 DOI 10.17150/2411-6122.2025.3.30-39 ISSN 2411-6122

Научная статья
УДК 343.9
EDN OKETHH
DOI 10.17150/2411-6122.2025.3.30-39

Характеристика способов совершения хищений криптовалютных активов

Н.И. Гайсин

Уфимский университет науки и технологий, г. Уфа, Российская Федерация,
nursultan9703@mail.ru

Аннотация. С быстрым развитием, распространением и растущей популярностью криптовалют увеличивается число преступлений, направленных на их хищение, поскольку они обладают реальной ценностью. Без знания технических особенностей при работе с криптовалютой, невозможно прийти к полному понимаю того, какими способами может быть совершено ее хищение. Настоящая статья посвящена характеристике наиболее часто встречающихся в настоящее время способов хищения криптовалютных активов в форме кражи и мошенничества. Перед тем, как перейти к самой характеристике способов, автор указывает на легализацию имущественного статуса криптовалюты в результате ее развития, распространения и признания обществом, а также описывает общие механизмы хищений криптовалюты в формах кражи, мошенничества, грабежа, разбоя и вымогательства. Автор приходит к выводу о том, что для эффективного расследования таких хищений необходимо знание технических особенностей при работе с криптовалютой. Для получения таких знаний необходимо обучение соответствующих специалистов и, в целом, пополнение системы знаний о способах совершения хищений криптовалюты.

Ключевые слова: криптовалюта, блокчейн, смарт-контракт, способы хищения, расследование.

Для цитирования: Гайсин Н.И. Характеристика способов совершения хищений криптовалютных активов / Н.И. Гайсин. — DOI 10.17150/2411-6122.2025.3.30-39. — EDN OKETHH // Сибирские уголовно-процессуальные и криминалистические чтения. — 2025. — № 3. — С. 30–39.

Original article

Characteristics of Methods of Stealing Cryptocurrency Assets

N.I. Gaisin

Ufa University of Science and Technology, Ufa, the Russian Federation,
nursultan9703@mail.ru

Abstract. The rapid development, spread and growing popularity of cryptocurrencies lead to an increase in the number of crimes aimed at stealing them because they have real value. Without knowing the technical specifics of dealing with cryptocurrencies it is impossible to gain a full understanding of how they can be stolen. The article characterizes the methods of stealing cryptocurrency assets that are currently most common, namely, theft and fraud. Before describing the methods themselves, the author points out the legalization of the property status of cryptocurrency as a result of its development, spread and recognition by the society, and describes the common mechanisms of stealing cryptocurrency, such as theft, fraud, robbery and blackmail. The author comes to the conclusion that the

effective investigation of such thefts requires the knowledge of technical specifics of working with cryptocurrencies. To obtain such knowledge, it is necessary to train the corresponding specialists and, in general, to replenish the systematic knowledge regarding the methods of stealing cryptocurrencies.

Keywords: cryptocurrency, blockchain, smart contract, methods of theft, investigation.

For citation: Gaisin N.I. Characteristics of Methods of Stealing Cryptocurrency Assets. *Sibirskie Ugolovno-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings,* 2025, no 3, pp. 30–39. (In Russian). EDN: OKETHH. DOI: 10.17150/2411-6122.2025.3.30-39.

Преступления, совершаемые с использованием информационно коммуникационных технологий, на сегодняшний день являются наиболее динамично развивающимися [1, с. 111].

Однако киберпреступления стремительно развиваются не только количественно. В современный период в значительной степени изменяются их структурные характеристики, связанные с развитием новых способов совершения традиционных преступлений. Эта тенденция детерминирована развитием блокчейн-технологий, появлением криптовалюты и токенов [2].

Одним из продуктов развития криптовалютной индустрии является новая группа корыстных преступлений, направленных на хищение цифровых валют [3, с. 181]. В научной литературе такие преступления, совершенные с использованием виртуальной валюты, технологий, позволяющих ее использовать для совершения преступлений (в основном связанных с незаконным оборотом товаров и услуг), а также ее хищением, получили название криптопреступлений, а их совокупность стала называться криптопреступностью [4].

