

Преступления, связанные с обращением криптовалют: особенности квалификации



Е.А. Русскевич

Доцент, кафедра уголовного права Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук. Адрес: 117997, Российская Федерация, Москва, ул. Академика Волгина, 12. E-mail: russkevich@mail.ru



И.И. Малыгин

Консультант, отдел государственной регистрации нормативных правовых актов в социальной и культурной сферах Департамента регистрации ведомственных нормативных правовых актов Министерства юстиции Российской Федерации. Адрес: 119991, Российская Федерация, Москва, Житная ул., д.14. E-mail: aspugpravo@yandex.ru



Аннотация

Процесс проникновения цифровых финансовых активов в повседневную жизнь граждан и деятельность хозяйствующих субъектов, а равно неуклонный рост преступлений, совершаемых с использованием, в отношении и по поводу криптовалют, актуализируют необходимость научного осмысления особенностей их квалификации. Цель исследования состоит в разработке теоретических рекомендаций к преодолению проблем, возникающих в связи с квалификацией такого рода преступлений. Реализация указанной цели достигалась путем изучения позиций по проблеме в отечественной доктрине уголовного права, оценки состояния отечественного уголовного законодательства, выявления проблем в судебно-следственной практике. Исследование основано на применении общенаучных и специальных методов (анализ, синтез, индукция, формально-юридический, абстрактно-логический и др.). Авторы формулируют выводы: во-первых, в современных условиях выделяются следующие основные группы преступлений, сопряженных с использованием в той или иной форме цифровых финансовых активов (криптовалют): преступления, в которых криптовалюта выступает средством их совершения; преступления, в которых криптовалюта выступает предметом посягательства; преступления, совершаемые в целях генерации (майнинга) криптовалюты; Во-вторых, использование лицом криптовалюты не может априорно свидетельствовать, что имела место легализация. Простое распоряжение виртуальной валютой (в целях оплаты товаров или услуг) без намерения придания правомерного вида преступным доходам не содержит признаков состава преступления, предусмотренного ст. 174.1 Уголовного кодекса. В-третьих, как незаконное предпринимательство (ст. 171) следует квалифицировать осуществление лицом деятельности, связанной с обменом криптовалюты на фиатные денежные средства и наоборот, направленной на получение прибыли за счет взимания комиссии по каждой операции. Поскольку лицензирование таких услуг невозможно по действующему законодательству, лицо несет ответственность за незаконное предпринимательство, если оно осуществляло указанную деятельность без

регистрации. В-четвертых, при квалификации посягательств на криптовалюту правоприменительные органы в качестве системной проблемы отмечают отсутствие на территории России органа, уполномоченного дать оценку ее стоимости на конкретную дату.



Ключевые слова

уголовное право, криптовалюта, цифровые финансовые активы, преступления, компьютерная информации, информационная безопасность.

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

УДК: 343

DOI: 10.17323/2072-8166.2021.3.106.125

Введение

Квалификация преступлений, совершаемых с использованием криптовалют, в целом основывается на общих руководящих началах (принципах) и правилах уголовно-правовой оценки деяния [Пинкевич Т.В., 2020: 45–48]. В рамках настоящего исследования нет цели рассмотреть каждое из указанных правил в отдельности, осветив множество доктринальных позиций и возможные проблемы правоприменения. Остановимся на вопросах, которые в современных условиях «привыкания» отечественного правоприменителя к новой (криптовалютной) преступности имеют сугубо прикладное значение. Несмотря на наличие известного правового вакуума¹, следует согласиться с мнением А.Н. Лясколо, что «расширение сферы обращения и повышенный криминальный интерес к использованию криптовалюты все чаще вынуждают правоприменителя признавать ее предметом или средством преступления» [Лясколо А.Н., 2019: 89].

Изучение доктринальных трудов и материалов отечественной судебной следственной практики позволяет выделить следующие основные группы преступлений, сопряженных с использованием в той или иной форме цифровых финансовых активов (криптовалют): преступления, в которых криптовалюта выступает средством их совершения; преступления, в которых

¹ В нашей стране оборот криптовалюты до настоящего времени не урегулирован. В Государственной Думе находится на рассмотрении сразу несколько законопроектов, направленных на решение данной проблемы. Статус криптовалюты оговаривается в предостережении Центробанка России от 27.01.2014 «Об использовании при совершении сделок «виртуальных валют», в письмах ФНС от 03.10.2016 № ОА-18-17/1027 и 13.10.2017 № 03-04-05/66994, информационном письме Федеральной службы по финансовому мониторингу от 06.01.2017 «Об использовании криптовалют», где она определяется как денежный суррогат.

криптовалюта выступает предметом посягательства; преступления, совершаемые в целях генерации (майнинга) криптовалюты.

По меткому замечанию М.И. Немовой, «попытка осмысления возможности применения Уголовного кодекса к преступным посягательствам, совершаемым посредством или в отношении криптовалют, — это попытка помещения динамично развивающихся экономических отношений в прокрустово ложе консервативного по своей сути уголовного закона» [Немова М.И., 2018: 585]. Согласимся с автором — во многом это действительно так. Однако зададимся вопросом — что же остается доктрине в условиях задумавшегося (надолго ли?) над проблемой законодателя? Ответ очевиден: на основе скрупулезного обобщения и анализа отдельных казусов, используя допустимую интерпретационную емкость уголовного закона, готовить рекомендации для правоприменительной практики, которая вынуждена уже сейчас реагировать на новые вызовы и угрозы, связанные с блокчейн-революцией.

Методологический инструментарий исследования включает комплексное сочетание общенаучных и частнонаучных средств познания. Из общенаучных методов научного познания использованы анализ, синтез, дедукция, индукция, классификация, структурно-функциональный и др. Особое значение в методологии исследования отведено системному методу, который выступал исходной посылкой при решении всех поставленных исследовательских задач. Эмпирические методы (анализ документов, печатных и электронных изданий) применены при накоплении и изучении материалов правоприменительной практики в целях выявления проблем совершенствования уголовно-правового противодействия преступлениям, совершаемым с использованием, в отношении и по поводу криптовалют.

