МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
КАЗАНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ

Д.В. Кузнецов

УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ВОПРОСЫ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ И ДРУГИХ ВИРТУАЛЬНЫХ АКТИВОВ

Учебное пособие

Казань
КЮИ МВД России
2022

ББК 67.410.2
К89

Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты
Кандидат юридических наук, доцент **Д.Н. Рудов**
(Белгородский юридический институт МВД России им. И.Д. Путилина)
О.А. Смирнова
(Главное следственное управление МВД по Республике Татарстан)

Кузнецов Д.В.
К89 Уголовно-процессуальные и организационно-тактические вопросы выявления и расследования преступлений, связанных с использованием криптовалют и других виртуальных активов: учебное пособие / Д.В. Кузнецов. – Казань: Казанский юридический институт МВД России, 2022. – 76 с.
ISBN 978-5-6048743-1-8

Учебное пособие направлено на формирование у обучающихся теоретических знаний и практических навыков расследования уголовных дел о преступлениях, совершенных с использованием криптовалют. В пособии представлены алгоритмы действий для правоохранительных органов по взаимодействию с криптовалютными биржами и реализации мер пресечения в отношении держателей криптовалюты.

Предназначено для преподавателей, курсантов и слушателей образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

ISBN 978-5-6048743-1-8 **ББК 67.410.2**

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Современное развитие преступности тесно связано с сокрытием полученных в ходе незаконной деятельности доходов. Много лет в России существовали и продолжают существовать целые сети организаций, осуществлявших обналичивание денежных средств, полученных преступным путем. В то же время доступ к ним был не у всех преступников, и нередко денежные средства они хранили в тайниках в наличной форме либо переводили их в драгоценные металлы. С появлением криптовалюты сокрытие преступных доходов стало общедоступным. Изначально при появлении криптовалютных бирж преступные элементы относились к ним несколько настороженно. Это было вызвано, в том числе, колебанием курса криптовалют, но в дальнейшем все больше денежных средств, полученных в результате совершения преступлений, переводилось в криптовалютную форму. Указанное стало актуальным для преступников не только из-за высокого уровня анонимности транзакций, но и в связи с появлением большого количества отечественных компаний, осуществляющих быстрые переводы денежных средств на криптовалютные счета. Наибольшую популярность криптовалюта обрела у наркоторговцев. Судебная практика дает основание утверждать, что большая часть подобных преступлений в настоящее время совершается с использованием различных криптовалют[1]. Противодействие указанному процессу в настоящее время ведется всеми правоохранительными органами России, однако возникает немалое количество вопросов, связанных с тем, каким образом проводить следственные и иные процессуальные действия в отношении держателей криптовалют.

В рассматриваемом пособии проводится анализ сложившейся ситуации с криптовалютой в рамках ее существования у лиц, привлекаемых к уголовной ответственности в России. Отдельно представляются способы организации взаимодействия с наиболее крупными и в том числе популярными в России криптовалютными биржами. Также рассматриваются способы реализации мер процессуального принуждения в отношении держателей криптовалют в уголовном процессе. Кроме того, для более глубокого изучения в пособии в качестве задач представлены типичные ситуации, которые могут возникать у сотрудников правоохранительных органов при расследовании преступлений с использованием криптовалют.

[1] Криптовалюты: тренды, риски, меры. Доклад для общественных консультаций. Центральный банк Российской Федерации, Москва, 2022.

ГЛАВА 1.
ПРАВОВОЕ РЕГУЛИРОВАНИЕ КРИПТОВАЛЮТ В КОНТЕКСТЕ ИХ СУЩЕСТВОВАНИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Первые шаги на пути нормативного закрепления понятия виртуальной валюты и порядка оборота цифровых активов были осуществлены законодателем 1 октября 2019 года, когда цифровые права были официально отнесены к объектам гражданских прав. Соответствующие изменения внесены в ст. 128 Гражданского кодекса РФ (ГК РФ)[1] Федеральным законом № 34-ФЗ от 18 марта 2019 года.

Правоприменительная практика сформировала подход, при котором криптовалюта получила статус иного имущества применительно к ст. 128 ГК РФ ввиду открытого перечня объектов гражданских прав. Цифровые активы по факту признали «законным имуществом» для целей налогообложения и учета при расчетах с кредиторами в процедурах банкротства. Разъяснения по вопросу отражения доходов российских организаций от операций с криптовалютой даны в письме Министерства финансов Российской Федерации от 09.02.2018 № 03-03-06/1/8061[2]. Судами биткоин признавался ликвидным имуществом, за счет которого могут быть удовлетворены права кредиторов (постановление 9-го ААС от 15.05.2018 по делу № А40-124668/2017[3], постановление 9-го ААС от 18.04.2019 по делу № А40-12639/2016[4] и т. д.). И если в указанных судебных актах признается возможность включения криптовалюты в конкурсную массу и истребования у владельцев, то фактически суд признает право лица «по своему усмотрению владеть, пользоваться, распоряжаться содержимым криптокошелька как своим собственным имуществом, совершать в отношении него лю-

---

[1] Гражданский кодекс Российской Федерации. Ч. 1. Ст. 128. URL: https://base.garant.ru/10164072/089c3288c5448786f472572a85a4941a/ (дата обращения: 10.01.2022).

[2] Письмо от 09.02.2018 № 03-03-06/1/8061. URL: https://www.v2b.ru/documents/pismo-minfina-rf-ot-09-02-2018-03-03-06-1-8061/ (дата обращения: 10.01.2022).

[3] Российский суд впервые признал криптовалюту имуществом // Clifford Chance, М.: 2018., С. 1 – 3.

[4] Криптовалюта как предмет преступления: проблемы квалификации и защиты// Право.ru URL: https://pravo.ru/opinion/215852 (дата обращения: 10.01.2022)

бые действия, не противоречащие закону и иным правовым актам и не нарушающие права и охраняемые законом интересы других лиц». То есть осуществлять полномочия, близкие к полномочиям собственника, предусмотренные ч. 2 ст. 35 Конституции РФ[1] и ст. 209 ГК РФ[2].

С другой стороны, когда речь идет о свободном распоряжении и сделках с цифровыми активами, их статус определяется как нелегальный, поскольку финансовая система страны является объектом правовой охраны публичного права, неурегулированное правовое положение криптовалюты позволяет Центробанку, прокуратуре и следственным органам квалифицировать ее как денежный суррогат. В связи с этим любым операциям по обращению и действиям по распространению информации о криптовалюте может быть дана уголовно-правовая квалификация, а владельцы цифровых активов нуждаются в уголовно-правовой защите собственности.

Сама по себе уголовно-правовая квалификация деятельности криптовалютных площадок без установления в действиях отдельно взятых лиц признаков конкретного состава преступления, во-первых, незаконна, во-вторых, произвольным образом направлена на ограничение прав их пользователей, в-третьих, противоречит фактическому принятию и закреплению в обороте цифровых активов. Эти факторы затрудняют работу следственных органов по квалификации преступлений, связанных с использованием криптовалютой.

В современных научных исследованиях виртуальная валюта рассматривается преимущественно в рамках исследования объектов гражданских прав. Однако, несмотря на разнообразие и широту предлагаемых позиций, ни ученым, ни практикам не удалось достигнуть единого понимания того, к какому объекту гражданских правоотношений относится криптовалюта, и допустимо ли рассматривать ее как предмет гражданских правоотношений. Одни авторы настаивают на признании криптовалюты вещью, другие видят в ней имущественные права, третьи придают ей статус иного имущества. Считая излишним детальный анализ существующих

---

[1] Конституция Российской Федерации. Ст.35. URL: http://www.consultant.ru/document/cons_doc_LAW_28399/2b3cdfcf41099657639e96a77b00849cacec38ca/ (дата обращения: 10.01.2022)

[2] Гражданский кодекс Российской Федерации. Ст. 209. URL: http://www.consultant.ru/document/cons_doc_LAW_5142/9bc79ae09d078798e7a4ee4647ac9ea495da9fa0/ (дата обращения: 31.01.2022)

позиций, обратимся к оценке сущностных признаков объектов гражданских прав.

Согласно ст. 128 ГК РФ к объектам гражданских прав относятся 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[1]. В настоящий момент судебная практика выработала ряд устойчивых признаков предмета гражданских правоотношений. Обозначим основной из них:

• отсутствие четкой зависимости между физическими и правовыми свойствами вещи. Одинаковым статусом могут обладать как предметы, имеющие индивидуально-определенные физические параметры, так и объекты со специфическими формами визуализации. Вещные права на них возникают не из-за их физических свойств, а в силу потребностей общества в их регулировании (например, энергия, газ, микроорганизмы, органы и ткани человека и др.). Как справедливо отмечает С.А. Синицын, «признанное законодательством качество и свойство вещи как объекта гражданских прав предопределены совокупностью факторов: потребностями гражданского оборота, физическими свойствами самой вещи, законодательной регламентацией и причислением отдельных объектов к видам вещей (пусть и особого рода). Именно потребности оборота являются фактором вынужденного распространения на объекты гражданских прав, не являющихся по своей сути вещами, правового режима вещи, включая и правовые последствия ее оборота»[2].

Наличие режима ограниченности гражданского оборота дало исследователям повод рассматривать криптовалюту как об объект гражданских прав, ограниченный в обороте[3]. Однако с этой позицией сложно согласиться на том основании, что ограниченность оборота того или иного имущества должна быть закреплена в законе. В постановлении Второго арбитражного апелляционного

---

[1] Гражданский кодекс Российской Федерации. Ст. 128. URL: https://base.garant.ru/10164072/089c3288c5448786f472572a85a4941a/ (дата обращения: 01.03.2022).

[2] Синицын С.А. Вещь как объект гражданских прав: возможные и должные критерии идентификации // Законодательство и экономика. 2016. № 11. С. 7 – 17.

[3] Воронцова А.А. Гражданский оборот. Доступ из СПС «КонсультантПлюс» (дата обращения: 01.03.2022).

суда от 26.11.2012 по делу № А28–9032/2011[1] «виды объектов гражданских прав, которые могут принадлежать лишь определенным участникам оборота либо нахождение которых в обороте допускается по специальному разрешению (объекты, ограниченно оборотоспособные), определяются в порядке, установленном законом». По мнению суда, это означает, что в законе должны предусматриваться исходные критерии отнесения объектов к ограниченно оборотоспособным и указываться государственные органы, уполномоченные определять конкретные их виды: шифровальная техника, радиоактивные вещества, яды и наркотические средства и т.д. В отличие от предметов с особым режимом оборота криптовалюта не закреплена в законе в качестве объекта гражданских прав, а значит, не обладает оборотоспособностью. В этом смысле она приближена к объектам, изъятым из оборота, поскольку не может быть оценена в денежной сумме. Согласно постановлению ФАС Поволжского округа от 24.05.2010 по делу № А57–5480/2009 «изъятые из оборота вещи не могут каким-либо образом отчуждаться или переходить от одного лица к другому, а следовательно, такие вещи не могут иметь и товарную (денежную) стоимость, определяемую потребительскими свойствами товара»[2].