Происходящие структурные изменения форм сохранения сбережений и способов управления финансовыми активами закономерным образом изменили вектор корыстных преступных посягательств. Их предметом в большинстве случаев становятся уже не вещи (включая наличные деньги), а безналичные денежные средства. А по мере развития, усложнения и диверсификации цифрового финансового и квазифинансового оборота предметом хищения все чаще становятся новые виды «бестелесных» активов, как, например, криптовалюта [5].

Долгое время вопрос о правовой природе криптовалюты являлся спорным, поскольку в Российской Федерации, как и во многих других государствах, не был закреплен ее правовой статус. По этой причине защита прав многих граждан не была обеспечена. Правоохранительные органы неоднократно отказывали в возбуждении уголовных дел по фактам совершенных хищений криптовалют, поскольку с правовой точки зрения отсутствовал необходимый элемент состава преступления — объект. Также имели место случаи, когда суды отказывались признавать виновными тех, кто совершил хищение криптовалюты. Однако следует отметить, что такие судебные акты отменялись или подвергались изменениям вышестоящими судами[1].

В настоящее время российский законодатель легализовал имущественный

[1] Апелляционное определение Санкт-Петербургского городского суда от 23 нояб. 2020 № 22-5295/2020, 1-95/2020 // СПС «КонсультантПлюс».

 DOI 10.17150/2411-6122.2025.3.30-39 ISSN 2411-6122

статус криптовалюты[2], что обязывает органы предварительного расследования надлежащим образом проводить предварительное расследование.

Современная наука криминалистики имеет недостаточно знаний о криминалистически значимых признаках таких хищений и их закономерных связях между собой. Наличие таких знаний способно не только помочь при расследовании преступлений, но и усовершенствовать тактику проведения отдельных следственных действий, а также методику расследования этих преступлений.

Методическое обеспечение расследования сталкивается с проблемой устаревания разработанных методик, не способных адекватно реагировать на вызовы цифровой эпохи. Необходимо разрабатывать и внедрять обновленные методические рекомендации, учитывающие современные тенденции в развитии преступности [6, с. 122].

Существует множество различных способов хищения криптовалютных активов. Некоторые из этих способов почти не отличаются от старых и современных способов хищения денежных средств, а некоторые являются новыми, поскольку были целенаправленно разработаны для хищения криптовалюты, с учетом особенностей, которые свойственны работе с криптовалютными активами.

Для совершения кражи злоумышленникам необходимо получить конфиденциальную информацию, воспользовавшись которой, возможно получить доступ к криптовалютным активам, либо согласие собственника на распоряжение криптовалютными активами в виде электронной подписи при взаимодействии со смарт-контрактами, либо доступ к устройству и приложению, откуда имеется возможность распоряжаться криптовалютой.

Вышеуказанная информация может быть похищена злоумышленником в оффлайн среде (некоторые собственники криптовалютных активов хранят мнемоническую фразу на бумажном носителе, так как такой способ хранения информации обеспечивает изоляцию от онлайн среды, а значит защищает от вредоносного программного обеспечения), либо передана собственником криптовалютных активов злоумышленнику под воздействием обмана или злоупотребления доверием, либо похищена или изменена при помощи вредоносного программного обеспечения.

Вредоносное программное обеспечение способно похитить или модифицировать конфиденциальную информацию, если будет загружено на устройство собственника криптовалютных активов, в котором такая информация хранится. Данное программное обеспечение может быть загружено на устройство собственником криптовалютных активов как под воздействием обмана или злоупотребления доверием, так и без такового воздействия. Также такая загрузка возможна самим злоумышленником при получении доступа к устройству.