1. Преступления, в которых криптовалюта выступает средством их совершения

Первую группу преступлений, с каждым днем получающих все большее распространение, составляют деяния, связанные с оборотом предметов, ограниченных или запрещенных в гражданском обороте, в которых криптовалюта выступает платежным инструментом. К таковым, прежде всего, относятся преступления, связанные с незаконным оборотом наркотических средств и психотропных веществ, оружия, а также порнографических материалов. Так, по одному из дел суд указал, что подсудимый примерно в январе 2019 г. посредством Интернета заплатил 25 000 руб., переведя указанные денежные средства в неотслеживаемую криптовалюту «Биткоин», перечислил указанные платежные средства на интернет-сайт «Рутор», осуществив заказ оружия. Затем, действуя умышленно и незаконно, приобрел путем подбора «тайника-закладки» в неустановленном месте возле станции метро «Нага-

тинская» в Москве пистолет, который был переделан самодельным способом из сигнального пистолета «МР-371». Также, имея на то преступный умысел, в неустановленное время, но не позднее 7.03. 2019, в неустановленном месте Москвы приобрел боеприпасы: 66 патронов калибра 9 мм. Не имея лицензии на приобретение оружия, его основных частей и боеприпасов, действуя в нарушение Федерального закона № 150-ФЗ «Об оружии» от 13.12.1996, и зная, что установлена уголовная ответственность за незаконный оборот оружия, его основных частей и боеприпасов, он обратил пистолет и патроны в свое противоправное владение, поместив их в своей квартире².

С использованием виртуальной валюты приобретаются также поддельные официальные и важные личные документы. Так, К. был осужден по ч. 3 ст. 327 Уголовного кодекса Российской Федерации (далее — УК РФ). Согласно приговору суда, К. приобрел поддельное водительское удостоверение на право управления транспортными средствами категории «В» через Интернет. Сумма заказа составила 40 000 рублей. С исполнителем все общение проходило посредством текстовых сообщений. К. оплатил всю сумму путем списания денежных средств с его электронного кошелька. Предварительно данную сумму он перевел в электронную валюту «Биткоин». Также через Интернет он переслал свою фотографию. Через две недели курьерской службой ему домой привезли конверт, в котором находилось водительское удостоверение на имя другого человека (Б.), но с фотографией К.³

Следует сделать вывод, что в судебно-следственной практике, как правило, нет трудностей в квалификации таких преступлений. Само по себе использование криптовалюты для приобретения соответствующих предметов не оказывает значимого влияния на оценку содеянного пост. 222, 228, 228.1 УК РФ и др., а относится в большей мере к криминологической и криминалистической характеристике содеянного. Равным образом специалисты сходятся во мнении, что использование цифровых финансовых активов не создает значимых проблем при юридической оценке финансирования преступной деятельности по ст. 205¹, 208, 282³, 359 УК РФ [Бегишев И.Р., Бикеев И.И., 2020: 74]; [Кунев Д.А., 2018: 60–63]; [Сидоренко Э.Л., 2016: 8–10].

Использование криптовалюты является распространенным средством легализации денежных средств, приобретенных преступным путем. Квалификация транзакций с цифровыми финансовыми активами по ст. 174 и 174.1 УК РФ основывается на позиции, сформулированной в п. 1 постановления Пленума Верховного Суда Российской Федерации (далее — ВС РФ)

² Приговор Перовского районного суда Москвы от 17.06.2019 по делу № 01-0603/2019 // СПС «Консультант-Плюс».

³ Приговор Сормовского районного суда Нижнего Новгорода от 07.09.2018 по делу № 1-212/2018 // СПС «Консультант-Плюс».

от 07.07.2015 № 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». Пленум ВС РФ разъяснил, что исходя из положений ст. 1 Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма (2005) и с учетом Рекомендации 15 ФАТФ предметом преступлений, предусмотренных ст. 174 и 174.1 УК РФ, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления.

Так, Ш. был осужден за совершение преступлений, предусмотренных п. «а» ч. 3 ст. 228.1, ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1, п. «а» ч. 3 ст. 174.1, ч. 2 ст. 228 УК РФ. Согласно приговору суда, Ш. и неустановленные лица разработали план легализации денежных средств, полученных в результате совершаемых преступлений, — незаконного сбыта наркотических средств неопределенному кругу лиц. Согласно данному плану, Ш. получал денежные средства от неопределенного круга лиц в качестве оплаты приобретаемых наркотических средств на различные номера виртуальных счетов/кошельков системы электронных платежей «Киви». Ш. должен был на обменном сервисе «Локал Биткойнс» в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами систематически и ежедневно совершать сделки купли-продажи виртуальной валюты «Биткойн». После совершения сделки купли-продажи виртуальной валюты, Ш. должен был, используя известную ему учетную запись на обменном сервисе «Локал Биткойнс», переводить приобретенную виртуальную валюту на «Биткойн-кошелек» неустановленным лицам. В свою очередь, неустановленные лица должны были переводить полученную от Ш. виртуальную валюту «Биткойн» на «Биткойн-кошелек», связанный с иной, известной неустановленным лицам и Ш., учетной записью на обменном сервисе «Локал Биткойнс», доступ к ресурсам которой имелся у Ш. Получив от неустановленных лиц на указанный «Биткойн-кошелек» виртуальную валюту, Ш. должен был вновь совершать сделки по ее продаже на указанном обменном сервисе с неопределенным кругом лиц, получая от тех в качестве оплаты за продаваемую виртуальную валюту российские рубли. Впоследствии, снимая денежные средства с различных номеров виртуальных счетов/кошельков системы электронных платежей «Киви» и придавая при этом правомерный вид владению, пользованию и распоряжению указанными денежными средствами, Ш. распоряжался ими по своему усмотрению⁴.

⁴ Приговор Волжского городского суда от 06.03.2018 по делу № 1-277/2018 // СПС «Консультант-Плюс».

Как нетрудно заметить, совершение транзакций (как правило, не имеющих экономического смысла) с криптовалютой направлено к единственной цели — скрыть реальных выгодоприобретателей того или иного вида преступной деятельности, разорвать прямой финансовый след между ними. Известным свойство отдельных криптовалют (Monero, Black Coin и др.) — их полная анонимность при осуществлении расчетов, ввиду чего установить информацию об отправителе /получателе цифровых финансовых активов невозможно.