Нелегко признать криптовалюту и вещным правом на том основании, что в данном случае отсутствует возможность непосредственного воздействия на вещь. Трактовка закрепленного в ст. 128 ГК РФ понятия «иное имущество» в отсутствие его легальной дефиниции, позволяющая некоторым специалистам неоправданно расширять его границы. В частности, на наш взгляд, нельзя согласиться с А.И. Савельевым в том, что квалификацию криптовалюты в качестве иного имущества допустимо сравнить с квалификацией непоименованного договора: она позволяет легитимировать договор. Автор, однако, оставляет без внимания одно весьма существенное свойство иного имущества – оно имеет особый режим оборота, прописанный в отдельных нормативных актах (например, электронная энергия, радиочастотный спектр и др.). Если же такой режим отсутствует, объект не может быть признан иным имуществом. В связи с этим весьма показательным является постановление

[1] Обзор судебной практики Верховного Суда Российской Федерации № 2 (2016), утвержденного Президиумом Верховного Суда 06.07 Российской Федерации // Журнал руководителя и главного бухгалтера ЖКХ. 2017. № 1.

[2] Сидоренко Э.Л. Правовой статус криптовалют в Российской Федерации // Экономика. Налоги. Право. 2018. № 2. С.131

ФАС Северо-Западного округа от 09.11.2007 № А56–50410/2005: «Отказывая в удовлетворении иска о признании права собственности на футбольное поле с газонным покрытием и предохранительную зону, суд пришел к выводу, что указанные объекты в отсутствии их особого режима оборота не могут быть самостоятельными объектами права и являются принадлежностью соответствующего земельного участка»[1].

На основании вышеизложенного необходимо признать, что предметами гражданских правоотношений считаются объекты, если они отвечают следующим признакам:

1) полная либо частичная регламентация их имущественных свойств на нормативном уровне;

2) оборотоспособность или способность участвовать в легальном гражданском обороте;

3) наличие общего или специального правового режима, который предусматривает регламентацию прав субъектов правоотношений, механизмы их регулирования и защиты.

Преломляя эти признаки под свойства криптовалюты, заключаем, что она не является ни вещью, ни имущественным правом, ни иным имуществом и, следовательно, не может быть признана объектом имущественных прав де-юре. Данный подход уже давно вышел за рамки теории и прочно укрепился в судебной практике. Так, согласно утверждению суда, к объектам гражданских прав не может относиться налог (постановление Арбитражного суда Восточно-Сибирского округа от 29.04.2015 № Ф02–1313/2015[2] по делу № А33–8699/2014), так как он не приравнивается к имущественным правам, посевам сельскохозяйственных культур (постановление Восемнадцатого арбитражного апелляционного суда от 17.06.2014 № 18АП-5837/2014 по делу № А07–22617/2013)[3] ввиду отсутствия правового режима незавершенного производства, а также самовольные строения (обзор судебной практики Верховного Суда Российской Федерации № 2 (2016), утвержденный Президиумом Верховного Суда РФ 06.07.2016)[4] ввиду нарушения режима регистрации имущества и др. Очевидно, что и криптовалюта

[1] Сидоренко Э.Л. Правовой статус криптовалют в Российской Федерации // Экономика. Налоги. Право. 2018. № 2. С.132.

[2] Там же. С.132.

[3] Там же. С.132.

[4] Обзор судебной практики Верховного Суда Российской Федерации № 2 (2016) (утв. Президиумом Верховного Суда Российской Федерации 06.07.2016). URL: http://www.consultant.ru/document/cons_doc_LAW_201474/ (дата обращения: 01.03.2022)

не может быть объектом гражданских прав ввиду отсутствия правовых гарантий участников сделки. Так, в 2014 г. был заключен договор купли-продажи между ИП А.С. Абрамовым и ООО «Виктория». Вопрос о криптовалютах в процессе появился тогда, когда к нему было привлечено третье лицо — сингапурская компания Magna Trading Ltd. Как утверждалось, А.С. Абрамов занял у иностранной фирмы 5 млн сингапурских долларов для покупки недвижимости в Хабаровском крае, однако в положенный срок деньги не отдал. В суде Абрамов А.С. заявил, что заем он вернул посредством перевода в криптовалюте. Этот довод судом был оценен критически, поскольку он «не подтверждает факта оплаты денежных средств ответчику по договору займа». Позднее вступившим в силу решением Арбитражного суда Дальневосточного округа было окончательно закреплено: криптовалюта и виртуальная валюта не расцениваются судами как деньги, а обязательства А.С. Абрамова не считают исполненными.

От гражданско-правового определения виртуальной валюты напрямую зависит ее определение как предмета и средства преступного посягательства. В настоящее время не ведется официальной статистики преступлений, совершенных с использованием криптовалют, но даже имеющихся отрывочных данных достаточно для того, чтобы говорить о стремительном увеличении оборота наркотиков и порнографии в теневом Интернете с использованием криптовалюты. По некоторым экспертным оценкам, «если в 2014 г. органами наркоконтроля был установлен один факт приобретения наркотиков за биткоины, то уже в 2015 г. об этом имелась информация более чем по 20 субъектам Российской Федерации, расположенным в шести федеральных округах». Согласно данным Центра цифровой экономики и финансовых инноваций МГИМО МИД России, в настоящее время при покупке наркотиков и порнографии преимущественно используется криптовалюта (90%), а только затем — платежные системы с анонимными кошельками[1]. Криминальное использование виртуальной валюты объясняется не только ее технологическими особенностями, но и трудностями квалификации преступлений. Мы выделили два принципиально разных подхода к определению криптовалют в уголовном праве: виртуальная валюта как средство совершения преступления и виртуальная валюта как предмет преступного посягательства. Судебная

[1] Сидоренко Э.Л. Правовой статус криптовалют в Российской Федерации // Экономика. Налоги. Право. 2018. № 2. С.133.

практика не испытывает серьезных трудностей с уголовно-правовой квалификацией оборота наркотических средств, психотропных веществ, их аналогов и прекурсоров, а также порнографии при использовании виртуальной валюты в качестве платежного средства в ходе приобретения указанных запрещенных предметов. Это объясняется тем, что объективную сторону составов преступлений согласно ст. 228–229.1, 242 Уголовного кодекса Российской Федерации (УК РФ) образуют действия лиц по обороту данных предметов.

Что же касается криптовалюты, то проведенная в блокчейне транзакция рассматривается как доказательство перехода предмета преступления от одного лица к другому, а крупный размер определяется количеством (свойствами) наркотиков (психотропных веществ, прекурсоров и др.), а не суммой криптовалюты. Намного сложнее определить правовой статус криптовалюты как предмета преступного посягательства. К числу уголовно-правовых нарушений, в которых виртуальная валюта является предметом преступления, относятся хищения (кража, грабеж, разбой, мошенничество) и вымогательство. Как обоснованно отмечено в постановлении Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[1], если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений п. 1 примечаний к ст. 158 УК РФ[2] и ст. 128 ГК РФ[3] содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб». Фактически высшая судебная инстанция вопрос об уголовно-правовом статусе криптовалюты поставила

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 (ред. от 29.06.2021). URL: http://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 01.03.2022).

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ// Ст. 158. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/57b5c7b83fcd2cf40cabe2042f2d8f04ed6875ad/ (дата обращения: 01.03.2022)

[3] Гражданский кодекс Российской Федерации // Ч. 1. Ст. 128. URL: https://base.garant.ru/10164072/089c3288c5448786f472572a85a4941a/ (дата обращения: 01.03.2022).

в зависимость от ее определения в гражданском праве. Этот подход уже нашел отражение в судебной практике. Ряжский районный суд (Рязанская область) рассмотрел иск местного жителя к ИП Бояркину Р.В. Истец перевел на сервер, принадлежащий Р.В. Бояркину, криптовалюту, но взамен получил в рублях гораздо меньшую сумму. Суд при вынесении решения отметил, что «поскольку в Российской Федерации отсутствует какая-либо правовая база для регулирования платежей, осуществляемых в «виртуальной валюте», в частности в биткоинах, а также отсутствует какое-либо правовое регулирование торговых интернет-площадок, биткоин-бирж, все операции с перечислением биткоинов производятся их владельцами на свой страх и риск». И хотя речь идет о гражданско-правовом споре, суд однозначно дает понять, что криптовалюта, не являясь объектом гражданских прав, не может рассматриваться и как предмет мошенничества. Не меньше вопросов вызывает оценка криптовалюты как предмета кражи. По экспертным оценкам, в настоящее время все чаще виртуальная валюта похищается из криптокошельков, но правоохранительные органы, как правило, отказывают в возбуждении уголовного дела, мотивируя это тем, что отсутствует предмет посягательства и, следовательно, состав кражи. С этим аргументом мы согласны лишь отчасти. С одной стороны, отсутствие у криптовалюты статуса объекта гражданских прав не позволяет говорить о нарушении охраняемых законом гражданско-правовых отношений и оценивать ее в денежном эквиваленте. С другой стороны, одной из задач уголовного законодательства является предупреждение совершения преступлений, и квалификация хищений криптовалюты не должна оставаться вне рамок уголовно-правового регулирования[1].

Понятие «криптовалюта» в законодательстве Российской Федерации не закреплено. Разработанные Минфином России совместно с заинтересованными федеральными органами исполнительной власти проекты федеральных законов «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» и «О внесении изменений в отдельные законодательные акты Российской Федерации» признаны Правительством Российской Федерации требующими доработки с учетом результатов мониторинга обращения денежных суррогатов (в том числе криптовалют), а также про-

[1] Сидоренко Э.Л. Правовой статус криптовалют в Российской Федерации // Экономика. Налоги. Право. 2018. № 2. С. 129-137.

ведения с учетом зарубежного опыта дополнительного анализа рисков их возможного использования в противоправных (преступных) целях[1].

1 января 2021 года в Российской Федерации вступил в силу закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ»[2], который заложил основы регулирования криптовалютной отрасли в России. Закон не дает полного ответа на вопрос, что должен делать гражданин или компания, чтобы инвестировать денежные средства в криптовалюту либо проводить иные операции с ней на законных основаниях.

В то же время в данном законе содержится понятие «цифровая валюта», которое мы относим и к существующим в настоящее время криптоваютам, выпущенным на блокчейне. Под данным термином понимается «совокупность электронных данных, содержащихся в информационной системе… в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных…». Закон напрямую не относит наиболее распространенные криптовалюты к цифровым финансовым активам. Указанное ведет к тому, что для приобретения криптовалюты гражданам нет необходимости соблюдать дополнительные требования законодательства, так как они в нем не предусматриваются.

Указанный закон проводит четкое разделение между цифровыми финансовыми активами и цифровыми валютами, это две абсолютно разные сущности.

Необходимо отметить, что в соответствии со статьей 1 данного закона предметом его регулирования и сферой действия являются «отношения, возникающие при выпуске, учете и обращении цифровых финансовых активов, особенности деятельности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и оператора обмена цифровых финансовых активов, а также отношения, возникающие при обороте цифровой валюты в Российской Федерации».

---

[1] Бабурина П.М. Виртуальная валюта как способ легализации доходов, полученных преступным путем // IX Международная научно-практическая конференция "Инновационное развитие российской экономики": в 6 т. Москва // РЭУ им. Г.В. Плеханова. 2016. С. 256-258.

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ. Доступ из СПС «КонсультантПлюс» (дата обращения: 01.03.2022).

