

Научная статья

<https://doi.org/10.24412/2220-2404-2024-12-5>

УДК 343.98



Attribution

cc by

## ОТДЕЛЬНЫЕ ЗАКОНОМЕРНОСТИ СОВЕРШЕНИЯ СОВРЕМЕННЫХ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ В КИБЕРПРОСТРАНСТВЕ

*Воротникова А.С.*

*Юго-Западный государственный университет*

**Аннотация.** Преступная деятельность в сфере информационных и коммуникационных технологий, в том числе с использованием криптовалютных активов (далее по тексту - криптовалюта), является одним из объектов современной цифровой криминалистики. Цель научной работы состоит в исследовании криптовалюты и экономических преступлений, совершаемых с ее использованием в киберпространстве. Анализ отдельных признаков и свойств криптовалюты, закономерностей совершения экономических преступлений с ее использованием, а также предложение некоторых мер по выявлению, раскрытию и расследованию таких преступлений составляют задачи настоящего исследования. В процессе работы использовались общенаучные методы исследования (наблюдение, описание, индукция, дедукция, анализ, синтез, гипотеза) и частнонаучные (сравнительно-правовой, формально-юридический). В результате исследования автором изучены и сформулированы свойства и особенности криптовалют, описаны способы отслеживания транзакций, а также предложены меры правового и комплексного характера с целью предупреждения экономических преступлений в киберпространстве.

**Ключевые слова:** киберпространство, криптовалюта, экономические преступления, информационные и коммуникационные технологии, цифровая криминалистика, киберкриминалистика, компьютерная форензика.

## SOME PATTERNS OF THE COMMISSION OF MODERN ECONOMIC CRIMES IN CYBERSPACE

*Anna S. Vorotnikova*

*South West State University*

**Abstract:** Criminal activity in the field of information and communication technologies, including the use of cryptocurrency assets (hereinafter referred to as cryptocurrency), is one of the objects of modern digital criminology. The purpose of the scientific work is to study cryptocurrency and economic crimes committed with its use in cyberspace. The analysis of individual signs and properties of cryptocurrency, patterns of economic crimes committed using it, as well as the proposal of some measures to identify, disclose and investigate such crimes constitute the objectives of this study. In the course of the work, general scientific research methods (observation, description, induction, deduction, analysis, synthesis, hypothesis) and private scientific (comparative legal, formal legal) were used. As a result of the research, the author studied and formulated the properties and features of cryptocurrencies, described ways to track transactions, and proposed legal and comprehensive measures to prevent economic crimes in cyberspace.

**Keywords:** cyberspace, cryptocurrency, economic crimes, information and communication technologies, digital criminology, cybercriminalism, computer forensics.

### Введение

Постоянно растущий уровень информатизации и цифровизации общества провоцирует развитие киберпространства, его отдельных элементов, а также вовлеченность их участников и профессионализм пользователей. Киберпространство – это специфическая среда – компьютерные

нейронные сети, пользователи которой применяют комплекс технических устройств, регулярно обращаются к ним, а участники – попадают под сферу их действия [1, с. 16].

Криптовалюта, такая как Bitcoin, Ethereum и другие, являясь частью киберпространства, становится всё более популярной и широко исполь-

зуемой в различных сферах. Криптовалюта представляет собой электронное имущество, использующее криптографические средства для обеспечения безопасности транзакций и контроля над созданием новых единиц, которое учитывается в реестре цифровых транзакций, в соответствии с закрепленными правилами его ведения [2, с. 83]. Условия относительной децентрализации и анонимности делают ее привлекательной для преступников. Однако некоторые свойства и особенности криптовалют делают отслеживание транзакций, в том числе совершение их в ходе преступной деятельности, доступным для выявления службами безопасности криптобирж и правоохранительными органами. Изучению отдельных закономерностей совершения экономических преступлений с использованием криптовалют посвящена настоящая статья.

### Обсуждение

В соответствии с решением Пленума Верховного Суда РФ, криптовалюта, наряду с иными имущественными ценностями, признана предметом преступлений, предусмотренных ст. ст. 174, 174.1 УК РФ [3]. Указанные составы относятся к главе 22 УК РФ – преступлениям в сфере экономической деятельности. В свою очередь, преступные посягательства с использованием криптовалют, тоже относятся к указанной группе, чья цель состоит в вовлечении незаконно полученного имущества в легальный экономический оборот.