Согласие на распоряжение криптовалютными активами в виде электронной подписи может дать собственник под воздействием обмана или злоупотребления доверием. Гипотетически, это действие может совершить и злоумышленник, но для этого ему необходим доступ к устройству собственника, а также возможность управления децентрализованным приложением, кото-

[2] О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации : Федер. закон от 29 нояб. 2024 № 418-ФЗ // СПС «КонсультантПлюс».

рому необходимо дать согласие, чтобы реализовать преступный умысел.

При совершении мошенничества собственник сам осуществляет перевод криптовалютных активов в адрес злоумышленников под влиянием обмана или злоупотребления доверием. В криптовалютной индустрии злоумышленники, чаще всего, вводят в заблуждение относительно возможности получения прибыли при совершении тех или иных действий, которые, на самом деле, направлены на перевод криптовалютных активов в адрес злоумышленников, реже — относительно намерений оказать какую-либо помощь. Пользователи очень часто обращаются за помощью в чаты различных мессенджеров или социальных сетей, где происходит обсуждение различных тем, связанных с криптовалютой, поскольку сталкиваются с разными трудностями. Например, не знают, как перевести свои криптовалютные активы из одного блокчейна на другой. Злоумышленники пользуются этим и откликаются под видом администратора или модератора чата.

Грабеж и разбой совершаются в оффлайн среде. Если кража и мошенничество, в большинстве случаев, направлены на неопределенный круг лиц, то вышеуказанные преступления совершаются в отношении конкретных лиц. Злоумышленникам, как минимум, известно, что у конкретного лица имеются криптовалютные активы. Грабеж может быть реализован путем открытого хищения устройства, где находится программное обеспечение, через которое возможен доступ к криптовалютным активам, а также конфиденциальной информации, которая необходима для получения доступа. Разбой может быть реализован путем нападения с последующим требованием произвести перевод криптовалютных активов в адрес злоумышленника, передать мнемоническую фразу или совершить любые другие действия, направленные на то, чтобы злоумышленник мог распоряжаться похищенным.

Вымогательство совершается путем распространения вирусных программ-блокираторов, либо путем направления текстовых сообщений по электронной почте, в социальных сетях или мессенджерах с требованием выкупа под угрозой распространения клеветнических сведений о потерпевшем и (или) сведений о личной жизни, которые последний желает сохранить в тайне либо под угрозой уничтожения имущества потерпевшего или юридического лица [7, с. 165].

В данной работе будут перечислены некоторые способы кражи и мошенничества, поскольку они наиболее распространены и разнообразны.

Одним из самых распространенных способов кражи криптовалютных активов является «фишинг», суть которого заключается в том, что злоумышленник создает сайт, приложение, расширение для браузера иное или программное обеспечение, которые аккумулируют логины, пароли, приватные ключи и мнемонические фразы от кошельков тех лиц, которые по своей невнимательности или незнанию основ безопасности при работе с криптовалютой передали вышеуказанную информацию. Сайты, приложения, расширения для браузера и иное программное обеспечение очень похожи на официальные сайты, приложения, расширения для браузера и программное обеспечение, где возможно производить те или иные действия с криптовалютными активами.

Например, злоумышленник может создать сайт, который похож по дизайну и URL-адресу с официальным сайтом централизованной криптовалютной биржи, где возможно покупать и продавать

криптовалюту. Адрес фишингового сайта, как правило, отличается от оригинального сайта одним символом. Например, вместо «blockchain.com» — «blockcnain.com». Такой способ хищения рассчитан на невнимательность пользователей или их неопытность в использовании сети Интернет. После того, как пользователь вводит свой логин и пароль от аккаунта на поддельном сайте, злоумышленник имеет возможность получить доступ к аккаунту пользователя и всем имеющемся на нем криптовалютным активам, которыми он сможет распорядиться по собственному усмотрению.