В соответствии с данным законом также «цифровыми финансовыми активами признаются цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном настоящим Федеральным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы. Цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам»[1].

Следовательно, в настоящее время для легального пользования криптовалютой необходимо перейти на соответствующий сайт компании, представляющей услуги по обмену криптовалюты либо на сайт биржи, осуществляющей торги, и заполнить информацию о себе, представив копию паспорта, подтверждение адреса регистрации, в некоторых случаях пройти процедуру видеорегистрации. Отчетность же до введения Федеральной налоговой службой России особых форм отчетности подается физическими лицами по форме 3-НДФЛ.

Вопросы для самоконтроля

1. Какой изначально статус получила криптовалюта применительно к ст. 128 ГК РФ ввиду открытого перечня объектов гражданских прав?

[1] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ. СПС «КонсультантПлюс» (дата обращения: 01.03.2022).

2. Запрещен ли оборот криптовалюты в соответствии с действующим законодательством России?

3. Когда вступил в силу Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ»?

4. Какое определение дано «цифровой валюте» в Федеральном законе № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ»?

5. Относит ли Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ» криптовалюту напрямую к цифровой валюте?

6. Каким образом осуществляется налоговая отчетность по доходам, полученным с криптовалюты?

ГЛАВА 2.
ВОЗБУЖДЕНИЕ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Криптовалюта все чаще становится предметом или объектом как киберпреступлений, так и преступлений вне виртуальной реальности. Киберпреступность – область, для расследования которой требуются не только юридические знания, но и понимание особенностей работы IT-технологий, и именно она постепенно становится основным инструментом правонарушителей.

Самая большая категория киберпреступлений, связанных с криптовалютами в мире в 2017 году, была связана с хакерскими атаками на обменники криптовалют с помощью создания, использования и распространения вредоносных компьютерных программ и в дальнейшем непосредственно кражей криптовалют или фишингом[1].

По статье мошенничество, в т.ч. и в сфере компьютерных технологий в основном возбуждаются дела, связанные с инвестированием проектов, выдвигаемых на ICO. Также к киберпреступлениям в данной сфере мы относим и организацию деятельности по привлечению денежных средств или иного имущества. По данным Международной фирмы по кибербезопасности Group-IB, более 56% средств на ICO было похищено с помощью фишинга. В 2017 году было похищено более 10% всех привлеченных инвестиций, а 80% проектов не выполнили обязательства перед инвесторами и исчезли после сбора средств[2].

В отдельную категорию необходимо выделить преступления, связанные с майнингом. Во-первых – это причинение имущественного ущерба путем обмана и злоупотребления доверием в сфере энергетики с помощью ненадлежащего использования оборудования для майнинга. А также мошенничество непосредственно при купле-продаже несуществующих ферм и их комплектующих.

Биткоин-брокеры, криптобиржи и криптообменники подвержены таким преступлениям, как незаконная банковская деятельность, вымогательство и убийство. В течение последних 18 месяцев обмен

[1] Манукян К.А., Васильев А.М. Криптоденьги и их влияние на криминогенную среду //Современный ученый. 2021. №. 4. С. 261-265.

[2] Group-IB представила отчет о киберпреступности и призвала рынок к хантингу. URL: https://www.group-ib.ru/media/hi-tech-crime-trends-2018/ (дата обращения: 11.03.2022).

криптовалютами остается фатальным недостатком в экосистеме. Благодаря централизованной инфраструктуре и контролю над средствами пользователей обменные процессы являются привлекательной приманкой для хакеров и других киберпреступников.

Применение криптовалюты при легализации (отмывании) доходов, полученных преступным путем, финансировании терроризма и финансировании распространения оружия массового уничтожения является предметом серьезной озабоченности международного сообщества. Создателями цифрового золота, безусловно, не предполагалось использование его в целях финансирования терроризма и обеспечения незаконного оборота наркотиков, но именно это оказалось черной меткой для криптовалют, которая настроила против нее все силовое лобби.

В Костромской области было возбуждено уголовное дело по части 2 статьи 172 УК РФ. По данным полиции, задержанные обналичили около 500 миллионов рублей путем обмена и перевода криптовалюты. Чтобы обменивать и переводить криптовалюту, обвиняемые оформили на своих родственников более 300 банковских и сим-карт. В сентябре 2017 года уголовное дело было передано в суд, информации о приговоре пока нет. Это первое в России дело об обналичивании биткоинов[1].

В Пермском крае возбуждено уголовное дело по статьям 210, 228.1, 174.1 УК РФ в связи с деятельностью злоумышленников, организовавших продажу наркотических средств и психотропных веществ на территории Перми, Екатеринбурга, Ижевска и Челябинска посредством интернет-магазина, оплата в интернет-магазине производилась посредством криптовалюты. Следствием установлено, что подсудимые обналичили порядка девяти миллионов рублей. В октябре 2018 года дело передано в суд[2].

В Кемерово Ленинским районным судом вынесен приговор по уголовному делу, предусмотренному ч. 3 ст. 30 - ч. 5 ст. 228.1 УК РФ. Фигурант являлся «сотрудником» интернет-магазина по торговле наркотиками, за участие в схеме торговли синтетической «солью» он получал оплату в виде криптовалюты. Признан виновным в августе

[1] Первое уголовное дело за обналичивание биткоинов заведено в России. URL: https://www.vedomosti.ru/technology/articles/2017/09/01/732040-politsiya-fsb-zaderzhali (дата обращения: 01.03.2022).

[2] В Прикамье перед судом предстанет лидер преступного сообщества наркодилеров. URL: https://zakonovest.ru/v-prikame-pered-sudom-predstanet-lider-prestupnogo-soobshhestva-narkodilerov/ (дата обращения: 01.03.2022).

2018 года с назначением наказания в виде 7 лет 6 месяцев лишения свободы с отбыванием в исправительной колонии строгого режима.

В Марий Эл возбуждено уголовное дело по факту мошенничества. По данным полиции, потерпевший в Интернете, используя игровую биржу, приобрел биткоины. После перевода денежных средств в сумме 100 тысяч рублей на счет продавца биткоины не поступили на его счет, а сайт оказался заблокирован. Злоумышленники создали так называемый сайт-двойник официального сайта биржи криптовалют, в названии которого имеется незначительная разница в знаках или буквах.

В Оренбургской области возбуждено уголовное дело по признакам преступления, предусмотренного частью 2 статьи 165 УК РФ на основании заявления от сотрудников энергетической компании о том, что зафиксирована потеря электроэнергии на территории одного из бывших заводов. На месте происшествия полицейские обнаружили более 6000 единиц техники, подключенной к электросети, и силовые кабели электропитания, ведущие к подстанции, расположенной рядом. Предварительно установлено, что высокотехнологичное оборудование использовалось для производства криптовалюты. Работа данного предприятия осуществлялась без учета потребления электроэнергии объемом свыше 8 миллионов КВт/ч[1].

В июне 2018 года жителя Королева задержали по подозрению в хищении у директора компании «Бизнес-сети» под предлогом продажи, т.е. путем обмана 103 биткоинов задержан 27-летний директор ООО «Центр Мед групп». Он проходил подозреваемым по возбужденному ранее уголовному делу по ч. 4 ст. 159 УК РФ и помещен Люблинским районным судом под домашний арест. Следствие установило обстоятельства дела и производила поиск возможных соучастников преступления. Ранее 25-летний уроженец Армении, работающий исполнительным директором ООО «Бизнес-сети», обратился в полицию с заявлением о мошенничестве. По данным источника агентства, неизвестные ввели потерпевшего в заблуждение и заверили, что помогут ему в продаже 103 биткоинов. Впоследствии мужчина передал криптовалюту стоимостью 45,3 млн руб. неизвестным в помещении некоего банка, название и адрес которого, по его словам, он не помнит, как не помнит мошенников, поскольку находился после хищения в шоковом состоянии. Как установила полиция, передача

[1] Возбуждение уголовных дел по криптовалюте и майнингу. URL: https://bitcryptonews.ru/lawyers/vozbuzhdenie-ugolovnyix-del-po-kriptovalyute-i-majningu (дата обращения: 01.03.2022).

биткоинов произошла в офисном помещении по адресу Малый Кисловодский пер., д. 1. После этого неизвестные скрылись и на связь не выходили[1].

В основном кражи криптовалют происходят с «горячих» кошельков, т.к. «холодный» кошелек не подключен к Интернету. Основная его особенность заключается в том, что он имеет два приватных ключа. Один из них отвечает за разблокировку и перенос биткоинов на «горячий» кошелек, другой же необходим при обнаружении, например, хакерской атаки. Владелец, обнаруживший проведение незаконной транзакции, в течение 24 часов после случившегося при помощи ключа восстановления может вернуть все потерянные средства. Это, пожалуй, самый эффективный способ борьбы с атаками хакеров на платежную систему Биткоин. Однако для того, чтобы он был действительно эффективным, все ключи восстановления должны снабжаться замедлителем, таймлоком. Именно благодаря этому уникальному механизму удалось вернуть все средства, похищенные с фондов TheDAO в Эфириуме и предотвратить атаку на сеть Steemit[2].

Необходимо отметить, что в 2018 году было совершено пять преступлений – квалифицированных мошенничеств на территории Петровского района Ставропольского края, города Пятигорска, Октябрьского района и Промышленного района города Ставрополя, а в 2019 году – четыре преступления, квалифицированных мошенничеств на территории города Кисловодска, города Буденновска и Октябрьского района города Ставрополя, связанных с попыткой покупки криптовалюты[3].

Чтобы использовать биткоин, необходимо зарегистрировать биткоин-кошелек (он создается с помощью установления программного обеспечения биткоин) или использование услуги по обмену биткоина через различные интернет-сайты, использование онлайн-кошелька. Отметим, что при создании биткоин-кошелька нельзя

---

1 Житель Королева похитил у москвича 103 биткоина. URL: https://www.innov.ru/news/accident/zhitel-koroleva-pokhitil-/ (дата обращения: 01.03.2022).

[2] Возбуждение уголовных дел по криптовалюте и майнингу. URL: https://bitcryptonews.ru/lawyers/vozbuzhdenie-ugolovnyix-del-po-kriptovalyute-i-majningu (дата обращения: 11.03.2022).

[3] Аветисян А.Д., Диденко Н.С. Отдельные проблемы противодействия преступлениям с использованием криптовалют в Российской Федерации. URL: https://cyberleninka.ru/article/n/otdelnye-problemy-protivodeystviya-prestupleniyam-s-ispolzovaniem-kriptovalyut-v-rossiyskoy-federatsii (дата обращения: 11.03.2022).

идентифицировать личность пользователя, если только нет возможности подтвердить адрес его электронной почты смс-сообщением, что представляет значительные трудности в выяснении личности пользователей при расследования уголовных дел. Лица, совершавшие мошенничества по обмену денежных средств на криптовалюту, создавали отдельные группы по инвестированию в криптовалюту путем перечисления денежных средств на банковскую карту отдельных лиц, размещали в Интернете информацию о возможности получения прибыли от торгов на криптовалютных биржах путем перечисления денежных средств на биткоин-кошелек. Во время расследования уголовных дел следователи при идентификации пользователей, размещавших информацию о возможности инвестирования в криптовалюту, не могли установить личности мошеннников в связи с тем, что те использовали методы анонимизации в своей деятельности в сети Интернет. При расследовании всех уголовных дел следователи по истечении сроков предварительного следствия приняли решение о приостановлении предварительного следствия в связи с неустановлением лиц, совершивших преступления по п. 1 ч. 1 ст. 208 Уголовно-процессуального кодекса РФ (УПК РФ)[1].

