



Научная статья

УДК 343.346.2

EDN: <https://elibrary.ru/OVHWCH>

ИПОН: 2007-0083-1/26-776

MOSURED: 77/27-005-2026-01-976

Правовое регулирование противодействия мошенничеству с цифровыми активами

Элиза Борисовна Михлина

Российский государственный университет правосудия имени В.М. Лебедева, Москва, Россия,

Mikhlina200@mail.ru

Аннотация. Исследуется комплекс правовых проблем, возникающих при квалификации и пресечении противоправных деяний с использованием цифровых активов. Особый акцент сделан на правовом регулировании квалификации мошеннических действий с цифровыми активами. Анализируется несоответствие традиционных составов преступлений, таких как мошенничество, специфике отношений в цифровой среде, выделены и проанализированы наиболее распространенные в настоящее время мошеннические схемы в данной сфере. Рассматриваются типичные схемы незаконного завладения криптовалютой и иными токенами. Предлагаются меры по совершенствованию отечественной правоприменительной практики и уголовно-правовых норм для эффективной защиты имущественных интересов в условиях цифровой трансформации экономики. Выделены определенные меры, способствующие развитию правоприменительной практики и методов борьбы с нарушениями законодательства в сфере обращения с цифровыми активами.

Ключевые слова: цифровые финансовые активы, цифровая валюта, мошенничество, противодействие мошенничеству, квалификация мошенничества

Для цитирования: Михлина Э. Б. Правовое регулирование противодействия мошенничеству с цифровыми активами // Криминологический журнал. 2026. № 1. С. 130–136. EDN: OVHWCH.

Original article

Legal regulation of countering digital asset fraud

Elisa B. Mikhlina

Russian State University of Justice named after V.M. Lebedev, Moscow, Russia, Mikhlina200@mail.ru

Abstract. The complex of legal problems arising in the qualification and suppression of illegal acts using digital assets is being investigated. Special emphasis is placed on the legal regulation of the qualification of fraudulent actions with digital assets. The discrepancy between traditional crimes, such as fraud, and the specifics of relations in the digital environment is analyzed, and the most common fraudulent schemes in this area are identified and analyzed. Typical schemes of illegal acquisition of cryptocurrencies and other tokens are considered. Measures are proposed to improve domestic law enforcement practice and criminal law norms for the effective protection of property interests in the context of the digital transformation of the economy. Certain measures have been identified that contribute to the development of law enforcement practices and methods to combat violations of legislation in the field of digital asset management.

Keywords: digital financial assets, digital currency, fraud, fraud prevention, fraud qualification

For citation: Mikhlina E. B. Legal regulation of countering digital asset fraud. Criminological Journal. 2026;(1):130–136. (In Russ.). EDN: OVHWCH.

© Михлина Э. Б., 2026



В современную эпоху стремительный прогресс в области информационно-коммуникационных средств коренным образом трансформировал традиционные модели гражданско-правовых отношений. Появление и широкое распространение разнообразных технологических платформ и устройств для заключения соглашений способствовало формированию таких видов имущественных благ как криптовалюты, цифровые активы и иные, ранее неизвестные правовому полю, а также юридических возможностей по их истребованию. Правовая сущность этих новейших категорий остается предметом оживленных теоретических споров и неоднозначных трактовок среди представителей как научного сообщества, так и юридической практики [2; 5–8; 10].

Общественные отношения в текущий период характеризуются глубокой и всепроникающей цифровой трансформацией. Если проанализировать сферу денежного обращения через призму взаимодействия ее участников, то очевиден кардинальный сдвиг: на смену прямому личному контакту, доминировавшему в прошлом, пришли полностью дистанционные операции. Сегодня такие взаимодействия реализуются в пространстве виртуальной реальности посредством сложных информационно-телекоммуникационных систем, ярким примером чему служит использование активов, основанных на криптографических технологиях, таких как криптовалюты.