Аналогичным примером является фишинг браузерных расширений или приложений. Злоумышленник создает расширения или приложения с таким же интерфейсом как, например, у криптовалютного кошелька. Основная цель — получить от пользователя его мнемоническую фразу, состоящих из 12 или 24 английских слов, которые должны быть расположены в определенном порядке. С помощью этой фразы возможно восстановить доступ к криптовалютному кошельку и распорядиться активами по собственному усмотрению.

В качестве еще одного примера можно привести фишинг различных децентрализованных приложений. Злоумышленники активно пользуются возможностью анонимно создавать и размещать на блокчейне децентрализованные приложения и программировать смарт-контракты по своему усмотрению. Введенные в заблуждение пользователи подключают свои криптовалютные кошельки к фишинговому децентрализованному приложению и подтверждают какое-либо действие (то есть запускают в работу смарт-контракт), которое направлено либо на разрешение распоряжаться криптовалютными активами, либо перевод криптовалютных активов на кошелек злоумышленника.

К видам фишинговых атак в зависимости от адресата можно отнести спам-рассылки (масштабный фишинг), целенаправленный фишинг, «Whaling» и «SMiShing». Спам-рассылка представляет собой электронные письма или сообщения в социальных сетях различного смыслового содержания, рассчитанные на обман неограниченного круга случайно определенных пользователей. Такие сообщения чаще всего носят рекламный характер (о розыгрыше призов, акциях магазинов, получении денежного приза и др.) и подкрепляются фотографиями публичных людей или их брендов.

Противоположен масштабному целенаправленный фишинг, рассчитанный на обман определенного человека или группы людей, объединенных общими интересами. При данном виде фишинг-атак текст письма содержит обращение к пользователю по его имени и фамилии, имеет четко сформулированную просьбу или требование, не вызывающие сомнений [8, с. 45].

Следующий способ хищения криптовалютных активов, который хотелось бы упомянуть, заключается в использовании вредоносных программных обеспечений. Для реализации данного способа необходимо, чтобы вредоносное программное обеспечение оказалось на устройстве, где хранятся персональные данные, позволяющие получить доступ к криптовалютным активам, либо при помощи которого осуществляются криптовалютные трансакции. Такое программное обеспечение может быть загружено пользователем как под влиянием обмана или злоупотребления доверием, либо без такового.

Как пример, пользователь под влиянием обмана загружает на свое устрой-

ство вредоносное программное обеспечение, функция которого заключается в получении данных криптовалютных кошельков или в подмене публичного ключа в буфере обмена. В момент, когда пользователь собирается произвести перевод криптовалюты на чей-либо публичный адрес, он должен скопировать публичный адрес, на который планируется перевод, в буфер обмена своего устройства. В момент вставки вредоносное программное обеспечение производит подмену скопированного публичного адреса на публичный адрес злоумышленника. В результате пользователь переводит криптовалюту на публичный адрес злоумышленника. Заметить подмену адресов затруднительно, поскольку адрес представляет собой достаточно длинный набор латинских букв и цифр.

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

Существует также множество способов хищения криптовалютных активов путем обмана или злоупотребления доверием. Чаще всего, пользователи сами осуществляют перевод своих активов на чужие публичные адреса. Злоумышленники используют множество разных способов, чтобы втереться в доверие и (или) ввести пользователей в заблуждение.

Для примера приведем один из таких способов. Некоторые пользователи желают обменять свою криптовалюту на национальную валюту. Сделать это возможно путем P2P обмена на централизованной бирже, суть которой состоит в том, что один из пользователей создает на бирже заявку о продаже или покупке криптовалюты по определенному курсу, а другой пользователь откликается на такую заявку. Пользователь, который желает продать криптовалюту, переводит ее на публичный адрес, указанный в заявке, а пользователь, который желает купить криптовалюту, переводит национальную валюту на номер карты, указанный в заявке. Посредником выступает централизованная биржа. В момент принятия заявки криптовалюта продавца замораживается на эскроу-счете биржи, где ни одна из сторон сделки не имеет к ней доступа. Далее покупатель криптовалюты переводит денежные средства по указанным реквизитам и сигнализирует об осуществлении оплаты. Продавец проверяет, поступили ли денежные средства на счет, после чего подтверждает факт поступления денежных средств. Далее биржа размораживает криптовалюту и переводит ее покупателю.