Практика показывает немалое количество трудностей, с которыми сталкиваются следственные органы при расследовании преступлений с использованием криптовалют.

В начале 2019 года по факту деятельности одной из криптовалютных платформ было возбуждено уголовное дело по ст. 172.2 УК РФ, предусматривающей ответственность за организацию финансовой пирамиды[2].

Возбуждение уголовного дела по данному составу поставило следственный орган перед вопросами квалификации преступления. В частности, как может быть незаконной та деятельность, которая законом не запрещена, а согласно зарубежным правовым нормам, и вовсе законна? Если криптовалюта не является денежным средством, то является ли она иным имуществом? А если является, то сопоставим ли его объем с объемом привлеченных средств или имущества? Каким образом подлежит установлению реальный объем криптовалютных транзакций в рамках торговой платформы?

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. URL:http://www.consultant.ru/document/cons_doc_LAW_34481/163a9531661e3d3fd143be93c3eb61c84ba333ef (дата обращения: 11.03.2022).

[2] Криптовалюта как предмет преступления: проблемы квалификации и защиты. URL: https://pravo.ru/opinion/215852/ (дата обращения: 11.03.2022).

В такой ситуации следственный орган нашел иной способ разрешения сложных вопросов, переквалифицировав деяние на ч. 4 ст. 159 УК РФ («Мошенничество, совершенное организованной группой либо в особо крупном размере»)[1].

В рамках уголовного дела в порядке ст. 91 УПК РФ следствие задержало подозреваемых и направило в суд ходатайство об избрании в отношении них меры пресечения в виде заключения под стражу.

Достаточным основанием избрания самой строгой меры пресечения, по мнению следствия, явилось совершение преступления дистанционным способом. При этом следователь заявил, что доказательств, достаточных для предъявления обвинения по ст. 159 УК РФ, не имеется, а именно: доказательств самого факта хищения денежных средств и (или) иного имущества путем обмана или злоупотребления доверием.

Все, чем располагало следствие, – это ряд физических лиц, заявивших о добровольном приобретении на личные средства криптовалюты и последующей неудачной инвестиционной деятельности с использованием криптовалютной платформы.

Таким образом, диспозиция ст. 159 УК РФ спорные вопросы квалификации криптовалюты как предмета преступления не сняла, но поставила следственный орган перед необходимостью доказать не только факт, но и способ хищения именно криптовалюты, а не денежных средств.

В результате в удовлетворении ходатайства об избрании меры пресечения суд отказал, подозреваемые были освобождены из-под стражи в зале суда.

Данный пример является показательным с позиции очевидного конфликта публично-правовых и частноправовых интересов непосредственных владельцев цифровых активов.

Многочисленные пользователи криптовалютной платформы, имеющие личные онлайн-кабинеты, располагая собственными денежными средствами, в разные периоды времени добровольно вкладывались в приобретение цифровых активов, что никогда не было запрещено законом Российской Федерации. Такие цифровые активы были приобретены через интернет-кошельки с использованием единственно возможного средства платежа на территории Российской Фе-

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ . Ст. 159. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/8012ecdf64b7c9cfd62e90d7f55f9b5b7b72b755/(дата обращения: 11.03.2022).

дерации – российского рубля. К нарушениям установленного государством порядка расчетов эти транзакции не привели.

Вопросы для самоконтроля

1. Какие преступления были самыми частыми в отношении держателей криптовалют в 2017 году?
2. Каким образом наиболее часто осуществляются мошенничества с использованием криптовалюты?
3. Можно ли при создании биткоин-кошелька идентифицировать личность пользователя?
4. Какие преступления с применением криптовалюты стали в последние годы серьезно волновать международное сообщество?
5. Как используется криптовалюта в наркоторговле?

ГЛАВА 3.
ПРОВЕДЕНИЕ СЛЕДСТВЕННОГО ОСМОТРА ПО ПРЕСТУПЛЕНИЯМ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Одним из самых важных следственных действий на первоначальном этапе расследования преступлений, совершенных с помощью криптовалют, является осмотр места происшествия. Сущность осмотра заключается в непосредственном исследовании следователем, дознавателем, а также другими участниками следственного действия обстановки места происшествия; выявлении, изучении, фиксации и изъятии в установленном законом порядке материальных объектов и следов на них с целью получения сведений и доказательств, имеющих значение для раскрытия и расследования преступлений, а также событий, содержащих признаки преступления. Проведение осмотра предполагаемого или действительного места происшествия в ряде случаев имеет решающее значение для установления факта наличия или отсутствия оснований для возбуждения уголовного дела. В связи с этим закон допускает производство данного следственного действия на основании ч. 2 ст. 176 УПК РФ[1] до возбуждения уголовного дела.

Основания для проведения осмотра и процессуальный порядок установлены в ст. 176 – 178 УПК РФ[2]. Осмотр по делам о преступлениях, совершенных с использованием криптовалют, позволяет установить ряд важных обстоятельств, а именно:

– наличие следов события, подлежащего расследованию;

– если факт наличия следов установлен, то необходимо установить, содержатся ли признаки состава преступления;

– кто непосредственно принимал участие в совершении преступления и какую функцию выполнял;

– наличие свидетелей совершения преступления;

– наличие на месте происшествия носителей информации, содержащих следы события, подлежащего расследованию;

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. Ст.176.
URL: http://www.consultant.ru/document/cons_doc_LAW_34481/544834cac95f015d568dc83cf8813b54c707cadc/ (дата обращения: 11.03.2022).

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. Ст.176, 177, 178.
URL: http://www.consultant.ru/document/cons_doc_LAW_34481/544834cac95f015d568dc83cf8813b54c707cadc/ (дата обращения: 11.03.2022).

– наличие технических средств, которые использовались для доступа к информации;

– имеются ли на месте происшествия следы подготовки к преступлению;

– были ли предприняты попытки сокрытия следов преступления, если да, то какие именно.

По делам о преступлениях, совершенных с использованием криптовалют, в качестве места происшествия могут выступать адрес местонахождения физического лица или организации и место нахождения используемых аппаратно-программных средств. Основными объектами, подлежащими осмотру, являются помещения, где расположена компьютерная техника, периферийные устройства, оптические и магнитные носители, распечатки, мобильные телефоны. При осмотре помещения необходимо обращать внимание на небольшие листки (клочки, обрывки) бумаги, которые нередко прикрепляются к компьютеру или находятся в непосредственной близости от него (на них могут быть записаны коды и другие важные для следствия пометки). Носители информации, имеющей отношение к расследуемому событию, могут быть с соблюдением установленного УПК РФ порядка изъяты и приобщены к уголовному делу в качестве вещественного доказательства. Сразу по прибытии на место происшествия необходимо принять меры к обеспечению сохранности информации в подлежащих осмотру объектах, для чего необходимо соблюдать следующие правила:

– никому не позволять прикасаться к объектам осмотра;

– никому не позволять выключать электроснабжение объекта;

– никому не позволять и не производить самому никаких манипуляций с техникой, если их результат заранее не известен;

– необходимо учитывать вероятность принятия лицами, заинтересованными в сокрытии преступления, мер по уничтожению информации и других ценных данных, а также вероятность установки в осматриваемую компьютерную технику специальных средств защиты от несанкционированного доступа, которые, не получив в установленное время специального сигнала или кода, автоматически уничтожают всю хранящуюся там информацию либо интересующую следствие наиболее важную ее часть и вероятность установки иных средств защиты информации от несанкционированного доступа.

На месте происшествия, как правило, могут находиться электронные носители информации: внешние накопители на жестких магнитных дисках, оптические диски, флеш-накопители. Соответственно,

в протоколе осмотра места происшествия необходимо указать на факт их наличия и отметить данные о месте нахождения носителя информации, его типе, названии, а также информацию, индивидуализирующую и идентифицирующую объект (маркировочные обозначения, серийные номера, характерные надписи и метки и т.п.). Также не исключается наличие на месте происшествия различной цифровой техники (ноутбуков, мобильных телефонов, планшетных компьютеров, электронных книг и т.п.), на носителях которых могут остаться следы события преступления. Наличие такого рода техники описывается в протоколе с указанием сведений, аналогичных сведениям, проводимым при обнаружении носителей информации, однако дополнительно указывается комплектация оборудования. Необходимо учитывать, что преступление, совершенное с использованием криптовалют, может быть совершено и с рабочего места, где все данные хранятся на сервере. Соответственно, необходимым условием для надлежащего проведения расследования является проведение осмотра помещения с сервером, на котором предположительно будет иметься информация, относящаяся к событию преступления. В данном случае в протоколе осмотра необходимо указать на факт наличия технических средств, к которым нет логического доступа непосредственно из осматриваемого помещения, поскольку рабочее место по управлению сервером находится, как правило, в другом помещении. Целесообразно будет указать на место доступа к серверу с правами администратора, и данное место также должно подлежать осмотру в качестве места происшествия.

При осмотре места преступления необходимо дополнительно обратить внимание на:

– обнаружение, осмотр и изъятие средств подготовки, совершения и сокрытия преступления;

– наличие электронных средств связи;

– наличие специальных технических средств для негласного получения информации;

– наличие специальной литературы, методических рекомендаций и цифровых видеофильмов, раскрывающих способ преступления;

– наличие электронных записей, находящихся в памяти цифрового устройства и содержащих криминалистически значимые сведения;

– биткоин-адреса, имена, номера телефонов, сетевые псевдонимы, сетевые адреса и другую информацию. Важно отметить, что по результатам осмотра следователь или дознаватель может установить,

совершено ли преступление с использованием криптовалют либо происшедшее событие является следствием негативных факторов или правонарушением иного рода. Осмотр предметов по делам о преступлениях, совершенных с использованием криптовалют, на первый взгляд, не содержит особой специфики по сравнению с аналогичным осмотром, проводимым по делам о преступлениях в сфере информационно-коммуникационных технологий, порядок и содержание которого детально описывались различными учеными. Вместе с тем, на наш взгляд, это не совсем верное утверждение. Специфика осмотра предметов и документов по делам о преступлениях, совершенных с использованием криптовалют, заключается в том, что осмотру подлежат, как правило, служебные журналы системных и прикладных программ, программ-кошельков, применяемых для осуществления транзакций, а также файлы wallet.dat или иные, содержащие сведения о кошельках. Это предполагает использование в ходе осмотра современного программного обеспечения, позволяющего быстро находить требуемые файлы и интерпретировать их содержимое. Использование в этих целях компьютера, специально не подготовленного для проведения осмотра, например рабочего компьютера следователя, нецелесообразно.