Феномен цифровых финансовых активов, включая криптовалюты, представляет собой принципиально новое явление для экономических и правовых систем. Государственная политика в настоящее время сфокусирована на создании комплексного нормативного регулирования для данной сферы, что находит прямое подтверждение в факте принятия специального закона — Федерального закона № 259-ФЗ от 31 июля 2020 г. «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [13].

В соответствии с этим нормативным актом, законодатель определяет цифровые финансовые активы как особый вид цифровых прав. К ним отнесены, в частности, требования денежного характера, возможности реализации прав из эмиссионных ценных бумаг, доли в уставном капитале непубличных акционерных обществ, а также права требования передачи подобных ценных бумаг. Ключевой технологической особенностью является то, что выпуск, учет и все операции с такими активами возможны исключительно путем фиксации записей в специальных информационных системах, в том числе построенных на основе распределенных реестров.

Динамика развития криптовалютного сегмента в условиях цифрового общества отличается исключительной скоростью и постоянным обновлением.

Процесс создания новых видов цифровых валют непрерывен, что отчасти связано с возникновением технических, экономических и регуляторных сложностей, присущих более ранним их прототипам.

С точки зрения гражданско-правовой доктрины, под цифровыми правами подразумеваются субъективные имущественные права конкретного носителя, которые существуют не в материальной, а в цифровой форме, будучи выраженными в виде уникального кода или записи.

Таким образом, это по своей природе остается правом на имущественную ценность, но облеченным в специфическую, нематериальную форму. Данный законодательный подход порождает серьезные дискуссии в научной среде.

В этой связи является вполне обоснованной критика, высказанная рядом ученых, например, С. В. Сарбашем, который указывает на условность самой категории «цифровые права» [12]. По его мнению, вводимая законодателем конструкция может рассматриваться как юридическая фикция, потребность в которой не была должным образом аргументирована фундаментальными научными изысканиями и всесторонним анализом природы регулируемых отношений.

Существующие в юридической науке теоретические противоречия и пробелы в законодательстве напрямую осложняют работу правоприменительных органов при расследовании и юридической оценке действий недобросовестных финансовых операторов. Злоумышленники часто предлагают гражданам инвестиционные схемы, сулящие баснословную прибыль от торговли на криптовалютных биржах, а также вводят в оборот собственные цифровые единицы — токены, движение которых крайне сложно отследить и проконтролировать [11].

В контексте уголовно-правовой действительности России одним из наиболее массовых и социально опасных деяний продолжает оставаться мошенничество, ответственность за которое установлена ст. 159–159.6 Уголовного кодекса Российской Федерации [14]. Согласно легальной дефиниции, под этим преступлением понимается противоправное изъятие имущества, принадлежащего другому лицу, либо незаконное получение юридических прав на такое имущество, осуществленное посредством введения потерпевшего в заблуждение или использования особых доверительных отношений.

Рост преступной активности в криптосфере, измеряемый в многократном увеличении числа инцидентов, обусловлен комплексом взаимосвязанных причин.

1. Колоссальный рост объемов нелегальных доходов закономерно порождает спрос на инновационные, высокотехнологичные методы их легализации, позволяющие скрыть происхождение средств [9].



2. Отсутствие четкого правового статуса виртуальных валют и действенных механизмов финансового надзора за их оборотом создает питательную среду для возникновения псевдофинансовых организаций. Эти структуры, используя технологию распределенного реестра, либо обеспечивают анонимное хранение денежных потоков, либо специализируются на конвертации криптоактивов в традиционные (фиатные) деньги.

3. К настоящему моменту на государственном уровне не сформирована единая и эффективная стратегия профилактики правонарушений в данной области.

В последние годы отмечается стремительная эскалация мошенничеств с применением цифровых валют. Важно подчеркнуть, что преступники постоянно эволюционируют, не ограничиваясь устоявшимися схемами, а активно изобретая новые, соответствующие последним технологическим трендам, методики реализации своих противоправных замыслов.