В процессе вышеуказанного обмена злоумышленник, желающий похитить криптовалюту, совершает действия, направленные на то, чтобы продавец подтвердил факт получения денежных средств. Для этого он может направить SMS-сообщение на номер телефона продавца, которое будет идентично сообщению, которое обычно получают пользователи при зачислении денежных средств на банковский счет. Про-

 DOI 10.17150/2411-6122.2025.3.30-39 ISSN 2411-6122

давец, который должным образом не убедился в получении денежных средств, подтверждает факт их получения. В результате злоумышленник совершает хищение криптовалюты. Также злоумышленник может осуществить перевод меньшей суммы, чем указано в заявке. В обоих примерах злоумышленники рассчитывают на невнимательность пользователей.

Существуют также способы мошенничества, рассчитанные на опытных пользователей. Так, например, злоумышленник намеренно предоставляет неограниченному кругу лиц, группе лиц или конкретному лицу данные для доступа к своему децентрализованному кошельку, на балансе которого имеется криптовалюта. Злоумышленник может сделать вид, что это произошло случайно, либо, якобы, попросить о помощи в совершении какого-либо действия (например, совершить трансакцию) за вознаграждение. Однако для совершения трансакции необходимо оплатить комиссию блокчейна, в котором находится эта криптовалюта. Как правило, оплата производится в основной монете блокчейна. Так, например, если необходимо совершить трансакцию в сети «Ethereum», оплата должна быть произведена в ETH, если в сети «Binance Smart Chain», то в BNB и т.д. Поэтому для совершения трансакции, для начала, необходимо пополнить баланс в основной монете блокчейна. Кошелек заранее подключен к смарт-контракту, функция которого заключается в автоматическом переводе криптовалюты, в которой предполагается оплата комиссии, на другой адрес кошелька и заранее дано согласие смарт-контракту на распоряжение монетой. В результате, пополняемый баланс всегда обнуляется, поскольку в автоматическом режиме происходит трансакция, инициируемая смарт-контрактом.

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

Вышеуказанный способ легко вызывает доверие у многих пользователей, потому что, действительно, в 2013, 2017 и 2021 гг. наблюдался экспоненциальный рост стоимости большого количества криптовалют. Более того, некоторые пользователи многократно приумножили свои вложения.

По этой причине многие желают повторить успех и под воздействием обмана или злоупотребления доверием совершают покупку рекламируемых токенов за криптовалюту, которая имеет реальную ценность.

Часто токен размещается на децентрализованной бирже. Далее злоумышленник выкладывает на своем канале подробную пошаговую инструкцию о том, как купить данный токен. Некоторые такие токены, действительно, показывают многократный рост для убедительности. Однако после покупки токена его невозможно продать. Злоумышленник ограничивает продажу токена через функции смарт-контракта. Он программирует смарт-контракт таким образом, что для продажи токена необходимо оплатить комиссию в размере 100 % стоимости суммы продажи. Совершение такой сделки экономически нецелесообразно.

Невозможно перечислить все имеющиеся на сегодняшний день способы хищения криптовалютных активов, но выше мы постарались перечислить одни из наиболее актуальных и распространенных. В зависимости от обстоятельств некоторые способы могут быть комбинированы. Вдобавок могут быть использованы методы социальной инженерии. Это особенно актуально, когда злоумышленники собираются совершить хищение в отношении конкретного лица.