В ходе проведения осмотра необходимо обратить внимание на то, что персональный компьютер (ПК) будет являться наиболее важным источником криминалистически значимой информации ввиду специфики совершаемых преступлений. Повышенное внимание необходимо обратить на аппаратное содержимое ПК, в первую очередь на жесткий диск (внутренний или внешний) и сетевую карту. Обусловлено это тем, что именно на жестком диске, как правило, хранится информация об используемом специализированном программном обеспечении (ПО) для работы с криптовалютами, а именно программы-кошельки и программы для майнинга. Сетевые карты, в свою очередь, обладают уникальным номером (MAC-адресом), который используется интернет-провайдерами для идентификации своих клиентов, что в последующем может стать важным для деанонимизации пользователя криптовалют. В процессе проведения осмотра необходимо установить IP- и MAC-адреса ПК. IP-адрес присваивается интернет-провайдером и используется для идентификации компьютера в сети Интернет при передаче и приеме информации. MAC-адрес задается каждому устройству, предназначенному для работы в компьютерных сетях, на заводе-изготовителе. Однако необходимо подчеркнуть, что MAC-адрес может быть подменен средствами опе-

рационной системы. Установление IP- и MAC-адресов и сопоставление их с данными, полученными от провайдеров интернет-услуг и платежных систем, позволяет установить причастность пользователя к совершению преступления. Также немаловажно изучить данные всех браузеров, установленных на ПК. Ввиду того, что многие пользователи криптовалют используют их для просмотра специализированных сайтов о криптовалютах, для регистрации онлайн-кошельков криптовалют, посещения сайтов бирж и обменников. Особо пристальное внимание необходимо уделять Tor-браузеру, в случае если подозреваемый (обвиняемый) им пользовался. Tor необходим для сокрытия личных данных и следов пребывания пользователя при работе в сети Интернет. Использование данного программного обеспечения свидетельствует об опытности пользователя и (или) его желании скрыть следы своей противоправной деятельности. С пользовательской точки зрения Tor представляет собой специальный браузер (на основе Mozilla Firefox).

При осмотре любого браузера необходимо проявлять осторожность: не закрывать открытые вкладки (это может привести к прекращению сеанса работы с сервисом, требующим ввода пароля), переход по гиперссылкам осуществлять в режиме «Открыть в новой вкладке». Существенное значение может иметь информация, полученная при изучении истории просмотра веб-страниц и закладок в браузере. При этом особого внимания заслуживают:

1) социальные сети («ВКонтакте», Facebook (признана экстремистской и запрещена на территории России), «Одноклассники» и т.д.). Изучение переписки может указать на факт передачи или получения закрытых ключей кошелька криптовалюты с целью его дальнейшего распоряжения или же адреса криптовалюты для получения или отправки переводов. Также необходимо проверить, состоит ли подозреваемый (обвиняемый) в группах, посвященных криптовалютам;

2) информация с различных сайтов, которые посещал подозреваемый (обвиняемый), содержащая сведения о криптовалютах, способах деанонимизации (миксерах), использовании сети Tor;

3) иные электронные платежные системы.

Изучив данные браузера, возможно установить и электронные платежные системы, которыми пользовался подозреваемый (обвиняемый), помимо криптовалютных. Например, такие платежные системы, как Qiwi, WebMoney, «Яндекс-деньги» и др. Они могут исполь-

зоваться как посредники для обмена криптовалют на фиатные деньги и обмена фиатных денег на криптовалюты.

При осмотре необходимо минимизировать влияние на носители информации: не копировать на них новые файлы (особенно крупные), не запускать требовательные к объему памяти программы или программы для обслуживания носителей информации для исключения утраты возможности восстановления недавно удаленных файлов. На заключительном этапе следственного осмотра при принятии решения об изъятии компьютера его целесообразно не выключать, а перевести в спящий режим, в этом случае сохраняется состояние всех запущенных приложений, а не только информация на жестком диске[1].

Все собранные в ходе осмотра материалы могут в перспективе стать не только достаточным подтверждением факта совершения преступления при возбуждении уголовного дела, но и важным доказательством в дальнейшем расследовании.

Вопросы для самоконтроля

1. Какие обстоятельства позволяет установить осмотр по делам о преступлениях, совершенных с использованием криптовалют?

2. Для чего при осмотре помещения необходимо обращать внимание на клочки, обрывки бумаги, которые нередко прикрепляются к компьютеру или находятся в непосредственной близости от него?

3. Какие электронные записи, находящиеся в памяти цифрового устройства могут содержать криминалистически значимые сведения?

4. Что может показать изучение переписки в социальных сетях держателя криптовалюты?

5. Какие платежные системы могут использоваться как посредники для обмена криптовалют на фиатные деньги и обмена фиатных денег на криптовалюты?

[1] Маркарян Э.С. Специфика проведения следственного осмотра при расследовании преступлений, совершенных с использованием криптовалют // Актуальные проблемы российского права. 2018 (6). С.146-152.

ГЛАВА 4.
УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ МЕР ПРОЦЕССУАЛЬНОГО ПРИНУЖДЕНИЯ В ОТНОШЕНИИ КРИПТОВАЛЮТ И ДРУГИХ ВИРТУАЛЬНЫХ АКТИВОВ

Возросшая популярность криптовалют обусловливает активное ее использование в торговле наркотиками, оружием, поддельными документами и в иной преступной деятельности. Данные факты, а также возможность бесконтрольного трансграничного перевода денежных средств и их последующего обналичивания служат предпосылками высокого риска потенциального вовлечения криптовалюты в схемы, направленные на легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма.

Данные утверждения подтверждаются обширной судебной практикой за последние несколько лет.

Так, в определении Свердловского областного суда от 12 мая 2017 г. № 22-3186/2017 устанавливается, что оплата распространителей наркотиков и иных участников осуществлялась посредством криптовалюты[1].

Однако перед началом нашего анализа уголовного процесса необходимо затронуть процесс арбитражный.

15 мая 2018 г. Девятый арбитражный апелляционный суд в постановлении № 09АП-16416/ 2018, А40-124668/2017 фактически признал криптовалюту имуществом, что, на наш взгляд, в корне не верно. Суд постановил в деле о банкротстве изъять у банкрота юридически несуществующую криптовалюту, продать ее, а деньги с ее продажи использовать по назначению. Однако в связи с этим возникает ряд трудностей, с которыми столкнется как арбитражный суд, так и любой другой[2].

Термин «криптовалюта» означает, что создание и передача имущественных прав основана на криптографии, т.е. на шифровании

---

[1] Определение Свердловского областного суда от 12.05.2017 № 22-3186/2017. URL:http:// www.ekboblsud.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=13139011 &delo_ id=4&new=0&text_number=1 (дата обращения: 01.03.2022).

[2] Постановление Девятого арбитражного апелляционного суда № 09АП-16416/2018, А40-124668/2017. URL:https://base.garant.ru/61623374/ (дата обращения: 01.03.2022).

и передаче информации таким образом, чтобы ее содержимое было защищено от нежелательного доступа третьих лиц. По аналогии с интернет-банкингом, где на сервере каждого финансового учреждения записано сальдо счета, но в случае с криптовалютой «сервер» основан на блокчейне, где никто не может самостоятельно распоряжаться цепочкой блоков. Ни один человек не может хранить биткоины на жестком диске компьютера (в виде, например, отдельного файла), так как физически они не существуют.

Как объект уголовно-процессуального регулирования криптовалюта должна рассматриваться в виде цифровой записи на удаленном носителе данных, охраняемой законом об информации.

Криптовалюта по смыслу ч. 1 ст. 104.1 УК РФ[1] может быть предметом имущественного обеспечения. Арест на нее может налагаться по правилам ч. 1 ст. 115 УПК РФ[2] в целях обеспечения исполнения приговора в части гражданского иска, взыскания штрафа, иных имущественных взысканий или возможной конфискации имущества. Обеспечение обусловлено угрозой утраты активов в результате действий обвиняемого или третьих лиц.

Арест криптовалюты сопряжен с трудностями эффективного технического обеспечения. С одной стороны, нужно «закрепить» цифровую запись таким образом, чтобы она не стала объектом нежелательных переводов и манипуляций. С другой – реальный доступ к криптовалюте должен сохраняться, поскольку необходимость в обеспечении может отпасть.

Обеспечение криптовалюты возможно при условии обладания публичным ключом доступа, который позволит идентифицировать правообладателя. В случае если ключами обладает третье лицо, адресатом процессуального решения должно быть именно оно.

Реальный доступ к криптовалюте обусловлен знанием логина и пароля от криптовалютного кошелька, позволяющими управлять найденными в кошельке цифровыми записями. Получение доступа к кошельку не гарантирует достаточной защиты данных от манипуляций с электронными данными, так как любое лицо, имеющее логин и пароль, может в любой момент войти в кошелек и вывести из него криптовалюту. Обвиняемый в таком случае гарантированно избежит

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. Ст. 104.1. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/f22429461fc4befb140b98a33cf3521eea282f7d/(дата обращения: 11.03.2022).

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. Ст. 115. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/b3c428e72da1062272e88f898f6d26b9c2469e4d(дата обращения: 11.03.2022).

обвинения в воспрепятствовании производству предварительного следствия.

Статья 115 УПК РФ предполагает, что нужно указывать вид обеспечиваемого имущества, сумму (эквивалент стоимости) и способ имущественного обеспечения (место хранения). В постановлении суда должен быть указан конкретный вид криптовалюты и единица ее расчета.

Криптовалюта должна обеспечиваться в денежном выражении. На практике это представляет значительную сложность, поскольку курсы большинства цифровых валют характеризуются высокой волатильностью. Для этих целей используют онлайн-биржи криптовалюты с высокой капитализацией, однако, поскольку количество таких бирж большое и каждая имеет свои котировки, за основу мы взяли данные по нескольким из них.

Большой риск значительных колебаний цены на криптовалюту приводит к тому, что в ходе судебного разбирательства стоимость изъятых единиц криптовалюты в пересчете на рубли может существенно меняться.

Поскольку суд должен описать способ имущественного обеспечения, ему потребуется указать наименование и адрес кошелька, в котором были размещены биткоины. Согласно общим правилам построения цепочек блоков адрес будет виден для всех пользователей сети. Для некоторых криптовалют к блокам можно поставить ярлык, указывающий, что они были обеспечены в рамках следствия. Можно указать также вынесший решение процессуальный орган, подписать цифровой подписью, однако все указанное требует в настоящий момент государственного регулирования. Проблема также обусловлена тем, что арест криптовалюты потребует создания специального следственного / судебного кошелька, на который будет переведена составляющая предмет обеспечения криптовалюта.

Следственные органы должны осуществлять арест по четким правилам, ведь даже малейшая ошибка может привести к необратимому упущению криптовалюты. Необходимо строго ограничивать круг лиц, которые вправе работать с устройствами, определять места хранения, способы документирования операций с использованием оборудования.

Необходимо иметь в виду, что, как и любой другой носитель информационных данных, кошелек подвергается повреждениям, в том числе системным.

Для борьбы с системными повреждениями рекомендуется использовать технологии мультиподписи, когда для совершения операции несколько ключей передаются разным лицам для совместной авторизации (например, членам следственной группы).

В перспективе возникнет вопрос: кто отвечает за технические операции в информационной системе, связанные с наложением ареста, — следователь, специалист или судья?

УПК РФ не уточняет, какой орган должен налагать арест на криптовалюту.