Следует, однако, указать, что такие транзакции с криптовалютой сами по себе не «отмывают» их происхождения. В конечном итоге виновный добивается лишь того, чтобы установить связь между капиталом, цифровыми финансовыми активами и конкретной преступной деятельностью было крайне затруднительно. Финансовый след теряется в цепочке сделок с цифровыми финансовыми активами, совершаемыми множеством участников на разных торговых площадках. Такое расширительное понимание легализации (признание таковой любых сделок с денежными средствами либо имуществом, добытыми преступным путем, в целях сокрытия их истинного происхождения) основано на рекомендациях ФАТФ и, пожалуй, является, целесообразным в современных условиях [Ализаде В.А., Волеводз А.Г., 2018: 5–13].

Обращаясь к обсуждаемой проблеме, М.И. Немова делает оговорку, что сама по себе конвертация криптовалюты в национальную или иностранную валюту не означает обязательной цели придания правомерного вида владению, пользованию и распоряжению преступным доходом, если конвертация была совершена в связи с необходимостью расходования полученного имущества на личные нужды. Автор делает акцент на том, что о наличии цели придания правомерного вида преступным доходам свидетельствуют дополнительные транзакции по переводу конвертированных денежных средств на электронные кошельки, дробление сумм, переводы на счета третьих лиц и т.п. [Немова М.И., 2019: 63–68].

Полагаем, что с мнением М.И. Немовой необходимо согласиться — использование криптовалюты не должно априорно свидетельствовать о том, что имела место легализация. При простом распоряжении виртуальной валютой, например, в целях оплаты товаров или услуг без намерения придания правомерного вида преступным доходам говорить о наличии признаков состава преступления, предусмотренного ст. 174.1 УК РФ, нельзя.

В первой группе преступлений следует также выделить посягательства на денежные средства граждан, которые хотя и совершаются без непосредственного использования виртуальной валюты, однако под предлогом совершения операций с нею (обмена, инвестирования и т.д.). В целом указанные деяния образуют признаки общеуголовного мошенничества (ст. 159 УК РФ). При подобных обстоятельствах злоумышленники используют низкую осведомленность граждан, делают упор на сверхдоходность криптовалютно-

го рынка, его свободу от государственного регулирования и налогообложения. Так, О., руководствуясь корыстными побуждениями, провела встречу с жителями города Бийска — партнерами компании «OneCoin». На данной встрече О. с целью введения присутствующих граждан в заблуждение, создавая видимость правомерности своих действий, сообщила заведомо ложные сведения о том, что она желает открыть общий «пул» (личный кабинет) на сайте «www.onelife.eu» компании «One Coin» на сумму 3 100 000 руб. для последующего приобретения криптовалюты по выгодной цене. В ходе данной встречи О. сообщила присутствующим, что для реализации данного бизнес-плана необходимо передать ей по 31 000 руб. (по 1/100 стоимости всего пула) для приобретения криптовалюты «One Coin». При этом О. пояснила, что принесенные с собой на встречу денежные средства необходимо передать непосредственно ей. После чего введенные в заблуждение потерпевшие, не догадываясь о преступных намерениях О., не предполагая обмана с ее стороны, поверив в достоверность слов последней, согласились на данное предложение О. Своими продолжаемыми преступными действиями О. путем обмана и злоупотребления доверием похитила 124 000 руб.⁵

Как мошенничество по ст. 159 УК РФ следует также квалифицировать случаи хищения денежных средств граждан под предлогом привлечения финансирования через ICO (Initial Coin Offering — форма привлечения инвестиций граждан в виде выпуска и продажи инвесторам новых криптовалют/токенов), когда субъекты реально не намеревались осуществлять подобного рода деятельность. Здесь можно привести известный пример из международного опыта. В октябре 2017 г. в газете «Ведомости» была опубликована статья о возбуждении в США уголовного преследования Максима Заславского, который предлагал инвесторам несуществующие токены и криптовалюту, обещая при этом солидные дивиденды от вложений⁶.

В теории уголовного права нет однозначного ответа на вопрос, следует ли квалифицировать как незаконное предпринимательство по ст. 171 УК РФ деятельность субъектов, которые занимаются обменными операциями с криптовалютой и извлекли при этом доход в крупном размере. Одним из главных аргументов против такой юридической оценки является неопределенный статус криптовалюты, который не позволяет говорить о том, что подобного рода деятельность могла быть зарегистрирована в принципе.

⁵ Постановление Бийского городского суда Алтайского края от 24.01.2018 по делу № 1-88/2018 в отношении О., обвиняемой в совершении преступления, предусмотренного ч. 2 ст. 159 УК РФ (дело прекращено по основаниям, предусмотренным ст. 76 УК РФ) // СПС «Консультант-Плюс».

⁶ В США возбудили первое в истории дело о мошенничестве при ICO. Available at: URL: <https://www.vedomosti.ru/technology/articles/2017/10/03/736241-ssha-delo-ico> (дата обращения: 04.06.2020)

В свою очередь, Ю.В. Трунцевский и А.Н. Сухаренко отстаивают позицию, согласно которой деятельность по обмену фиатных денег на криптовалюты на территории России соответствует всем признакам незаконного предпринимательства [Трунцевский Ю.В., Сухаренко А.Н., 2019: 45]. Подобный подход нашел отражение и в материалах правоприменительной практики. Так, Д.Е.А., Д.Е.Н. и Е. признаны виновными в совершении преступления, предусмотренного п. «а» ч. 2 ст. 171 УК РФ. Согласно приговору суда, в составе организованной группы как самостоятельно, так и с привлечением неосведомленных о преступном характере их деятельности иных лиц, без регистрации и без лицензии они осуществляли сопряженную с извлечением дохода в крупном размере (свыше 2,6 млн. руб.) предпринимательскую деятельность по оказанию посредством Интернета неопределенному кругу лиц возмездных (в размере не менее 0,5% от суммы поступивших денежных средств) услуг по переводу с использованием платежного сервиса «Visa QIWI Wallet» электронных денежных средств и купле-продаже «титულიных знаков» электронных платежных систем расчетов и бирж («Perfect Money», «WebMoney», «Payeer», «BTC-E»).

В апелляционной жалобе адвокат поставил вопрос об отмене приговора в связи с тем, что инкриминированная Д.Е.А. деятельность в принципе не могла быть зарегистрирована в качестве предпринимательской. Гражданское законодательство не содержит понятия криптовалюты. Имеющая существенное значение для квалификации содеянного сумма полученного Д.Е.А. дохода от деятельности обменных сервисов в ходе производства по делу не установлена. Результаты банковских экспертиз относительно суммы полученного дохода носят вероятностный (предположительный) характер, основанный на произвольном предположении следствия о взимании осужденными вознаграждения (теневой комиссии) в размере 0,5% от поступившей суммы.