В завершение хотелось бы отметить, что развитие рынков цифровых активов и их использование требуют эффективной реакции правоохранительных органов и их партнеров, включая обучение новых поколений специалистов в этой сфере [9, с. 67]. Ряд способов совершения хищения криптовалютных активов имеют свою специфику и для успешного предварительного расследования необходимо знать технические особенности при работе с криптовалютой. Современная наука криминалистики нуждается в пополнении системы знаний о способах совершения хищений криптовалютных активов и их технических особенностях. Обладая этими знаниями, следователи (дознаватели) смогут выстраивать типичные следственные версии совершения преступлений, оценивать благоприятность следственной ситуации, эффективнее планировать и совершать следственные действия, а также взаимодействовать с оперативно-розыскными органами.

Изучение криминалистической характеристики способов подготовки, совершения и сокрытия хищений в сфере оборота криптовалют имеет практическую значимость для органов предварительного следствия и дознания, поскольку именно способ обусловливает выбор орудий и средств совершения хищений, характеризует типичную следовую картину для каждой конкретной ситуации, позволяет установить наличие у лиц, совершивших преступление, определенных профессиональных навыков, знаний и умений, а также причины и условия, повлиявшие на совершение преступлений [10, с. 82].

Список использованной литературы

1. Репецкая А.Л. Криптовалюта как объект уголовно-правового и криминологического исследования / А.Л. Репецкая, А.О. Миронов. — DOI 10.55001/2312-3184.2022.78.15.010. — EDN XLTNYQ // Вестник Восточно-Сибирского института МВД России. — 2022. — № 3 (102). — С. 109–120.

2. Долгиева М.М. Социальная обусловленность возникновения уголовно- правовых запретов нарушений, совершаемых в сфере оборота криптовалюты / М.М. Долгиева. — DOI 10.17803/1994-1471.2018.95.10.225-235. — EDN YOICCD // Актуальные проблемы российского права. — 2018. — № 10(95). — С. 225–235.

3. Шнейдерова Д.И. Анонимность как способ сокрытия хищений в сфере оборота криптовалют / Д.И. Шнейдерова. — EDN LXFFTE // Актуальные проблемы уголовного процесса криминалистики : сб. статей. — Могилев, 2020. — С. 181–186.

4. Долгиева М.М. Криптопреступность как новый вид преступности: понятие, специфика / М.М. Долгиева. — EDN CBKUCR // Современное право. — 2018. — № 10. — С. 109–115.

5. Капинус О.С. Цифровизация преступности и уголовное право / О.С. Капинус. — DOI 10.17150/2411-6262.2022.13(1).22. — EDN NZNOMN // Baikal Research Journal. — 2022. — Т. 13, № 1. — С. 22–22.

6. Макаренко И.А. Содержание криминалистического обеспечения расследования преступлений / И.А. Макаренко // Криминалистика, уголовный процесс и судебная экспертология в XXI веке: векторы развития : материалы Междунар. науч.-практ. конф., Москва, 25 апр. 2025 г. — Москва, 2025. — С. 119–127.

7. Шнейдерова Д.И. Хищения в сфере оборота криптовалюты в структуре киберпреступлений: виды, проблемы расследования (белорусский опыт) / Д.И. Шнейдерова. — DOI 10.37973/VESTNIKKUI-2024-58-20. — EDN BVZAUM // Вестник Казанского юридического института МВД России. — 2024. — Т. 15, № 4 (58). — С. 161–170.

8. Шнейдерова Д.И. Криминалистический анализ способов хищений в сфере оборота криптовалют / Д.И. Шнейдерова. — DOI 10.51980/2542-1735_2020_2_41. — EDN GMNREF // Вестник Сибирского юридического института МВД России. — 2020. — № 2 (39). — С. 41–48.

9. Коломинов В.В. Особенности расследования преступлений, совершенных с использованием криптовалюты / В.В. Коломинов. — DOI 10.17150/2411-6122.2025.1.60-68. — EDN MXNHWT // Сибирские уголовно-процессуальные и криминалистические чтения. — 2025. — № 1. — С. 60–68.