Криптовалюта, не являясь традиционным средством обращения, тем не менее является предметом экономических преступлений, поскольку может использоваться при расчете, а затем конвертироваться в наличные, безналичные и цифровые деньги. Указанными свойствами криптовалют пользуются злоумышленники. Например, в г. Саранск выявлено преступное сообщество, организованное в целях бесконтактного расчета с использованием криптовалюты Bitcoin за приобретение и сбыт наркотических средств посредством сети «Интернет». Покупатели наркотических средств переводили деньги на криптокошельки, а участники преступного сообщества через программы Интернет-банкинга обналачивали указанные средства путем дробления денежных средств в пределах 15 тысяч рублей для осуществления операции без открытия счета [4]. В конечном итоге денежные средства зачислялись на счета, открытые в банках ПАО «Сбербанк» на имена подставных лиц – так называемых «дропов». Ими, как правило, становятся незащищен-

ные слои населения, которые за денежное вознаграждение передают свои персональные данные преступникам.

Отмывание денежных средств является одним из основных видов преступлений в сфере криптовалют. Преступники используют криптовалюты для перемещения и скрытия незаконно полученных денег, создавая тем самым сложности для правоохранительных органов в выявлении и пресечении таких преступных действий. Они включают в себя такие методы, как миксинг-сервисы, которые смешивают средства разных пользователей, чтобы усложнить отслеживание источника денег [6, с. 33]. Использование децентрализованных сервисов в целях отмывания денег имеет ограниченный успех, поскольку даже в условиях отсутствия идентификации личности, в цифровом поле фиксируется каждая сделка.

Помимо этого, совершаются атаки на криптобиржи, где хакеры пытаются осуществить хищение средств других пользователей, личных ключей от чужих кошельков или манипуляции с курсами криптовалют. Кроме того, в сфере криптовалют также происходит финансирование незаконной деятельности.

Согласно сообщению пресс-службы образовательной платформы в области цифрового и бизнес-права Moscow Digital School, в России в 2023 году количество судебных споров, связанных с криптовалютой, выросло на 72%, в сравнении с аналогичным показателем 2022 года, и составило 2653 гражданских, уголовных и административных дел. Специалисты связывают такую динамику с развитием криптоиндустрии в стране, а также ростом интереса общества к быстрому обмену криптовалютой с минимальными комиссиями и отсутствием разницы курсов традиционных валют [5].

В связи с этим назрела необходимость различать и отделять от преступных посягательств легальное использование криптовалюты. Пленум Верховного Суда РФ реализовал рекомендацию Международной группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), которая предписала всем государствам-участникам принять меры по недопущению использования криптовалюты в преступных целях. Однако, по мнению некоторых исследователей, созданный на этом фоне закон от 31 июля 2020 г. № 259-ФЗ в большей степени ограничивает оборот криптовалюты, а не решает главную задачу – пресечение и предупреждение преступлений с использованием криптовалюты [7; 8].

Тем временем в странах Евросоюза применяется Директива о борьбе с отмыванием денег, в соответствии с которой все участники крипторынка считаются посредниками, передающими деньги. Такой статус возлагает на криптобиржи обязанности идентифицировать своих клиентов и конечных бенефициаров по транзакции, применять меры внутреннего контроля и сотрудничать с правоохранительными органами, сообщая им о подозрительных операциях. В США на федеральном уровне правовое регулирование оборота криптовалют отсутствует, однако в некоторых штатах криптовалюты тождественны денежным средствам в наличной и безналичной форме [9, с. 142-146].

### Результаты

Анонимность в киберпространстве является условной, поскольку все действия оставляют цифровые следы. В большинстве криптовалютных сетей пользователи скрыты за адресами, которые не связаны напрямую с их реальной личностью. Псевдоанонимность Bitcoin, где транзакции публичны, но пользователи остаются анонимными, усложняет процесс расследования преступлений. Это создает значительные трудности для правоохранительных органов при попытке идентификации преступников, однако не делает эту задачу невыполнимой.

Основным инструментом для расследования преступлений с использованием криптовалют является блокчейн-аналитика. Блокчейн представляет собой публичный регистр всех транзакций в сети криптовалюты [10, с. 53]. Несмотря на анонимность участников, сами транзакции являются публичными и неизменяемыми, что позволяет отслеживать движение денежных средств.

Одним из способов блокчейн-аналитики является кластеризация адресов. Она позволяет объединять адреса, которые с высокой долей вероятности принадлежат одному и тому же пользователю или организации. Эта задача достигается путем анализа паттернов транзакций и использования эвристик, таких как повторное использование адресов и сопутствующие транзакции.