Суд, не согласившись с доводами защиты, в решении указал, что деятельность по оказанию через сайты «Freshobmen.ru» и «Cashservise.com» услуг по переводу денежных средств и купле-продаже «титულიных знаков» являлась предпринимательской деятельностью, осуществляемой без регистрации. Доводы стороны защиты о том, что инкриминированная осужденным деятельность в принципе не могла быть зарегистрирована в качестве предпринимательской, были оценены судом как несостоятельные, поскольку деятельность «обменного сервиса» фактически сводилась к оказанию услуг по посредничеству в денежно-кредитной сфере, входящих в Общероссийский классификатор продукции по видам экономической деятельности⁷.

⁷ Апелляционное определение Костромского областного суда от 18.10.2018 г. по делу № 22-827/2018 // СПС «Консультант-Плюс».

Нельзя не отметить, что первоначально участникам данной преступной группы были предъявлены обвинения по ч. 2 ст. 172 УК РФ, однако в ходе производства по делу их действия переквалифицировали на ст. 171 УК РФ по той причине, что криптовалюта не считается официально признанным в России денежным средством, поэтому операции с ней не могут быть квалифицированы как банковские.

По мнению М.М. Долгиевой, в приведенном примере квалификация по ст. 171 УК РФ является вынужденной в свете отсутствия норм, которые бы предусматривали ответственность за такие действия. Автор также ссылается на то, что услуги по обмену криптовалюты на рубли не являются законными на территории России, соответственно, и регистрация в таком качестве или получение лицензии на оказание таких услуг невозможны по действующему законодательству [Долгиева М.М., 2019: 216].

Полагаем, что ответственность за незаконное предпринимательство в ситуации осуществления деятельности, связанной с обменом криптовалюты на фиатные денежные средства и наоборот, направленной на систематическое получения прибыли за счет взимания комиссии по каждой операции, все-таки возможна. Поскольку получение лицензии на оказание таких услуг невозможно по действующему законодательству, лицо будет нести ответственность за незаконное предпринимательство при условии, если оно осуществляло указанную деятельность без регистрации.

В отечественной науке уголовного права также обсуждается проблема использования криптовалюты для совершения преступлений, связанных с процедурой банкротства (ст. 195, 196, 197 УК РФ). Действительно, в силу известных свойств виртуальные валюты выступают весьма удобным средством для оперативного и надежного вывода активов хозяйствующего субъекта с целью последующего уклонения от исполнения обязательств перед контрагентами. Е.Г. Быкова и А.А. Казаков делают справедливый вывод, что, если вложение денежных средств гражданина в криптовалюту привело к возникновению признаков банкротства, не усматривается препятствий для юридической оценки содеянного по ст. 196 УК РФ при наличии к тому оснований [Быкова Е.Г., Казаков А.А., 2018: 14].

Полагаем, что при квалификации подобных действий традиционно основной проблемой будет выступать установление того обстоятельства, что лицо, совершая соответствующие транзакции, осознавало их заведомо убыточный характер и тем самым стремилось к банкротству. Вряд ли следует оспаривать, что в отдельных случаях поведение лица может быть обусловлено добросовестным стремлением к получению прибыли на волатильности курсов цифровых финансовых активов. В любом случае указанные обстоятельства должны оцениваться в обязательном порядке, в том числе с учетом мнения представителей экспертного сообщества. При этом, на наш взгляд,

непозволительным будет формирование на уровне правоприменения презумпции, согласно которой факт инвестирования в еще не получившие официальный статус криптовалюты является признаком совершения заведомо убыточных, ведущих к банкротству действий.

Проблемой совершенно другого порядка является квалификация действий руководителя организации, совершившего реализацию цифровых финансовых активов (в размере, эквивалентном 2 250 000 руб.) при наличии признаков банкротства. Применение ст. 195 УК РФ в подобной ситуации наталкивается на невозможность установление юридически значимой связи между криптовалютой и конкретным хозяйствующим субъектом. Как справедливо отмечают Е.Г. Быкова и А.А. Казаков, юридическое лицо не может владеть, пользоваться и распоряжаться криптовалютой ввиду отсутствия у последней законодательно закреплённого правового статуса [Быкова Е.Г., Казаков А.А., 2018: 14].

2. Преступления, в которых криптовалюта выступает предметом посягательства

В отечественной теории уголовного права нет однозначной точки зрения относительно вопроса о том, может ли криптовалюта выступать предметом хищения. М.А. Простосердов отстаивает позицию, что криптовалюта, как цифровой информационный продукт, т.е. совокупность уникальных компьютерных данных, объединённых в виртуальный носитель, обладающих всеми признаками товара, собственной стоимостью и принадлежащих на праве собственности другому лицу, может выступать предметом хищения в преступлениях, предусмотренных ст. 159, 159.6 и 160 УК РФ [Простосердов М.А., 2016: 18].

М.М. Долгиева также отмечает, что криптовалюта в силу специфических свойств, ценности и возможности являться предметом гражданского оборота должна быть отнесена к видам иного имущества в рамках ст. 128 Гражданского кодекса Российской Федерации (далее — ГК РФ) [Долгиева М.И., 2018: 45]. Эта позиция получает все большую поддержку в отечественной науке уголовного права. Ю.В. Грачева, С.В. Маликов и А.И. Чучаев напрямую указывают, что ст. 128 и 141.1 ГК РФ позволяют криптовалюту относить к имуществу и тем самым снимают проблему квалификации деяний, в которых она выступает предметом преступления [Грачева Ю.В., Маликов С.В., Чучаев А.И., 2020: 207]. В связи с этим нельзя не упомянуть, что в отечественной судебной практике уже создан прецедент, в рамках которого криптовалюта фактически признана иным имуществом.

В своем решении Девятый арбитражный апелляционный суд выразил позицию, что «согласно ст. 128 ГК РФ к объектам гражданских прав относят-

ся вещи, включая наличные деньги и документарные ценные бумаги, иное имущество, в том числе безналичные денежные средства, бездокументарные ценные бумаги, имущественные права; результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага. В силу диспозитивности норм гражданского права в ГК РФ отсутствует закрытый перечень объектов гражданских прав. Поскольку... действующее гражданское законодательство не содержит понятия «иное имущество», упомянутое в статье 128 ГК РФ, с учетом современных экономических реалий и уровня развития информационных технологий допустимо максимально широкое его толкование»⁸.