10. Шнейдерова Д.И. Способы подготовки, совершения и сокрытия хищений в сфере оборота криптовалют: криминалистическая характеристика / Д.И. Шнейдерова. — EDN MBDIMP // Вестник Могилевского института МВД. — 2022. — № 1 (5). — С. 77–82.

References

1. Repetskaya A.L., Mironov A.O. Cryptocurrency as an Object of Criminal Law and Criminological Research. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii = Vestnik of the Eastern Siberia Institute of the Ministry of the Interior of the Russian Federation*, 2022, no. 3, pp. 109–120. (In Russian). EDN: XLTNYQ. DOI: 10.55001/2312-3184.2022.78.15.010.

2. Dolgieva M.M. Social Conditionality of the Emergence of Criminal Law Prohibitions of Violations Committed in the Field of Cryptocurrency Turnover. *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law*, 2018, no. 10, pp. 225–235. (In Russian). EDN: YOICCD. DOI: 10.17803/1994-1471.2018.95.10.225-235.

3. Shneiderova D.I. *Anonymity as a Method of Concealing Theft in the Sphere of Cryptocurrency Trade. Collected Papers*. Moscow, 2020, pp. 181–186. (In Russian). EDN: LXFFTE.

4. Stukonog I.V. Cryptocrime as a New Type of Crime: Concept and Specificity. *Sovremennoe pravo = Modern Law*, 2018, no. 10, pp. 109–115. (In Russian). EDN: CBKUCR.

5. Kapinus O.S. Digitalization of Crime and Criminal Law. *Baikal Research Journal*, 2022, vol. 13, no. 1, pp. 22–22. (In Russian). EDN: NZNOMN. DOI: 10.17150/2411-6262.2022.13(1).22.

6. Makarenko I.A. The Contents of Criminalistic Support of Crime Investigation. *Criminalistics, Criminal Process and Forensic Expertise in the 21st Century: Development Vectors. Materials of International Scientific Conference, Moscow, April 25, 2025.* Moscow, 2025, pp. 119–127. (In Russian).

7. Shneiderova D.I. Theft in the Sphere of Cryptocurrency Turnover in the Structure of Cybercrime: Types, Problems of Investigation (Belarusian Experience). *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA Russia*, 2024, vol. 15, no. 4, pp. 161–170. (In Russian). EDN: BVZAUM. DOI: 10.37973/VESTNIKKUI-2024-58-20.

8. Shneiderova D.I. Criminalistic Analysis of Methods of Theft in the Sphere of Cryptocurrency Turnover. *Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii = Vestnik of Siberian Law Institute of the MIA of Russia*, 2020, no. 2, pp. 41–48. (In Russian). EDN: GMNREF. DOI: 10.51980/2542-1735_2020_2_41.

9. Kolominov V.V. Specific Features of Investigating Crimes Committed with the Use of Cryptocurrency. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2025, no. 1, pp. 60–68. (In Russian). EDN: MXNHWT. DOI: 10.17150/2411-6122.2025.1.60-68.

10. Shneiderova D.I. Methods of Preparation, Commission and Concealment of Thefts in the Sphere of Cryptocurrency Turnover: Criminalistic Characteristics. *Vestnik Mogilevskogo instituta MVD = Bulletin of Mogilev Institute of the Ministry of Internal Affairs*, 2022, no. 1, pp. 77–82. (In Russian). EDN: MBDIMP.

Информация об авторе

Гайсин Нурсултан Ильгизович — аспирант, кафедра криминалистики, Уфимский университет науки и технологий, г. Уфа, Российская Федерация.

Author Information

Gaisin, Nursultan I. — Ph.D. Student, Department of Criminalistics, Ufa University of Science and Technology, Ufa, the Russian Federation.

Поступила в редакцию / Received 03.05.2025
Одобрена после рецензирования / Approved after reviewing 30.06.2025
Принята к публикации / Accepted 19.09.2025
Дата онлайн-размещения / Available online 16.10.2025