К числу наиболее распространенных разновидностей криптомошенничеств можно отнести следующие.

Фишинговые ресурсы и поддельные кошельки.

В условиях развития цифровых технологий злоумышленники освоили создание детально скопированных дубликатов легитимных веб-сайтов. На таких ресурсах пользователь, не подозревая об обмане, может заниматься майнингом или покупкой виртуальной валюты. Мошенники часто изменяют в адресе всего один символ, а идентичность дизайна и интерфейса делает подмену практически незаметной для жертвы. Регистрируясь на фишинговом портале, пользователь добровольно передает конфиденциальные данные в распоряжение киберпреступников [15].

Для хранения криптоактивов необходимы специальные электронные кошельки, которые содержат как сами цифровые ценности, так и историю всех операций в блокчейне. Злоумышленники разрабатывают и распространяют фальшивые приложения, маскирующиеся под известные кошельки (например, GreenAddress, Simple Bitcoin Wallet), цель которых — хищение средств. Установив такое приложение, пользователь активно им пользуется, а при достижении остатком на счете определенного порога средства автоматически переводятся разработчикам-мошенникам.

Схема Понци (криптопирамида).

Данная модель хищения имеет общие черты с классической финансовой пирамидой, где деньги новых вкладчиков используются для выплат «доходов» предыдущим участникам. Механизм Понци основан на перераспределении средств: выплаты «прибыли» ранним инвесторам осуществляются исключительно за счет взносов тех, кто присоединился позднее. Ярким примером является платформа Bitconnect, основатель которой, Сатиш Кумбхани, был привлечен к ответственности за организацию масштабного крип-

томошенничества [16]. В 2021 г. Банк России опубликовал перечень организаций, демонстрирующих признаки нелегальных финансовых пирамид, куда вошли, в частности, Crypto-Max, Crypto Inc и Exchange Coindesk [17].

Облачный майнинг.

Суть этого мошенничества заключается в привлечении инвестиций под ложные предлоги. Жертвам предлагают вложить деньги в развитие якобы существующего мощного дата-центра для добычи биткоинов, обещая регулярный процент от будущей «прибыли» [1].

Мошеннические обменные сервисы и биржи.

Добытая майнингом криптовалюта сама по себе не может служить законным средством платежа на территории РФ, где таковым является только рубль. Для ее конвертации используются специализированные площадки. Мошеннические биржи заманивают клиентов выгодными условиями: множеством способов пополнения депозита, низкими комиссиями и курсами. Однако после внесения средств и покупки криптовалюты (например, BTC) пользователь сталкивается с невозможностью их вывода обратно.

Практика «пампинга» (искусственного накачивания стоимости).

Отличительная черта этого мошенничества — целенаправленное манипулирование рыночной ценой цифрового актива. Преступная группа скупает большой объем малоизвестной криптовалюты, после чего начинает массовую рассылку ложных или вводящих в заблуждение сообщений. В них, часто под видом «инсайдерской» информации, инвесторов призывают срочно покупать данный актив, прогнозируя его взрывной рост. В результате ажиотажного спроса, созданного обманутыми пользователями, цена действительно растет, после чего организаторы схемы моментально продают свои запасы по завышенной стоимости, обрушая рынок и оставляя остальных владельцев с обесценившимися активами.

Анализ преступных схем, связанных с дистанционным хищением имущества, а также с манипуляциями разнообразными объектами, выраженными в цифровой форме, сопряжен для правоприменителей и исследователей со значительными сложностями в части юридической оценки этих деяний.

Это объясняется тем, что в условиях современной цифровой экономики злоумышленники активно внедряют ранее неизвестные методы нанесения имущественного вреда, применяя новейшие технологические решения. Правовой режим применения и использования таких технологий либо вообще не урегулирован действующим гражданским и финансовым законодательством России, либо их трактовка в нормативных актах отличается неопределенностью и порождает множество дискуссионных вопросов [18].