В свою очередь Э.Л. Сидоренко отмечает, что из-за отсутствия легальной дефиниции криптовалюты в российском законодательстве ее нельзя признать объектом гражданских прав и, следовательно, любые формы ее присвоения априори не могут быть признаны хищением, поскольку криптовалюта не обладает свойственными для предмета хищения определенными экономическими и материальными параметрами [Сидоренко Э.Л., 2017: 147].

Изучение судебно-следственной практики позволяет сделать вывод, что функционирование криптовалютных площадок, к сожалению, сопряжено с деятельностью лиц, которые, используя свои знания в области информационных технологий, осуществляют действия, направленные на изъятие цифровых финансовых активов пользователей. Одной из распространенных преступных схем является завладение криптовалютой пользователей под предлогом ее обмена на российские рубли или иную валюту. Так, суд согласился с квалификацией действий виновного по ч. 2 ст. 159 УК РФ, который из корыстных побуждений с целью хищения чужого имущества путем обмана и злоупотребления доверием под никнеймом «polu2218» на сайте «www.LocalBitcoins.com» вступил в переписку с потерпевшим, в ходе которой договорился о покупке у данного пользователя криптовалюты в размере 0.03875392 «BTC-e», заранее не намереваясь выполнять обязательства по ее оплате. В ходе переписки потерпевший оценил данную сделку на сумму 20 000 руб. Продолжая реализовывать преступный умысел, направленный на хищение чужого имущества путем обмана и злоупотребления доверием, не намереваясь выполнять обязательства по оплате криптовалюты, злоумышленник отправил потерпевшему смс-сообщение, полностью повторяющее по своему содержанию смс-сообщение от сервиса «Мобильный банк». Будучи введенным в заблуждение, полагая, что смс-сообщение получено от сервиса «Мобильный банк», потерпевший подумал, что виновный свои обязательства по

⁸ Постановление Девятого арбитражного апелляционного суда Москвы от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017 // СПС «Консультант-Плюс».

оплате криптовалюты исполнил и перевел на биткоин-кошелек под никнеймом «polya2218» на сайте «www.LocalBitcoins.com» криптовалюту на сумму 0,03875392 «BTC-e» стоимостью 20 000 руб.⁹

Следует отметить, что такие действия довольно часто сопряжены с неправомерным доступом к охраняемой законом компьютерной информации, а именно — к личным кабинетам других пользователей. Так, например, Ш. и О. были осуждены по ч. 3 ст. 159 и ч. 3 ст. 272 УК РФ. Согласно приговору суда, указанные лица вступили в предварительный сговор с целью хищения чужого имущества («BTC-e» кодов) посредством сети «Интернет» путем незаконного получения доступа к учетным записям пользователей и под предлогом обмена «BTC-e» кодов. Продолжая совместные преступные действия, Ш. и О. осуществили неправомерный доступ к учетным записям пользователей «wmalliance» и «Djin37», после чего изменили их учетную информацию, добавив свой уникальный идентификационный номер для общения в реальном времени, а также от имени пользователей «wmalliance» и «Djin37» создали тему «Выход BTC-e / Биткоинов. +7%» и положительные комментарии к ней от имени других неустановленных пользователей сайта.

После этого Ш. и О., имея умысел на хищение у ранее незнакомого лица, использующего программу «ICQ» и имя «Gambit», ввели его в заблуждение, пообещав ему обменять «BTC-e» код на российские рубли, чего заведомо не намеревались делать. Потерпевший, будучи введенным в заблуждение относительно преступных намерений Ш. и О., используя свою учетную запись «ser198», с целью обмена принадлежащего ему «BTC-e» кода на 10 000 долл. США на российские рубли в личном сообщении передал пользователю «wmalliance» (доступ к которому имели Ш. и О.) «BTC-e» код на 10 000 долл. США. Рыночная стоимость кода по состоянию на дату отправки сообщения, согласно заключению эксперта, составляла 821 100 руб. Далее Ш. и О. зачислили полученный BTC-e код, принадлежащий потерпевшему, на счет своей учетной записи, тем самым похитили его и в дальнейшем распорядились им по своему усмотрению¹⁰.

Тайное хищение цифровых финансовых активов, как правило, сопряжено с неправомерным доступом к личному кабинету клиента торговой площадки. Пытаясь получить неправомерный доступ к аккаунту клиента, злоумышленники предварительно взламывают электронную почту потерпевшего. Нельзя не отметить, что в правоприменительной практике такие действия довольно часто получают неполную квалификацию. Следственные органы, возбуждая уголовные дела по ст. 158 УК РФ, оставляют без внимания, что на

⁹ Приговор Октябрьского районного суда Тамбова от 15.02.2019 по делу № 1-134/19 // СПС «Консультант-Плюс».

¹⁰ Приговор Сургутского городского суда Ханты-Мансийского автономного округа от 13.11.2017 г. по делу № 1-762/2017 // СПС «Консультант-Плюс».

стадии приготовления к совершению хищения злоумышленник совершил самостоятельное преступление, предусмотренное ч. 2 ст. 272 УК РФ.

Посягательства на цифровые финансовые активы могут носить и открытый характер. В зависимости от фактических обстоятельств содеянного (прежде всего характера насилия к потерпевшему) противоправное изъятие криптовалюты может быть квалифицировано как грабеж или разбой.

Требования о передаче цифровых финансовых активов, соединенные с угрозой применения насилия к потерпевшему, уничтожения или повреждения его имущества, а равно под угрозой распространения сведений, порочащих потерпевшего или его близких, образуют признаки вымогательства.

Правоприменительные органы в качестве системной проблемы, возникающей при расследовании подобной категории дел, отмечают отсутствие на территории России органа, уполномоченного дать оценку стоимости криптовалюты на конкретную дату. В настоящее время при расследовании уголовных дел установление размера причиненного ущерба потерпевшему основывается либо на заключении специалиста, либо посредством получения информации о курсе криптовалюты на время совершения преступления непосредственно через данные торговой площадки (криптобиржи).