Ранее в статье мы приводили пример использования децентрализованных сервисов для совершения экономических преступлений. Однако наряду с ними с указанной целью применяются и централизованные площадки, где аккаунты регистрируются на подставных лиц. Как правило мониторинговые сервисы служб безопасности любой биржи сразу выявляют подозрительную активность и блокируют таких пользователей.

Важно отметить, что пользователи, законно использующие криптовалюты могут столкнуться с блокировкой карты и счета. Почему так происходит? Чаще всего пользователи сталкиваются с такими ограничениями, получая уведомление со ссылкой на закон от 07.08.2001 N 115-ФЗ. В соответствии с ним банки обязаны отслеживать операции клиентов и выяснять источники их средств. Главная задача банка в рамках указанного закона – убедиться, что деньги поступают из легального источника, и клиент может подтвердить их происхождение. Сам закон напрямую не регулирует операции с криптовалютами, но при обороте крупных сумм на счете банк неизбежно заинтересуется, откуда эти деньги взялись. Однако, если злоумышленник представит фиктивное подтверждение основания и источника денежного перевода: например, подложный договор и акт выполненных работ (услуг), то избежит блокировки своего банковского счета, если факт подлога документов не будет выявлен. Если речь идет о регулярных переводах крупных сумм, так называемой «перегонке средств по кругу», то банк тоже наверняка заблокирует карту для выяснения обстоятельств.

### Заключение

В связи с рассмотренными особенностями криптовалюты представляется важным разработать и внедрить эффективные способы, средства и методы, позволяющие разграничивать отмывание преступных доходов с использованием криптовалюты от законного ее использования. Принципиальным здесь является поддержка государственных органов, регулирующих финансовые операции, внедрение прозрачной системы мониторинга и контроля за использованием криптовалют в целях пресечения и предотвращения преступных действий.

Одна из возможных стратегий в этой области – сотрудничество между государственными органами и экспертами в области криптовалюты. Взаимодействие и обмен информацией между этими сторонами поможет не только быстро выявлять и расследовать преступления, но и активно пресекать их. Создание специальных отделов или подразделений, занимающихся анализом и мониторингом операций с криптовалютами в структуре правоохранительных органов, позволит усилить борьбу с отмыванием преступных доходов.

Для эффективной борьбы с преступлениями, связанными с криптовалютой, в России необходимо законодательное закрепление обязательного сопровождения полной информацией о клиенте всех электронных и цифровых переводов. В

этом контексте властные структуры должны учесть важность идентификации личности при совершении транзакции для ведения реестра. В

настоящее время уже началась разработка законов в данной сфере, что указывает на необходимость принятия соответствующих мер.

**Конфликт интересов**

Не указан.

**Conflict of Interest**

None declared.

**Рецензия**

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

**Review**

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

**Литература:**

1. Ищенко Е.П. У истоков цифровой криминалистики // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 3 (55). С. 15-28.
2. Фарахиев Д.М. Деятельность органов внутренних дел в процессе раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий (на примере криптовалютных активов) // Юридический вестник Самарского университета. 2023. Т. 9. № 3. С. 81-90.
3. Постановление Пленума Верховного Суда РФ от 26.02.2019 № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // СПС «Консультант Плюс». URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_319191/](https://www.consultant.ru/document/cons_doc_LAW_319191/) (дата обращения: 07.10.2024).
4. Уголовное дело № 1-125/2017. Архив Ленинского районного суда г. Саранск Республики Мордовия // Интернет-ресурс «Судебные и нормативные акты РФ». URL: <https://sudact.ru/regular/doc/Y6XofyVXCQHJ/> (дата обращения: 08.10.2024).
5. Количество связанных с криптовалютой судебных дел в России увеличилось на 72% // Российское агентство правовой и судебной информации. URL: [https://rapsinews.ru/incident\\_news/20240326/309755535.html](https://rapsinews.ru/incident_news/20240326/309755535.html) (дата обращения: 08.10.2024).
6. Рябина Т.К., Ряполова Я.П., Чистилина Д.О. Актуальные проблемы выявления и расследования дистанционных хищений с банковского счета // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2023. № 4. С. 31-38.
7. Дорж Энхтур, Хайрутдинова Ирина Викторовна Проблемы легализации (отмывания) денежных средств через криптовалюту // Юридическая наука. 2021. №2. URL: <https://cyberleninka.ru/article/n/problemy-legalizatsii-otmyvaniya-denezhnyh-sredstv-cherez-kriptovalyutu> (дата обращения: 20.09.2024).
8. Федеральный закон "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" от 31.07.2020 N 259-ФЗ // СПС «Консультант Плюс». URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_358753/](https://www.consultant.ru/document/cons_doc_LAW_358753/) (дата обращения: 07.10.2024).
9. Ларин Д.С. Возможность использования биткоинов в отмывании денег // Известия Санкт-Петербургского государственного экономического университета. 2018. № 1. С. 142-146.
10. Рябина Т.К., Чистилина Д.О. Вспомогательные средства и способы борьбы с хищением денежных средств с банковского счета в России и за рубежом // В сборнике: Актуальные вопросы устойчивого развития государства, общества и экономики. сборник научных статей 2-й Всероссийской научно-практической конференции. Курск, 2023. С. 50-54.
11. Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ // СПС «Консультант Плюс». URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_32834/](https://www.consultant.ru/document/cons_doc_LAW_32834/) (дата обращения: 07.10.2024).