С позиции гражданско-правового и финансового регулирования процедура конвертации традиционных денежных средств в токены с их последующей трансформацией в виртуальные условные единицы сама по себе не образует состава правонарушения. Подобные активы находят свое отражение в ст. 128 и 141.1 Гражданского кодекса Российской Федерации и легализуются в качестве так называемых «цифровых прав».

Диспозитивная природа гражданского права, закрепленная в ст. 8 ГК РФ, подразумевает, что юридически значимые права и обязанности могут возникать не только из прямо предусмотренных законом оснований, но и из действий субъектов, которые, не будучи прописаны в нормативных актах, соответствуют основным началам и смыслу всего гражданского законодательства.

Аналогично, в силу ст. 421 ГК РФ, физические и юридические лица обладают свободой договора и могут заключать как поименованные, так и непоименованные в законе соглашения. Однако в контексте подобных операций остро встает проблема идентификации правообладателя: какими доказательствами участники схемы могут подтвердить законность своих имущественных притязаний?

В соответствии с п. 1 и 2 ст. 140 Гражданского кодекса РФ единственным законным платежным средством, обязательным к приему на всей территории страны, является российский рубль. В этом ключе различные титульные знаки, представляющие собой виртуальные единицы расчетов внутри конкретных электронных систем, эмитируемые самими пользователями, не признаются разрешенным средством платежа. Следовательно, они не могут являться объектом договора цессии (уступки права требования). Также их нельзя отнести к вещам, определяемым родовыми признаками, поскольку они лишены материальной формы и не существуют в физически осязаемом пространстве.

Важную правовую позицию по данному вопросу сформулировал Верховный Суд РФ в Определении от 1 июня 2021 г. № 48-КГ21-3-К7 [19]. Суд указал, что виртуальные расчетные единицы, вне зависимости от их валютного эквивалента, изначально приобретаются за вполне реальные денежные средства и, таким образом, обладают опосредованной, но очевидной материальной связью с имуществом как предметом преступного посяательства.

Из этого следует важный для квалификации вывод: при рассмотрении подобных действий как мошеннических, предметом преступления должны признаваться не сами виртуальные единицы, а те реальные денежные средства, которые потерпевший затратил на их приобретение, но не получил взамен ожидаемого актива или услуги.

После рассмотрения типичных способов соверше-

ния криптовалютных мошенничеств целесообразно перейти к вопросу о методике их выявления и расследования. Как отмечает И. И. Кучеров, традиционная методика расследования финансовых преступлений в значительной степени базируется на получении необходимой информации от кредитных организаций, которые предоставляют ее следственным органам в документальной форме на основании официальных запросов. Однако в случае с операциями, использующими криптовалюту, реализовать такой подход не представляется возможным [4, с. 19].

Это обусловлено фундаментальным отличием криптовалютных транзакций: в них полностью отсутствует посредническая функция как банков, так и небанковских кредитных учреждений. Все расчеты осуществляются по принципу peer-to-peer, т. е. напрямую между отправителем и получателем средств, что радикально усложняет традиционный следственный путь, связанный с отслеживанием денежных потоков через финансовые институты.

При осуществлении расследования уголовных дел, связанных с противоправными операциями с использованием цифровых валют, центральной задачей следствия становится установление первоначального источника, с которого произошло списание денежных средств. Для решения этой задачи в первую очередь требуется идентифицировать криптографический адрес кошелька, т. е. установить его открытый (публичный) и закрытый (приватный) ключи.

После этого уполномоченный орган традиционно формирует официальный запрос о предоставлении документации или сведений, касающихся операций с виртуальной валютой. Однако специфика альтернативных платежных инструментов, функционирующих в сети Интернет, заключается в отсутствии единого администратора или иного субъекта, который бы осуществлял централизованное управление всеми транзакциями. Вследствие этой децентрализованной архитектуры правоохранительные структуры лишены возможности адресного направления подобных запросов конкретному ответственному лицу или организации.