3. Преступления, совершаемые в целях генезиса (майнинга) криптовалюты

Последнюю группу составляют преступные посягательства, которые совершаются в целях генерации (майнинга) криптовалюты. Анализ современной правоприменительной практики показывает, что к таковым относятся все посягательства, ответственность за которые предусмотрена главой 28 УК РФ «Преступления в сфере компьютерной информации». Прежде всего, следует выделить неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ). Так, Б. признан виновным в неправомерном доступе к охраняемой законом компьютерной информации, содержащейся в административной части сайта «regionorel.ru» ГУП ОО «Орловский издательский дом». Незаконный доступ повлек ее модификацию путем внедрения кода скрипта с индивидуальным ключом для получения криптовалюты «Monero» в личное пользование, а также уничтожение компьютерной информации, содержащей сведения обо всех посещениях сайта пользователями и изменениях компьютерной информации сайта (журналы истории посещений и истории команд) объемом 45 Гб, совершенных из корыстной заинтересованности.

Согласно решению суда, Б. состоял в трудовых отношениях с указанным ГУП ОО в должности ведущего специалиста и разработал сайт, который к 2012 г. обрел свой вид и был размещен на домене «epressa.su» на сервере, расположенном в редакции газеты «Орловская правда». В 2014 г. редакция при-

няла решение о переименовании сайта и смены доменного имени, и вместо «epressa.su» был приобретен домен «regionorel.ru». В июне 2015 г. Б. уволился, после чего никакого отношения к сайту «regionorel.ru» не имел.

Прекратив трудовые отношения с «Орловским издательским домом» с 17.06.2015, перестав иметь законные основания на доступ к серверу и к административной части сайта «regionorel.ru», Б. со своего рабочего компьютера осуществил неправомерный доступ к информации, содержащейся на административной части сайта «regionorel.ru», владельцем которого является «Орловский издательский дом», путем создания новой учетной записи с правами администратора на любые изменения, регистрации нового пользователя сайта и введения кода скрипта с индивидуальным ключом для получения криптовалюты «Монего» в личное пользование.

Сторона защиты, не согласившись с решением суда первой инстанции в апелляции указывала, что файлы, в которые вносились изменения, являлись общедоступными, автором сайта «regionorel.ru» является Б., а «Орловскому издательскому дому» принадлежит только адрес. Сторона защиты не согласилась также с вменением квалифицирующего признака «корыстная заинтересованность», поскольку доказательства возможности получения денежных средств из криптовалюты, их ценность и возможность конвертации обвинением не были предъявлены.

Хотя контент сайта не был приведен в непригодное состояние, суд апелляционной инстанции также признал, что это само по себе не влияет на квалификацию действий осужденного, поскольку приведенными доказательствами достоверно установлено, что скрипт, внедренный Б. в тело файлов «header.php» и «footer.php», модифицировал сайт «regionorel.ru» в целях получения криптовалюты «Монего» в его личное пользование путем использования вычислительных ресурсов неограниченного круга посетителей пользовательской части сайта «regionorel.ru».

Наличие в действиях Б. квалифицирующего признака «корыстная заинтересованность» суд счел установленным, сославшись на то, что в личном кабинете Б. на сайте «Coinhive» имеется информация о том, что сайт, используемый для майнинга — это «regionorel.ru», а сумма «монет», заработанная за весь период, составила 0,03225 XMR. Доводы защиты о необходимости доказательств получения денежных средств из криптовалюты суд посчитал необоснованными, поскольку «сведения о криптовалютах как о платежных средствах в Интернете, являются общеизвестными и общедоступными, содержащимися в Интернете, где также приводятся и их списки, и курс¹¹.

Использование вредоносных компьютерных программ (ст. 273 УК РФ), как правило, осуществляется лицами для обеспечения неправомерного до-

¹¹ Апелляционное постановление Орловского областного суда от 23.08.2019 по делу № 22-1120/2019 // СПС «Консультант-Плюс».

ступа к вычислительным ресурсам потерпевших и последующего майнинга криптовалюты.

Так, согласно приговору суда, у Ш. возник преступный умысел, направленный на использование из корыстных побуждений аппаратной мощности серверов различных организаций, расположенных на территории России, для генерации криптовалюты (майнинга) путем установки на него своего программного обеспечения и получения таким способом денежных средств. В период с 28.11.2017 по 9.01.2018 Ш., получив с помощью компьютерной программы IP-адрес сервера с открытым портом, принадлежащего местной муниципальной организации, Ш. с целью реализации своего преступного умысла, находясь по месту своего жительства, умышленно, из корыстной заинтересованности ввел IP-адрес организации во вредоносную компьютерную программу и с помощью своего персонального компьютера, подключенного к Интернету, запустил ее, тем самым предприняв попытку получить удаленный доступ к интернет-ресурсам организации, размещенным на сервере. Через некоторое время вредоносная компьютерная программа подобрала логин и пароль к серверу организации. После этого Ш. с помощью незаконно полученных логина и пароля осуществил доступ к серверу и установил на нем свое программное обеспечение (не являющееся вредоносным) для генерации криптовалюты (процесса майнинга)¹².

В приведенном примере квалификация содеянного только по ст. 273 УК РФ, на наш взгляд, является неверной. Исходя из фабулы дела, виновный не только подобрал сетевые идентификаторы к серверу, но и установил программное обеспечение для майнинга криптовалюты, что позволяет утверждать о модификации компьютерной информации. Таким образом, полная юридическая оценка содеянного должна была также включать квалификацию самого неправомерного доступа к серверу с последующей модификацией информации по ст. 272 УК РФ.

По ст. 274 УК РФ как преступное нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей следует оценивать действия работников организации, использовавших ее вычислительные мощности для вычисления (майнинга) криптовалюты. Подобный подход нашел отражение и в правоприменительной практике. Так, Б. был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 274 УК РФ. Согласно приговору суда, Б., заведомо зная о действующих в ФГУП «РФЯЦ-ВНИИЭФ» запретах на подключение служебной вычислительной сети к Интернету, а также на использование на автоматизированных рабочих местах программ-

¹² Приговор Курганского городского суда Курганской области от 29.11.2018 по делу № 1-1186/18 // СПС «Консультант-Плюс».