**References**

1. Ishchenko E.P. At the origins of digital forensics // Bulletin of the O.E. Kutafin University (MGUA). 2019. № 3 (55). Pp. 15-28.

2. Farakhiev D.M. *Activity of internal affairs bodies in the process of disclosure and investigation of crimes committed using information and communication technologies (on the example of cryptocurrency assets)* // *Legal Bulletin of Samara University*. 2023. Vol. 9. No. 3. pp. 81-90.
3. *Resolution of the Plenum of the Supreme Court of the Russian Federation dated 02/26/2019 No. 1 "On Amendments to the Resolution of the Plenum of the Supreme Court of the Russian Federation dated July 7, 2015 No. 32 "On Judicial practice in cases of legalization (laundering) of funds or other property acquired by criminal means, and on the acquisition or sale of property knowingly obtained by criminal means"* // *SPS Consultant Plus*. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_319191/](https://www.consultant.ru/document/cons_doc_LAW_319191/) (date of application: 07.10.2024).
4. *Criminal case No. 1-125/2017. Archive of the Leninsky District Court of Saransk, Republic of Mordovia* // *Internet resource "Judicial and regulatory acts of the Russian Federation"*. URL: <https://sudact.ru/regular/doc/Y6XofyVXCQHJ/> (date of appeal: 08.10.2024).
5. *The number of cryptocurrency-related court cases in Russia has increased by 72%* // *Russian Agency for Legal and Judicial Information*. URL: [https://rapsinews.ru/incident\\_news/20240326/309755535.html](https://rapsinews.ru/incident_news/20240326/309755535.html) (date of application: 08.10.2024).
6. Ryabinina T.K., Ryapolova Ya.P., Chistilina D.O. *Actual problems of detecting and investigating remote theft from a bank account* // *Bulletin of the Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin*. 2023. No. 4. pp. 31-38.
7. Dorj Enchtur, Khairutdinova Irina Viktorovna *Problems of money legalization (laundering) through cryptocurrency* // *Yuridicheskaya nauka*. 2021. No.2. URL: <https://cyberleninka.ru/article/n/problemny-legalizatsii-otmyvaniya-denezhnyh-sredstv-cherez-kriptovalyutu> (date of appeal: 09/20/2024).
8. *Federal Law "On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation" dated 07/31/2020 No. 259-FZ* // *SPS Consultant Plus*. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_358753/](https://www.consultant.ru/document/cons_doc_LAW_358753/) (date of reference: 07.10.2024).
9. Larin D.S. *The possibility of using bitcoins in money laundering* // *Izvestiya of St. Petersburg State University of Economics*. 2018. No. 1. pp. 142-146.
10. Ryabinina T.K., Chistilina D.O. *Auxiliary means and methods of combating the theft of funds from a bank account in Russia and abroad* // *In the collection: Topical issues of sustainable development of the state, society and economy. collection of scientific articles of the 2nd All-Russian Scientific and Practical Conference. Kursk, 2023*. pp. 50-54.
11. *Federal Law "On Countering the legalization (laundering) of proceeds from crime and the financing of terrorism" dated 08/07/2001 No. 115-FZ* // *SPS Consultant Plus*. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_32834/](https://www.consultant.ru/document/cons_doc_LAW_32834/) (date of access: 07.10.2024).

#### **Информация об авторе:**

**Воротникова Анна Сергеевна**, преподаватель кафедры уголовного процесса и криминалистики; юридический факультет, Юго-Западный государственный университет; ORCID 0000-0002-6438-5478. E-mail: seamni46@mail.ru

**Anna S. Vorotnikova**, teacher of the Department of Criminal Procedure and Criminalistics; Faculty of Law, Southwestern State University; Kursk, Russia.