В рамках процессуальных действий крайне важно определить целевое назначение осуществленного перевода. Для достижения данной цели следователям необходимо проводить допросы, а также очные ставки с привлечением лиц, выступавших в роли отправителя и получателя средств. Каждая операция в данной сфере оставляет неизгладимый цифровой отпечаток в распределенном реестре — блокчейне. Этот факт предоставляет оперативным сотрудникам возможность путем проведения специализированных оперативно-розыскных мероприятий выявлять обстоятельства, свидетельствующие о противозаконном получении криптовалюты.



Важнейшими элементами, подлежащими установлению в процессе расследования для установления наличия состава преступления, являются: наименование криптовалютной биржи и данные учетной записи (аккаунта), с которых было произведено хищение финансовых активов; технический способ осуществления транзакции; точные суммы всех операций; а также все сопутствующие реквизиты и иная значимая информация.

Необходимо особо подчеркнуть, что цифровые технологии, в том числе лежащая в их основе система распределенного реестра (блокчейн), представляют собой принципиально инновационный феномен, коренным образом отличающийся от классических банковских механизмов. Технология блокчейн играет ключевую роль в процессах документирования и формирования доказательственной базы. Как отмечает В. П. Галушин [3, с. 91], оставляемые в цифровой среде следы создают новые, дополнительные возможности для доказывания фактов криминального использования виртуальных активов.

В текущих условиях обеспечение сохранности криптовалютных активов пользователя выступает в качестве приоритетной функции для сервисов онлайн-кошельков, а также локальных и мобильных приложений. В этих электронных системах повсеместно применяются такие средства защиты, как двухфакторная аутентификация и специальная seed-фраза (сид-фраза), предназначенная для восстановления доступа.

Согласно существующим прогнозам, в ближайшей перспективе ожидается рост уровня мошеннической активности с применением цифровых активов. Особую актуальность этот тренд приобретает в связи с внедрением цифрового рубля, который, начиная с 1 августа 2023 г., официально приобрел статус третьей формы национальной валюты наравне с наличными и безналичными деньгами.

Для противодействия дальнейшей эскалации преступности в сфере виртуальных активов государственным органам необходимо системно решать задачи, направленные, с одной стороны, на профилактику мошенничеств с использованием криптовалют, а с другой — на сохранение и поддержку инвестиционного потенциала граждан. Население традиционно стремится к повышению уровня личного благосостояния путем размещения свободных средств на банковских депозитах.

Однако с течением времени финансовые организации предлагают все менее привлекательные условия: процентные ставки снижаются, в то время как уровень инфляции в экономике сохраняется на значимом уровне. В результате граждане вынуждены искать альтернативные, более доходные способы инвестирования, зачастую не подозревая, что многие из предлагаемых в digital-среде схем носят откровенно мошеннический характер.

Помимо этого, можно сделать вывод о том, что для обеспечения эффективного противодействия мошенничеству с цифровыми активами необходимо активное совершенствование действующего законодательства. Одним из предложений может стать расширение полномочий Банка России с целью предоставления ему возможности производить блокировку подозрительных операций, что будет способствовать снижению уровня финансовых потерь как физических, так и юридических лиц.

Также представляется, что результативным механизмом в осуществлении вышеназванного противодействия может послужить усиление ответственности за нарушение неприкосновенности частной жизни, к которой может относиться торговля персональными данными лиц. Для того, чтобы совершить мошеннические действия с использованием, к примеру, банковских реквизитов лица, либо его криптовалютой, преступнику необходимо обладать информацией о реквизитах лица. Такую информацию можно найти в сети Интернет, так как зачастую ее продают на различных платформах. В связи с этим, усиление санкции за данные деяния в ст. 137 УК РФ представляется действенным механизмом.

Наконец, создание некой единой базы кибермошенников позволит правоохранительным органам более оперативно реагировать на выявленные признаки мошеннических действий, так как он будет содержать систематизированную информацию как о самих преступлениях, так и о лицах, их совершивших.