ного обеспечения, не разрешенного к применению соответствующей комиссией Института, умышленно, из корыстной заинтересованности, под непосредственным контролем со стороны других соучастников путем соединения предоставленных вычислительных систем (серверов) осуществил сборку вычислителя, необходимого для майнинга криптовалюты. Для соединения собранного вычислителя с Интернетом Б. подключил к нему GSM-модем, после чего, по согласованию с другими соучастниками и под их контролем, загрузил из Интернета программное обеспечение, предназначенное для майнинга криптовалюты, а также программное обеспечение «eth-proxy», предназначенное для получения через Интернет задач на вычисление (майнинг) криптовалюты, сбора результатов вычислений и их отправки в Интернет на «Pool» (сервер, который связан со всеми участниками майнинга криптовалют). После этого Б., находясь в здании Института, в течение нескольких недель преимущественно в ночное время запускал процесс майнинга криптовалют.

Указанные действия Б. привели к нарушению условий действия аттестата соответствия на объект информатизации. Это, в свою очередь, обусловило необходимость внеочередной повторной аттестации служебной локальной вычислительной сети научно-исследовательского института, стоимость которой составила 1 140 157 руб. 10 коп. Таким образом, нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации, совершенное Б., повлекло причинение ФГУП «РФЯЦ-ВНИИЭФ» крупного материального ущерба, составляющего 1 140 157 руб. 10 коп.¹³

Важно отметить, что если действия, связанные с майнингом криптовалюты, были сопряжены с нарушением правил доступа и (или) эксплуатации категоризированных информационных ресурсов (в соответствии с Федеральным законом от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»), содеянное необходимо квалифицировать по ч. 3 ст. 274.1 УК РФ.

Заключение

В современном мире криптовалюта приобретает все более широкое распространение. Судя по всему, это необратимый процесс. Привлекательность и, как следствие, нарастающая популярность данного финансового инструмента XXI века легко объяснима — криптовалюты удобны в использовании, транзакции очень хорошо защищены, а сведения о них обеспечены высоким уровнем анонимности, прежде всего, с точки зрения контроля со стороны государства. Последний аспект, однако, бросает весьма негативную тень на

¹³ Приговор Саровского городского суда Нижегородской области от 17.09.2019 по делу № 1-149/2019 // СПС «Консультант-Плюс».

криптовалюты. Складывается представление (и небезосновательное), что этот финансовый инструмент есть всего лишь свидетельство кризиса мировой финансовой системы, кризиса доверия между государством и обществом, и подтверждение нарастающего влияния криминала на современную экономику.

Для правоохранительных органов криптовалюты ознаменовали принципиально новый этап в борьбе с преступностью. С одной стороны, криптовалюты стали активно использоваться в гражданском обороте законопослушными гражданами и хозяйствующими субъектами, в том числе как инструмент хранения капитала, что поставило задачу их надлежащей правовой защиты. С другой — децентрализованный характер и анонимность криптовалют изменили механизм совершения многих традиционных преступлений, раскрытие и расследование которых стало чрезвычайно трудно разрешимой задачей.

Уже сейчас можно констатировать, что правоохранительные органы смогли преодолеть многие из трудностей противодействия криптовалютной преступности. Нарбатываются новые методики и тактики, во взаимодействии практических органов и научный коллективов подготовлены рекомендации. Вместе с тем вряд ли можно с полной уверенностью утверждать, что проблем не осталось вовсе.

Развитие и внедрение блокчейн-технологий связаны с высоким уровнем неопределенности. Равным образом этот вывод можно распространить на будущее виртуальных валют. Это означает, что мы не имеем четкого понимания, как будет трансформироваться новая (криптовалютная) преступность. Однако трудность процесса цифровизации уголовно-правовой сферы предполагает повышенную ответственность научного сообщества, которое должно обеспечить надлежащий уровень осмысления формирующихся тенденций. Предпринятая в настоящей статье попытка обобщить и проанализировать особенности правоприменения в части квалификации вышерассмотренных преступлений, конечно, не претендует на абсолютность, носит субъективно-несовершенный, а, значит, и незавершенный характер. Вместе с тем не вызывает сомнений, что совместные усилия экспертного сообщества в сфере высоких технологий и юристов в ближайшей перспективе внесут определенность в понимание правового статуса криптовалюты, следовательно, и правовой оценки действий, совершаемых с нею.



Библиография

Ализаде В.А., Волеводз А.Г. Неприменение ст. 174.1 УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов // Наркоконтроль. 2018. N 1. С. 5–13.

- Бегишев И.Р., Бикеев И.И. Преступления в сфере обращения цифровой информации. Казань: Познание, 2020. 300 с.
- Быкова Е.Г., Казаков А.А. Проблемы квалификации криминальных банкротств с использованием криптовалюты // Уголовное право. 2018. N 6. С. 10–15.
- Грачева Ю.В., Маликов С.В., Чучаев А.И. Предупреждение девиаций в цифровом мире уголовно-правовыми средствами // Право. Журнал Высшей школы экономики. 2020. N 1. С. 188–210.
- Долгиева М.М. Противодействие легализации преступных доходов при использовании криптовалюты // Вестник Томского государственного университета. 2019. N 4. С. 213–218.
- Долгиева М.М. Конфискация криптовалюты // Законность. 2018. N 11. С. 45–49.
- Кунев Д.А. Современные угрозы использования криптовалют в преступных целях // Финансовая безопасность. 2018. N 20. С. 60–63.
- Ляскало А.Н. Криптовалюта как предмет и средство преступления / Уголовное право: стратегия развития в XXI веке: материалы XVI Международной конференции. М.: РГ-Пресс, 2019. С. 87–92.
- Немова М.И. Уголовный закон и криптовалюта: вызовы и перспективы / Уголовное право: стратегия развития в XXI веке: материалы XV Международной конференции. С. 585–587.
- Немова М.И. Использование криптовалюты при легализации (отмывании) денежных средств или иного имущества: приобретенных преступным путем: анализ судебной практики // Уголовное право. 2019. N 4. С. 63–68.
- Пинкевич Т.В. Проблемы уголовно-правового противодействия преступной деятельности с использованием криптовалют // Юрист-Правоведъ. 2020. № 4. С. 45–48.
- Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: Автореф. дис. ...к. ю. н. М., 2016. 28 с.
- Сидоренко Э.Л. Криминальное использование криптовалюты: международные оценки // Международное уголовное правосудие и международная юстиция. 2016. N 6. С. 8–10;
- Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. N 6. С. 147–154.
- Трунцевский Ю.В., Сухаренко А.Н. Противодействие использованию криптовалюты в незаконных целях: состояние и перспективы // Международное публичное и частное право. 2019. N 1. С. 43–47.