Представляется, что процессуальное решение по этому вопросу должен принимать суд по правилам п. 9 ч. 2 ст. 29[1] и ст. 165 УПК РФ[2], а технически исполнять это решение должен следователь с обязательным привлечением специалиста (п. 5 ст. 115 УПК РФ).

На практике возможен вариант производства обыска с изъятием компьютерной информации[3].

Сотрудники правоохранительных органов, которые осуществляют обеспечение, специалисты должны иметь теоретический и практический опыт в сфере технического функционирования виртуальных валют.

Однако в вопросах ареста криптовалюты возникает резонный вопрос: как следственным органам установить наличие криптовалюты у того или иного лица?

Фактически создается ситуация, при которой любое лицо способно держать в тайне свои криптовалютные счета, и если оно само добровольно не сообщит о наличии у него криптовалютного кошелька, то следствие не сможет установить это извне. Такие проблемы создает даже самая «открытая» криптовалюта, но каждый день появляются другие, более защищенные системы.

Однако транзакции криптовалюты не остаются полностью анонимны. Если в Сети сложно получить какую-либо информацию, то, воспользовавшись стандартным методом проверки исходящего и вхо-

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. Ст.29. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/64329d36cb8ecd39ae5eb9b05fb844d9b92d7297/ (дата обращения: 11.03.2022).

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. Ст.165. http://www.consultant.ru/document/cons_doc_LAW_34481/72239d24544cfabe7fa915829922e8b347de59a4/ (дата обращения: 11.03.2022).

[3] Литвинов А.С., Гультяев Д.О. Поймай меня, если сможешь. О вопросах ареста криптовалюты в уголовном процессе // Закон и право. 2019. №. 3. С. 155.

дящего интернет-трафика, возможно найти подозрительные IP-адреса и интернет-ресурсы, которые могут указывать на совершение тех или иных действий с криптовалютой. Добытчиков же валюты можно найти по скачкам электроэнергии, потребляемой специальным оборудованием.

Подводя итог, необходимо подчеркнуть, что в настоящее время криптовалюта стоит на пороге двух реальностей: материальной и информационной.

С одной стороны, государство лишь пытается ее урегулировать, с другой – некоторые суды уже определяют ее в те или иные отношения. В уголовном преследовании криптовалюта занимает далеко не последнее место, однако одностороннее применение судами в отношении криптовалюты тех или иных решений может привести к серьезным правовым последствиям. Поскольку криптовалюта остается деперсонифицированной, независимой единицей без какого-либо регулирования, то трудности, связанные с ее применением, должен решать именно законодатель, а не судебная система.

Криптовалюта не обеспечена реальной стоимостью, не содержит информации о ее держателях (все ее использование анонимно). Оборот криптовалюты обеспечивают организации и предприниматели, осуществляющие прием криптовалюты в качестве средства платежа за оказанные услуги или предоставленный товар, либо трейдеры, обменивающие ее на различные валюты (рубли, доллары США, евро и т.д.) на онлайн-биржах. Процесс выпуска и обращения криптовалюты полностью децентрализован и отсутствует возможность его регулирования, в том числе со стороны государства.

Фактическое нахождение криптовалюты вне правового поля регулирования обусловливает активное использование криптовалюты в торговле наркотиками, оружием, поддельными документами и в иной преступной деятельности.

Данные факты, а также возможность бесконтрольного трансграничного перевода денежных средств и их последующего обналичивая служат предпосылками высокого риска потенциального вовлечения криптовалюты в схемы, направленные на легализацию (отмывание) доходов, полученных преступным путем, финансирование терроризма.

Помимо этого, криптовалюта является способом ухода от уплаты налогов, поскольку не требует ведения специальной отчетной документации, а это, в свою очередь, способствуют росту теневой

экономики. Поэтому, на наш взгляд, вопрос о регулировании криптовалюты сохраняет свою актуальность, особенно сейчас, в период падения популярности среди обычных пользователей и, соответственно, роста внимания в криминальной сфере, как и необходимость дальнейшего ее урегулирования в будущем.

Из способов реализации мер процессуального принуждения, доступных в настоящее время следствию, необходимо выделить лишь вариант активного противодействия использованию криптовалюты. Данный механизм может быть реализован следующими способами.

1. Подписка о невыезде и надлежащем поведении

При реализации данной меры процессуального принуждения следует детализировать формулировку «иным путем не препятствовать производству по уголовному делу». При этом в ходе составления самой подписки необходимо указывать, что под препятствованием производства по уголовному делу может пониматься любое использование криптовалюты со стороны подозреваемого или обвиняемого. Самому подозреваемому (обвиняемому) необходимо разъяснить, что использование криптовалюты может быть расценено судом как попытка сокрытия доходов от совершения преступления. Информация об использовании подозреваемым (обвиняемым) криптовалюты может быть получена путем допроса свидетелей либо, при наличии данных о его криптокошелке, путем осмотра соответствующих сайтов с участием специалиста. В ходе осмотра необходимо отражать информацию о движении криптовалюты с конкретного криптокошелька[1]. В то же время самостоятельно, без участия специалиста в сфере оборота криптовалюты следователь проверить указанное не сможет. Выявление движения денежных средств с криптокошелька подозреваемого (обвиняемого) будет в таком случае нарушением подписки о невыезде и надлежащем поведении и приведет к изменению меры пресечения на более строгую. При этом с учетом того, что в рассматриваемой ситуации практически будет невозможно гарантировать, что подозреваемый (обвиняемый) не будет использовать криптовалюту при нахождении его даже на домашнем аресте (на что следует обращать внимание судов при направлении ходатайств), единственной эффективной мерой пресечения будет являться заключение лица под стражу.

[1] Blockchain. URL: https://www.blockchain.com (дата обращения: 22.03.2022).

2. Личное поручительство, наблюдение командования воинской части, присмотр за несовершеннолетним обвиняемым

Поскольку указанные меры пресечения базируются на подписке о невыезде и надлежащем поведении, избираться они могут по аналогии с ней. В то же время следует обратить внимание на следующие особенности. Так, при избрании наблюдения командования воинской части и присмотра за несовершеннолетним обвиняемым, лицам, на которых будет возложена ответственность за наблюдением (присмотром) за обвиняемым, следует разъяснять, что в их обязанности, если по уголовному делу установлено, что у обвиняемого имеется криптовалюта либо навыки ее использования, входит в том числе контроль либо запрет на использование Интернета подопечным. Выявление факта неисполнения указанного реализуется по ранее указанному способу.

3. Запрет определенных действий

Следует обратить внимание на следующую формулировку, указанную в ч. 6 ст. 105.1 УПК РФ:

Суд с учетом данных о личности подозреваемого или обвиняемого, фактических обстоятельств уголовного дела и представленных сторонами сведений при избрании меры пресечения в виде запрета определенных действий может возложить следующие запреты:

1) выходить в определенные периоды времени за пределы жилого помещения, в котором он проживает в качестве собственника, нанимателя либо на иных законных основаниях;

2) находиться в определенных местах, а также ближе установленного расстояния до определенных объектов, посещать определенные мероприятия и участвовать в них;

3) общаться с определенными лицами;

4) отправлять и получать почтово-телеграфные отправления;

5) использовать средства связи и информационно-телекоммуникационную сеть «Интернет»;

6) управлять автомобилем или иным транспортным средством, если совершенное преступление связано с нарушением правил дорожного движения и эксплуатации транспортных средств[1].

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. Ст.105.1. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/39bb7315db98bf67ba58287d2c6a202c48823d59/ (дата обращения: 22.03.2022).

Соответственно, в рамках противодействия использованию подозреваемым (обвиняемым) криптовалют, необходимо при составлении ходатайства указывать на п. 5 ч. 6 ст. 105.1 УПК РФ (использовать средства связи и информационно-телекоммуникационную сеть «Интернет»). При этом необходимо обращать внимание суда на то, что подозреваемый (обвиняемый), используя средства связи (в т.ч. Интернет), может легализовать преступные доходы через криптовалюту, даже не имея такого рода навыков. Отсутствие навыков работы с криптовалютой в настоящее время компенсируется наличием большого количества инструкций, а также различных ресурсов, представляющих услуги по приобретению криптовалюты лицам, не разбирающимся в ней. Таким образом, указанное должно быть отражено в решении суда.

4. Залог

Залог с использованием криптовалюты в настоящий момент в связи с отсутствием официальных криптокошельков у органов государственной власти невозможен. В то же время не следует исключать возможность применения указанной меры пресечения в отношении держателя криптовалюты. Так, ему при назначении данной меры пресечения судом, должен быть поставлен срок в соответствии с ч. 7 ст. 106 УПК РФ[1] на перевод криптовалюты в российские рубли и внесение их в качестве залога. При этом суду необходимо также указывать на дальнейший запрет оборота криптовалюты обвиняемым. При избрании указанной меры пресечения необходимо также обратить внимание на возможность реализации такого рода обмена лишь при представлении обвиняемым возможности присутствия стороны обвинения с участием специалиста в процессе реализации обмена криптовалюты на российские рубли и фиксации данного процесса. В случае отказа действия обвиняемого могут быть расценены как приготовление к легализации денежных средств либо их сокрытие.

Вопросы для самоконтроля

1. Могут ли быть арестованы криптовалютные активы по аналогии со стандартными денежными средствами?

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. Ст.106. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/5654e9b2d28b27133fc43779b755fcb8d8aad844/ (дата обращения: 22.03.2022).

2. Какие сведения могут указывать на совершение тех или иных действий с криптовалютой при осуществлении изучения электронных устройств и сетей методом проверки исходящего и входящего интернет-трафика?

3. Каким образом может быть реализована подписка о невыезде и надлежащем поведении в отношении держателя криптовалют?

4. Что нужно указывать в ходатайстве при избрании меры пресечения в виде запрета определенных действий в рамках противодействия использованию подозреваемым (обвиняемым) криптовалют?

5. Каким образом может быть реализован залог как мера пресечения в отношении держателя криптовалют?

ГЛАВА 5.
ПОРЯДОК ОРГАНИЗАЦИИ БЛОКИРОВКИ КРИПТОВАЛЮТЫ В РАМКАХ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ ЧЕРЕЗ LOCALBITCOINS

LocalBitcoms.com – это одноранговая биржа биткойнов со штаб-квартирой в Хельсинки (Финляндия), которая сотрудничает с правоохранительными органами через Центральную криминальную полицию Финляндии.

В отличие от традиционных бирж, которые выступают в качестве контрагента в торгах, LocalBitcoins – это одноранговая торговая площадка, аналогичная Ebay. Как одноранговая торговая площадка, LocalBitcoins не получает и не обрабатывает евро, доллары или другие официальные валюты своих клиентов, а также не покупает и не продает биткоины.

Пользователи создают объявление (для покупки или продажи биткоинов) с указанием цены и способа оплаты, приемлемым для себя, а LocalBitcoins предоставляет услуги условного депонирования, которое защищает биткоины во время торговли.

Для использования сайта клиентам необходимо зарегистрировать аккаунт. При регистрации указывается имя пользователя, адрес электронной почты и пароль. Пользователь может по желанию предоставить номер телефона, имя, фамилию и удостоверение личности с фотографией.

