In Russ.) DOI: https://doi.org/10.47643/1815-1337_2023_6_367

14. Stulin OB. How to prevent counteraction to the investigation. *Legality*. 2000;(2):26-27. (In Russ.)

15. Chernysheva YuA. Human rights in the context of digitalization of society. *Psychology and law*. 2019;9(4):90-102. (In Russ.) DOI: https://doi.org/10.17759/psylaw.2019090407

16. Stalans LJ, Donner CM. Explaining Why Cybercrime Occurs: Criminological and Psychological Theories. In: Jahankhani, H. (eds) *Cyber Criminology. Advanced Sciences and Technologies for Security Applications*. Springer, 2018. Cham. P. 25–45. DOI: https://doi.org/10.1007/978-3-319-97181-0_2

ИНФОРМАЦИЯ ОБ АВТОРАХ

Векленко Василий Владимирович

Доктор юридических наук, профессор, профессор кафедры уголовного права, Санкт-Петербургский государственный университет.

199106, Санкт-Петербург, 22-я линия В.О., д. 7.
veklenkovv@yandex.ru
https://orcid.org/0000-0003-1373-6271

Чихрадзе Анна Михайловна

Кандидат юридических наук, доцент кафедры криминалистики, Санкт-Петербургский университет Министерства внутренних дел Российской Федерации.

198206, г. Санкт-Петербург, ул. Летчика Пилютова, д. 1.
anna.chikhradze@mail.ru
https://orcid.org/0009-0000-0763-2228

INFORMATION ABOUT THE AUTHORS

Vasily V. Veklenko

Doctor of Law Sciences, Professor, Professor of the Department of Criminal Law, St. Petersburg State University.

7 22nd line V.O., St. Petersburg 199106, Russia.
veklenkovv@yandex.ru
https://orcid.org/0000-0003-1373-6271

Anna M. Chikhradze

Candidate of Law Sciences, Associate Professor of the Department of Criminalistic, St. Petersburg, St. Petersburg University of the MIA of Russia.

1 Letchika Pilyutova str., St. Petersburg 198206, Russia
anna.chikhradze@mail.ru
https://orcid.org/0009-0000-0763-2228

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

ВКЛАД АВТОРОВ

Вклад авторов равноценный.

CONTRIBUTION OF THE AUTHORS

The contribution of the authors is equivalent.

Дата поступления статьи / Received: 07.11.2024.
Дата рецензирования статьи / Revised: 03.12.2024.
Дата принятия статьи к публикации / Accepted: 05.12.2024.