Pravo. Zhurnal Vysshey Shkoly Ekonomiki. 2021. No 3

Crimes Related to Cryptocurrencies: Features of Qualification



Evgeny Russkevich

Associate Professor, Department of criminal law, Moscow University of the Ministry of Internal Affairs, Candidate of Juridical Sciences. Address: 12 Academic Volgin St., Moscow 117997, Russian Federation. E-mail: russkevich@mail.ru



Ivan Malygin

Consultant, Department of regulatory acts registration in the social and cultural spheres, Ministry of Justice. Address: 14 Zhitnaya St., Moscow 119991, Russian Federation. E-mail: aspugpravo@yandex.ru



Abstract

Process of penetration of digital financial assets into the daily lives of citizens and the activities of business entities, as well as the steady increase in crimes committed using, with respect to and about cryptocurrencies, actualizes the need for a scientific understanding of the features and problems of their qualifications. The purpose of the study is to develop theoretical recommendations to overcome the problems that arise in connection with the qualification of crimes committed using, in relation to and about cryptocurrencies. The implementation of this goal was achieved by examining the existing positions on the problem in the domestic doctrine of criminal law, assessing the state of domestic criminal legislation, identifying problems in judicial investigative practice. The study is based on the application of general and special methods of research (analysis, synthesis, induction, formal legal, abstract logical, etc.). Based on the study, the author formulates the following conclusions: in modern conditions the following main groups of crimes associated with the use of digital financial assets (cryptocurrencies) in one form or another can be distinguished: a) crimes in which cryptocurrency acts as a means of committing them; crimes in which cryptocurrency acts as an object of encroachment; crimes committed for the purpose of generating (mining) cryptocurrency; the use by a person of cryptocurrency cannot a priori indicate that legalization has taken place. A simple disposal of virtual currency (in order to pay for goods or services) without the intention of giving a legitimate form to criminal proceeds does not contain signs of corpus delicti provided for in Art. 174.1 of the Criminal Code; as an illegal business (Article 171 of the Criminal Code of the Russian Federation), one should qualify a person to carry out activities related to the exchange of cryptocurrency for fiat money and vice versa, aimed at making profit by charging a commission for each operation. Considering that obtaining a license to provide such services is not possible under applicable law, a person will be liable for illegal business, provided that he carried out the specified activity without registration; when qualifying encroachments on cryptocurrency, law enforcement authorities as a systemic problem note the absence in the territory of Russia of a body authorized to assess its value on a specific date. Currently, in the investigation of criminal cases, the determination of the amount of damage caused to the victim is based either on the expert's opinion or by obtaining information about the cryptocurrency rate at the time the crime was committed.



Keywords

criminal law; cryptocurrency; crimes; digital financial assets; computer information; information security.

For citation: Ruskevich E.A., Malygin I.I. (2021) Crimes Related to Cryptocurrencies: Features of Qualification. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 3, pp. 106–125 (in Russian)

DOI: 10.17323/2072-8166.2021.3.106.125



References

Alizade V.A., Volevodz A.G. (2018) Non-application of Art. 174.1 of the Criminal Code of the Russian Federation on drug-related crimes committed using cryptocurrency. *Nar-kokontrol'*, no 1, pp. 5–13 (in Russian)

- Begishev I.R., Bikeev I.I. (2020) *The crimes in the digital information field*. Kazan: Posnaniye publishers, 300 p. (in Russian)
- Bykova E.G., Kazakov A.A. (2018) Qualification problems of criminal bankruptcies using cryptocurrency. *Ugolovnoe pravo*, no 6, pp. 10–15 (in Russian)
- Dolgieva M.M. (2019) Countering the legalization of criminal proceeds when using cryptocurrency. *Vestnik Tomskogo universiteta*, no 4, pp. 213–218 (in Russian)
- Dolgieva M.M. (2018) Confiscation of cryptocurrency. *Zakonnost'*, no 11, pp. 45–49 (in Russian)
- Gracheva Y.V., Malikov S.V., Chuchaev A.I. (2020) Prevention Deviations in the Digital World by Criminal Law Means. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 1, pp. 188–210 (in Russian)
- Kunev D.A. (2018) Modern threats of using cryptocurrencies for criminal purposes. *Finansovaya bezopasnost'*, no 20, pp. 60–63 (in Russian)
- Lyaskalo A.N. (2019) Cryptocurrency as an object and means of crime. *Ugolovnoe pravo: strategiya razvitiya v XXI veke: materialy Mezhdunarodnoj konferencii*. Moscow: RG-Press, pp. 87–92 (in Russian)
- Nemova M.I. (2018) Criminal law and cryptocurrency: challenges and prospects. *Ugolovnoe pravo: strategiya razvitiya v XXI veke: materialy Mezhdunarodnoj konferencii*. Moskva: RG-Press, pp. 585–587 (in Russian)
- Nemova M.I. (2019) The use of cryptocurrency in the legalization (laundering) of money or other property: acquired by criminal means: analysis of judicial practice. *Ugolovnoe pravo*, no 4, pp. 63–68 (in Russian)
- Pinkevich T.V. (2020) On legal counteraction to cryptocurrencies criminality. *Jurist-pravoved*, no 4, pp. 45–48 (in Russian)
- Prostoserodov M.A. (2016) Economic crimes committed in cyberspace and countermeasures against them. Candidate of Juridical Sciences Summary. Moscow, 28 p. (in Russian)
- Sidorenko E.L. (2016) The criminal use of cryptocurrencies: international assessments. *Mezhdunarodnoe ugolovnoe pravosudie i mezhdunarodnaya justitsiya*, no 6, pp. 8–10 (in Russian)
- Sidorenko E.L. (2017) Criminological risks of cryptocurrency turnover. *Ekonomika. Na-logi. Pravo*, no 6, pp. 147–154 (in Russian)
- Truncevskij Yu.V., Suharenko A.N. (2019) Countering the use of cryptocurrency for illegal purposes: state and prospects. *Mezhdunarodnoe publichnoe i chastnoe pravo*, no 1, pp. 43–47 (in Russian)