Кошелек LocalBitcoins работает по принципу общего кошелька, также как на большинстве других крупных биткоин-бирж. Вместо того, чтобы у каждого клиента был свой собственный биткоин-кошелек, защищенный своим личным ключом, LocalBitcoins оперирует одним биткоин-кошельком, который используется всеми пользователями. Это означает, что увидеть на биткоин-адрес в блокчейне невозможно, чтобы определить сколько биткоинов имеет определенный пользователь LocalBitcoins, эти данные хранятся только в закрытой базе данных клиентов.

Входящие и исходящие транзакции в LocalBitcoins не связаны. Когда биткоины, например, отправляются клиенту LocalBitcoins «Алисе», у которой есть адрес Y, а затем клиент «Боб» осуществляет транзакцию со своей учетной записи LocalBitcoins на адрес X, она может быть проведена с адреса Y. Если эту транзакцию проанализировать с использованием некоторых наиболее известных блокчейн-

инструментов, то результат будет показывать, что она была осуществлена «Алисой», в то время как реальным отправителем являлся «Боб». Таким образом, установить, кто именно осуществляет транзакцию, в настоящее время самостоятельно практически невозможно.

В целях наложения ареста на криптовалюты либо получения информации об их движении необходимо подготовить международный запрос, который может быть передан по каналам Интерпола.

Информационные запросы, направляемые в LocalBitcoins, должны соответствовать приведенным ниже правилам, законодательству Финляндии и направляться по надлежащим каналам. Запрос должен отвечать следующим требованиям:

1. Запрос должен быть представлен на английском, финском или шведском языке, на официальном бланке ведомства и быть подписан уполномоченным для сбора информации лицом.

2. Текст должен предоставляться в цифровом формате (Word). Сканированные документы направляются только в качестве приложений.

3. Каждый запрос должен быть конкретизирован.

4. Необходимо указать характер расследуемого преступления и номер уголовного дела.

5. Указать, где и когда совершено преступление, его краткое содержание, кто является потерпевшим и какой причинен ущерб.

6. Какое отношение объект запроса (то есть учетная запись LocalBitcoins, биткоин-кошелек или транзакция) имеет к преступлению и его участникам.

7. Каковы цели и задачи запроса.

8. Срочность исполнения запроса. Причина срочности должна быть обоснована.

9. Контактные данные исполнителя (имя, должность, организация, номер телефона, адрес электронной почты адрес, страна).

10. Контактные данные следователя (имя, должность, организация, номер телефона, адрес электронной почты, адрес, страна).

11. Детально указать информацию, которую необходимо получить. Неконкретные и пространные запросы и вопросы игнорируются и остаются без исполнения.

В случае соблюдения указанных требований и если не указано иное, LocalBitcoins информирует, что запрос принят к исполнению.

В случаях, когда наказанием за преступление является штраф, запрос обрабатывается LocalBitcoins только в случае его достаточного обоснования.

Запросы, лишенные ясности, и запросы не по существу («запрос ради запроса») компанией не обрабатываются.

Если необходима общая информация об учетной записи пользователя, запрашивающая сторона представляет страну, не являющуюся членом ЕС, направляется запрос по каналам Интерпола или SIENA.

В случае если требуются данные контента, такие как журналы чата (chat-togs), или необходим арест активов, необходимо запросить информацию в рамках Европейской конвенции о взаимной правовой помощи по уголовным делам или иных применимых мнгосторонних или двусторонних соглашений с Финляндией.

Возможно также направление запроса по дипломатическим каналам или через компетентные органы юстиции. Запросы, отправленные по почте, также должны содержать данные в электронной форме (например CD- или USB-накопитель). Печатный текст увеличивает риск опечаток и искаженной информации.

Идентификация пользователей по запросу

Запросы по персональным данным

Для идентификации предполагаемого пользователя необходимо указать:

- имя пользователя LocalBitcoins, адрес электронной почты;
- номер телефона в международном формате (общий международный телекоммуникационный план нумерации E.164);
- полное имя и дату рождения предполагаемого пользователя. Данный способ идентификации является наиболее трудоемким. Предпочтительнее указывать имя пользователя (username) или адрес электронной почты.

Запросы по биткоин-транзакциям

Чтобы таким образом идентифицировать предполагаемого пользователя, необходимо указать выходной адрес биткоина (output address) и идентификатор транзакции предполагаемого пользователя Необходимо указать в запросе, отправлялась ли интересующая транзакция пользователю LocalBitcoins или пользователем LocalBitcoins.

Запросы по биткоин-сделкам

Чтобы таким образом идентифицировать предполагаемого пользователя, необходимо предоставить идентификатор сделки и указать, запрашивается и информация в отношении покупателя, продавца или обеих сторон.

Существует семь категорий доступных для получения сведений:

- регистрационные данные,
- идентификационные данные,
- журналы учетных записей пользователей,
- информация о биткоин-кошельке,
- информация о сделках с биткоинами,
- информация о рекламных объявлениях пользователей,
- информация о торговых чатах.

Регистрационные данные содержат общую информацию об аккаунте и клиенте. Следующие данные предоставляются при запросе регистрационных данных учетной записи:

Имя пользователя - имя зарегистрированного пользователя аккаунта Localbrtcoins.com.

Полное имя - неподтвержденные имя фамилия пользователя или подтвержденные имя, фамилия, если пользователь верифицировал их удостоверением личности.

Статус проверки (верификация) - показывает, было ли проверено реальное имя пользователя.

Адрес e-mail - указанный пользователем адрес электронной почты, подтвержденный опознавательным маркером (token) направленным через e-mail.

Статус проверки e-mail показывает, была ли верифицирована электронная почта пользователя.

Номер телефона - указанный пользователем неподтвержденный или подтвержденный через смс номер телефона. Статус проверки телефонного номера показывает, был ли верифицирован номер телефона.

Дата создания учетной записи

Дата регистрации аккаунта

Последнее использование учетной записи - дата последней активности пользователя на сайте

По конкретному запросу может быть предоставлена нижеследующая информация в отношении пользователей, верифицированных по документам, удостоверяющим личность.

Идентифицирующая информация содержит сведения о документе, удостоверяющим личность пользователя, если он/она верифицировали себя на сайте с их помощью. В отношении юридических лиц идентификационные денные будут содержать документ, удостоверяющий личность законного представителя и регистрационные документы компании.

Журнал учетных записей пользователя

Некоторые действия пользователя регистрируются и заносятся в журнал учетных записей пользователя. Следующая информация может быть предоставлена по запросу:

- отметка времени по UTC (всемирное координированное время);
- имя учетной записи пользователя IP-адрес;
- действие - зарегистрированное действие, выполненное пользователем.

По конкретному запросу из пользовательских журналов может быть предоставлена следующая информация:

- пользовательский агент - браузер пользовательского агента; HTTP Accept - браузер HTTP Accept;
- LBC браузер - файл cookie-идентификации браузера LocalBitcoins.

Следующая информация может быть предоставлена по запросу об аккаунте кошелька:

- баланс биткоин-кошелька - актуальный баланс кошелька;
- список адресов-получателей - все адреса, назначенные пользователем для получения биткойн-транзакций;
- список входящих транзакций - отметка времени (UTC), адрес получателя, сумма, описание;
- список исходящих транзакций - отметка времени (UTC), адрес получателя сумма, описание.

Следующая информация может быть предоставлена по запросу о биткоин-сделках.

- ID - уникальный ID-номер, присвоенный конкретной сделке;
- дата начала сделки;
- дата, завершения сделки и отправления биткоинов покупателю;
- способ оплаты - наименование способа оплаты (только дли онлайн-торгов);
- имя пользователя покупателя - имя пользователя учетной записи LocalBitcoins, покупающего биткоины;
- имя пользователя продавца - имя пользователя учетной записи LocalBitcoins, продающего биткоины;

• сумма сделки FIAT - сумма сделки, выраженная в валюте, указанной в объявлении;

• сумма сделки - сумма сделки в биткоинах;

• биткоин-цена - цена биткоина, выраженная в валюте торговой сделки;

• валюта - трехбуквенный стандартный код ISO (Международная организация по стандартизации).

Следующая информация может быть предоставлена по запросу о рекламных объявлениях (предложениях). Ниже перечислены поля, заполняемые при составлении объявления. Не все обязательны к заполнению:

• ID-объявления - уникальный ID-номер, присвоенный конкретному предложению;

• дата создания (JTC) - дата и время создания рекламного объявления;

• корректировка (UTC) - дата и время обновления (корректировки) предложения;

• тип сделки - указывает, какой вид объявления хочет создать пользователь (например «Продажа биткоинов онлайн»);

• эквивалент цены (при совпадении спроса и предложения) - определение цены сделки исходя из почасовой рыночной цены (цена за указанный период (пиковый или непиковый) в указанный день, умноженный на коэффициент формирования по часам);

• цена, указанная в объявлении;

• валюта;

• минимальная сумма - минимальный лимит транзакций в одной сделке;

• максимальная сумма - максимальный лимит транзакций в одной сделке;

• код страны - для онлайн-торговли пользователям необходимо указывать свои страны;

• город;

• способ оплаты;

• условия сделки - условия, определенные автором объявления, и инструкции о том, как торговый партнер должен завершить сделку;

• реквизиты платежа - необязательное поле, где продавец может указать реквизиты платежа для покупателя;

• ограничения для совершающего первую сделку;

• ограничения на определенные суммы в валюте;

• требование представить полное имя покупателя;

• требование предоставить отзыв (компания использует систему отзывов, которая показывает оценку о публичном профиле. Эта оценка, выраженная в процентах, отражает количество позитивных отзывов *у* пользователи);

• требование предоставить подтверждение идентификации LBC (аббревиатура LocalBitcoins);

• требование предоставить подтверждение ID автора объявления;

• требование предоставить объем сделки;

• требование предоставить информацию об уровне доверия участника сделки (статус «проверенный пользователь»);

• требование смс-верификации;

• информация о том, когда объявление видно (определенные часы);

• объем торгов биткоинами.

Торговые биткоин-чаты

Сделки с биткоинами, совершенные на LocalBitcoins, содержат функцию чата, так что пользователи могут отправлять сообщения друг другу во время торговли. Данные чатов хранятся в течение 180 дней с момента завершения сделки или дольше, если за какой-либо из сторон сделки была замечена подозрительная активность или она является субъектом ордера на сохранение данных.

Для получения указанной информации запрос должен соответствовать положениям статьи 4 главы 10 закона Финляндии «О мерах принудительного характера», в которой указывается возможность сбора информации взамен перехвата телекомуникационных сообщений (примечание в конце инструкции).

Общие основания применения данного мероприятия указаны в статье 2 главы 10 закона[1].

К запросу должно быть приложено судебное решение или иной документ, подтверждающий полномочия на истребование такого рода сведений. При их отсутствии в исполнении запроса будет отказано.

[1] Coercive Measures Act. URL: https://finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf (дата обращения: 25.03.2022).