Таким образом, весь комплекс указанных мер будет способствовать адаптации правового регулирования противодействия мошенничеству с цифровыми активами к новым реалиям действительности. Такой комплексный подход, объединяющий в себе как правовое регулирование и достаточный уровень квалификации правоохранительных органов, так и сознательность самих людей, позволит значительным образом снизить уровень мошенничества с цифровыми активами.

Список источников

1. Архипов А. В. Мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) // Уголовное право. 2019. № 5. С. 16–20.
2. Бурмистрова А. А., Осокин Р. Б. Уголовно-правовая характеристика провокации взятки либо коммерческого подкупа // Криминологический журнал. 2021. № 1. С. 35–38.
3. 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.
4. Кучеров И. И. К вопросу о методике расследования преступлений, совершенных с исполь-



- зованием криптовалюты // Российский следователь. 2018. № 12. С. 17–21.
5. Осокин Р. Б., Немтинов Д. В. К вопросу о признаках преступлений в сфере экономической деятельности, совершаемых путем обмана и (или) злоупотребления доверием // Общество и право. 2016. № 2 (56). С. 121–128.
 6. Осокин Р. Б., Ковригин В. С. К вопросу о совершенствовании уголовного законодательства об ответственности за присвоение или растрату // Вестник Московского университета МВД России. 2025. № 1. С. 118–123.
 7. Осокин Р. Б. К вопросу о целесообразности применения конфискации имущества при назначении наказания за мошенничество (российский и таджикский опыт) // Вестник экономической безопасности. 2025. № 3. С. 104–108.
 8. Осокин Р. Б. Психологические особенности личности мошенников // Профессиональное образование сотрудников органов внутренних дел. Педагогика и психология служебной деятельности: состояние и перспективы: сб. науч. тр. II междунар. конф. (Москва, 6–7 июня 2018 г.). М. : Московский университет МВД России имени В.Я. Кикотя, 2018. С. 600–602.
 9. Иванцов С. В., Сидоренко Э. Л., Спасенников Б. А. и др. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции // Всероссийский криминологический журнал. 2019. Т. 13. № 1. С. 85–93.
 10. Рожкова М. А. Цифровые права (digital rights) — что это такое и нужны ли они в Гражданском кодексе? // Закон.ру. 17 авг. 2020.
 11. Урошлева А. Объекты на цифровых носителях, цифровые права и деньги: тенденции правовой теории и практики // URL: <https://www.garant.ru/article/1220358/>
 12. Экспертное заключение Совета при Президенте РФ по кодификации и совершенствованию гражданского законодательства по проекту федерального закона № 424632-7 «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации» // URL: <http://privlaw.ru/wp-content/uploads/2018/04/meeting-190418-zakonoproekt-2-project-conclusion.pdf>
 13. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31. Ч. I. Ст. 5018.
 14. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.
 15. Ключевые определения и потенциальные риски в сфере ПОД/ФТ // URL: https://eurasian-group.org/files/FATF_docs/Virtualnye_valyuty_FATF_20i4.pdf
 16. Bits Media. Биткоин форум // URL: <https://bits.media/organizatoru-piramidy-bitcon-nect-predyavleny-ofitsialnye-obviniya/>
 17. В черный список ЦБ попали представители криптоиндустрии // URL: <https://www.rbc.ru/crypto/news/60b609409a7947268c5945>
 18. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32. Ст. 3301.
 19. Определение СК по гражданским делам Верховного Суда Российской Федерации от 1 июня 2021 г. № 48-КГ21-3-К7 // URL: <https://www.garant.ru/products/ipo/prime/doc/401291417/>

References

1. Arkhipov A. V. Fraud using electronic means of payment (art. 159.3 of the Criminal Code of the Russian Federation) // Criminal law. 2019. No. 5. P. 16–20.
2. Burmistrova A. A., Osokin R. B. Criminal and legal characteristics of provocation of a bribe or commercial bribery // Criminological Journal. 2021. No. 1. P. 35–38.
3. Galushin P. V., Karlov A. L. Information on operations with cryptocurrencies (using Bitcoin as an example) as evidence in a criminal case // Scientific Notes of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2017. Vol. 2. No. 4.
4. Kuchеров I. I. On the issue of the methodology for investigating crimes committed using cryptocurrencies // Russian investigator. 2018. No. 12. P. 17–21.
5. Osokin R. B., Nemtinov D. V. On the issue of signs of crimes in the sphere of economic activity committed by deception and (or) abuse of trust // Society and Law. 2016. No. 2 (56). P. 121–128.
6. Osokin R. B., Kovrigin V. S. On the issue of improving criminal legislation on liability for embezzlement or embezzlement // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2025. No. 1. P. 118–123.
7. Osokin R. B. On the question of the expediency of using confiscation of property when punishing fraud (Russian and Tajik experience) // Bulletin of Economic Security. 2025. No. 3. P. 104–108.
8. Osokin R. B. Psychological characteristics of



- the personality of fraudsters // Professional education of law enforcement officers. Pedagogy and psychology of professional activity: current state and prospects: Collection of scientific papers of the II International Conference (Moscow, June 6–7, 2018). М. : Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', 2018. P. 600–602.
9. Ivantsov S. V., Sidorenko E. L., Spasennikov B. A. and others. Crimes related to the use of cryptocurrencies: the main criminological trends // All-Russian Journal of Criminology. 2019. Vol. 13. No. 1. P. 85–93.
 10. Rozhkova M. A. Digital rights — what are they and are they needed in the Civil Code? // Zakon. ru. August 17, 2020.
 11. Uroshleva A. Objects on digital media, digital rights and money: trends in legal theory and practice // URL: <https://www.garant.ru/article/1220358/>
 12. Expert opinion of the Presidential Council for the Codification and Improvement of Civil Legislation on the draft Federal Law No. 424632-7 «On Amendments to Parts One, Two and Four of the Civil Code of the Russian Federation» // URL: <http://privlaw.ru/wp-content/uploads/2018/04/meeting-190418-zakonoproekt-2-project-conclusion.pdf>
 13. Federal Law No. 259-FZ of July 31, 2020
 - «On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation» // Collection of Legislation of the Russian Federation. 2020. No. 31. Part I. Art. 5018.
 14. Criminal Code of the Russian Federation dated June 13, 1996 No. 63-FZ // Collection of Legislation of the Russian Federation. 1996. No. 25. Art. 2954.
 15. Key definitions and potential risks in the field of AML/CFT // URL: https://eurasian-group.org/files/FATF_docs/Virtualnye_valyuty_FATF_20i4.pdf
 16. Bits Media. Bitcoin Forum // URL: <https://bits.media/organizatoru-piramidy-bitcon-nect-predyavleny-ofitsialnye-obvineniya/>
 17. Representatives of the crypto industry were blacklisted by the Central Bank // URL: <https://www.rbc.ru/crypto/news/60b609409a7947268c5945>
 18. The Civil Code of the Russian Federation (part one) of November 30, 1994, No. 51-FZ // Collection of Legislation of the Russian Federation. 1994. No. 32. Art. 3301.
 19. Definition of the IC on Civil cases of the Supreme Court of the Russian Federation dated June 1, 2021 No. 48-KG21-3-K7 // URL: <https://www.garant.ru/products/ipo/prime/doc/401291417/>

Информация об авторе

Э. Б. Михлина — аспирант Российского государственного университета правосудия имени В.М. Лебедева.

Information about the author

E. B. Mikhlina — Postgraduate student of the Russian State University of Justice named after V.M. Lebedev.

Статья поступила в редакцию 09.02.2026; одобрена после рецензирования 16.02.2026; принята к публикации 24.02.2026.

The article was submitted 09.02.2026; approved after reviewing 16.02.2026; accepted for publication 24.02.2026.