Предписание на сохранение данных

Если в ходе расследования было установлено, что существует риск уничтожения запрашиваемых данных или стало очевидным, что потребуется больше времени для подготовки запроса о правовой помощи, предпочтительно направить ордер на сохранение данных в соответствии с процедурой направления запроса. Согласно закону Финляндии «О мерах принудительного характера», ордер о сохранении данных выдается на три месяца и может быть при необходимости продлен. При таком запросе LocalBitcoins не информирует пользователя о сохранении его данных. Необходимо учитывать, что даже после того как пользователь запросил удаление учетной записи через сайт рассматриваемой компании, LocalBitcoins сохраняет все данные учетной записи в течение 5 лет, за исключением торговых чатов Bitcoin, которые хранятся в течение 180 дней с момента завершения сделки, если в ее отношении не действует ордер о сохранении данных либо не отмечена подозрительная активность.

Экстренные запросы

В случае возникновения чрезвычайной ситуации, связанной с неизбежным риском смерти или получения серьезных увечий, сотрудники правоохранительных органов могут направить экстренный запрос посредством электронной почты с указанием темы: «Экстренный запрос данных» по адресу datarequest@locelbitcoins.com.

В экстренных запросах должны быть четко отражены следующие позиции:

- информация, необходимая для идентификации пользователя;
- характер чрезвычайной ситуации (например, терроризм, похищение людей и т.д.);
- ФИО, подразделение, почтовый адрес, номер телефона и адрес электронной почты запрашивающего лица;
- какая именно информация требуется, почему соответствующее должностное лицо запрашивает ее и как она соотносится с расследованием.

При связи с правоохранительными органами по электронной почте LocalBitcoins отвечает только на письма с официальных доменов электронной почты правоохранительных органов.

При таком запросе в любом случае потребуется официальный запрос из ЦКП Финляндии, чтобы предоставить данные, но компания проведет предварительную проверку в отношении подозреваемого,

соберет все соответствующие данные, подготовит письмо для срочного ответа, а также сообщит в ЦКП об ожидаемом экстренном запросе.

Временная блокировка биткоин-кошелька

В случае совершения тяжкого преступлений допускается запросить LocalBitcoins о блокировке биткоин-кошелька подозреваемого. При этом в запросе требуется указать достаточную информацию о серьезности преступления и причинах блокировки кошелька. Запрос, содержащий просьбу о блокировке кошелька, не должен включать обязательство о конфиденциальности. LocalBitcoins принимает решение о необходимости блокировки кошелька в каждом конкретном случае. Если будет принято решение блокировать кошелек (необходимо, чтобы в кошельке были отправляемые биткоины), он будет заморожен на 24 дня. 24-дневный период стартует с даты, когда компания обработает запрос и уведомит ЦКП о блокировке кошелька с указанием даты ее начала. По истечении 24 дней кошелек будет разблокирован, если не будет получен официальный запрос правоохранительных органов на изъятие активов.

Вопросы для самоконтроля

1. Является ли LocalBitcoins биржей по продаже криптовалют?
2. Каким образом осуществляется торговля криптовалютой через LocalBitcoins?
3. Какие данные пользователь указать при регистрации в LocalBitcoins в обязательном порядке, а какие данные он представляет по желанию?
4. Каким образом и на каких кошельках LocalBitcoins осуществляет хранение биткойнов пользователей и как осуществляется процесс транзакции?
5. Через какие каналы направляется запрос для получения информации либо наложения ареста на криптовалюты в LocalBitcoins.
6. Какие категории сведений может представить LocalBitcoins по запросу?
7. Законодательству какой страны должны соответствовать информационные запросы, направляемые в LocalBitcoins?

ГЛАВА 6.
ВЗАИМОДЕЙСТВИЕ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ С КРИПТОВАЛЮТНЫМИ БИРЖАМИ

Криптовалютные биржи – это площадки, на которых осуществляется купля, продажа и мена криптовалют на фиатные деньги. На данный момент существуют и наиболее распространены следующие криптовалютные биржи;

– Binance;

– Huobi;

– Coinbase.

Также в России распространены следующие криптовалютные биржи, позволяющие приобретать криптовалюты за российские рубли:

– Yobit (поддерживает две национальные валюты. Вывести средства в рублях можно через платежные системы: Яндекс.Деньги, Киви-кошелек, WebMoney, платежи принимаются также через банковские карты и мобильные переводы);

– CryptoLocator (поддерживает более 9 национальных валют. Вывести средства в рублях можно через такие платежные системы, как Яндекс.Деньги, Киви-кошелек, Advcash, PayPal, Perfect Money, Neteller, WebMoney, WesternUnion, WeChat, Skrill, платежи принимаются также через банковские карты и мобильные переводы);

– EXMO (поддерживает 7 национальных валют. Вывести средства можно с помощью таких национальных валют, как Advcash, Payeer, платежи принимаются также через банковские карты, Киви-кошелек, Яндекс.Деньги, Enfins, SEPA)[1].

Самой крупной мировой биржей на данный момент является Binance. Существует немало разнящейся информации касательно данной биржи. По данным компании, средний объем торгов в сутки на данной площадке составляет около 3,8 млрд долларов[2]. Официально компания не представляет своего юридического адреса. Ввод денежных средств на счета компании с помощью банковских карт осу-

[1] Топ лучших российских бирж криптовалют. URL: https://vc.ru/finance/328030-top-luchshih-rossiyskih-birzh-kriptovalyut?comment=3580225 (дата обращения: 25.03.2022).

[2] Главные события Binance в 2020 году: поворотный момент. URL: https://binance.com/ru/blog/all/главные-события-binance-в-2020-году-поворотный-момент-421499824684901410 (дата обращения: 25.03.2022).

ществляется компанией Bifinity UAB (регистрационный номер компании: 305595206; юридический адрес: Didžioji g. 18, Вильнюс, Литва). Данный адрес может быть актуален в случае установления правоохранительными органами, что денежные средства вводились на биржу через пластиковую карту. На него могут быть направлены соответствующие запросы о перечислениях. В то же время практика взаимодействия с Bifinity UAB в данной области на момент подготовки пособия отсутствует. Напрямую Binance свои контактные данные для связи с правоохранительными органами не представляет, однако на фоне немалого количества совершенных через данную компанию преступлений, на сайты была выставлена информация о руководстве для правоохранительных органов. Данное руководство направляет к интегрированной в сайт Binance форме запроса. При этом для представления ответа компания требует от правоохранительных органов решение суда, что в целом соответствует требованиям российского законодательства. Binance также указывает на возможность сохранения доказательств по запросу от правоохранительных органов (в течение 90 суток и более при поступлении запроса о продолжении хранения). Под данным термином понимается возможность компании по запросу хранить данные о движении денежных средств по счетам Binance. Компания с учетом принятия ей международных принципов KYC и AML (принципы известности клиентов и контрагентов, существующие в сфере противодействия легализации денежных средств, полученных преступным путем и финансированию терроризма), не будет возражать против блокировки операций по запросу правоохранительных органов при наличии на то оснований.

Для направления запроса в компанию, кроме соответствующего решения суда, необходимы следующие данные:

– идентификатор транзакции (TXID);

– адрес кошелька;

– ID платежа/Memo/Тег;

– другие идентификаторы (если имеются);

– официальный электронный адрес ведомства.

К форме запроса прикрепляется сканированное решение суда и иные, имеющие отношение к делу документы.

Следует учитывать, что Binance собирает по запросу от пользователей и может представить правоохранительным органам следующую информацию:

1) адрес электронной почты;

2) название;

3) пол;

4) дату рождения;

5) домашний адрес;

6) национальность;

7) код страны;

8) другую информацию, идентифицирующую пользователя.

Кроме того, компания автоматически собирает и хранит следующие данные:

1) адрес интернет-протокола (IP), используемый для подключения компьютера пользователя к Интернету;

2) логин, адрес электронной почты, пароль и местоположение устройства или компьютера пользователя;

3) метрики Binance Services (например, возникновение технических ошибок, взаимодействие пользователя с функциями и контентом службы, а также предпочтения пользователя в настройках);

4) настройки версии и часового пояса;

5) история транзакций.

Компания Huobi ранее содержала отдельный русифицированный интернет-ресурс, однако в настоящий момент он прекратил свое существование. Было решено объединить сайт Huobi Россия с Huobi Global и продолжить работу в том числе для местных пользователей в России.

Несмотря на то, что на официальном сайте компании отсутствует информация о взаимодействии с правоохранительными органами, в политике конфиденциальности Huobi указано, что данные пользователей могут быть представлены без их согласия в соответствии с требованиями судебных разбирательств и разрешения споров или в соответствии с требованиями административных и судебных органов[1].

Также компания с учетом принятия ей международных принципов KYC и AML по аналогии с Binance может представить по запросу правоохранительных органов следующие данные:

личная информация пользователя:

1) имя, адрес;

2) дата рождения;

3) гражданство;

4) другая доступная информация;

5) действительная фотография (фотография, на которой пользователь держит документ, удостоверяющий личность, перед грудью).

[1] Политика конфиденциальности. URL: https://www.huobi.com/support/ru-ru/detail/360000298601 (дата обращения: 25.03.2022).

6) контактная информация:

7) номер телефона / мобильного телефона;

8) действующий адрес электронной почты[1].

Интернет-ресурс компании для связи содержит центр поддержки по электронному адресу: https://huobiglobal.zendesk.com/hc/en-us/requests/new?ticket_form_id=1900000015088.

По указанному адресу содержится соответствующая форма, к которой можно приложить сканированное решение суда.

Компания Coinbase (COINBASE GLOBAL, INC) – корпорация США, представляющая платформу для обмена криптовалют. Как и многие другие схожие компании, Coinbase не имеет официально зарегистрированного адреса. В то же время данная компания пользуется услугами агента The Corporation Trust Company, через которого можно направить свои претензии по адресу USA, State of Delaware, 1209 Orange Street, in the City of Wilmington, County of New Castle, Zip Code 19801[2]. При этом сама корпорация не предлагает отдельной системы взаимодействия с правоохранительными органами. В то же время в политике конфиденциальности Coinbase представляется официальная почта сотрудника по защите данных компании, которому можно обратиться, в том числе с запросом от правоохранительных органов – dpo@coinbase.com[3]. Необходимо обратить внимание, что в соответствии с пп.G п.7.1 ч.7 Пользовательского соглашения Coinbase может отказать в завершении или приостановить, заблокировать, отменить санкционированную пользователем транзакцию (даже после того, как средства были списаны со счета Coinbase), приостановить, ограничить или прекратить доступ пользователя к любым или всем услугам Coinbase, деактивировать или аннулировать учетную запись Coinbase в случае, если она является предметом любого незавершенного судебного разбирательства, расследования или иного государственного разбирательства[4]. Необходимо обратить внимание, что компания в

---

[1] Руководство пользователя Huobi по борьбе с отмыванием денег и финансированием терроризма . URL: https://www.huobi.com/support/ru-ru/detail/360000121402 (дата обращения: 25.03.2022).

[2] Amended and restated certificate of incorporation of Coinbase global, Inc. URL: https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/exhibit31-sx1.htm (дата обращения: 25.03.2022).

[3] Coinbase Global Privacy Police. URL: https://www.coinbase.com/legal/privacy (дата обращения: 25.03.2022).

[4] Coinbase User Agreement. URL: https://www.coinbase.com/legal/user_agreement/kenya (дата обращения: 25.03.2022).

соответствии с указанным Пользовательским соглашением собирает в свои базы следующие данные о пользователях:

– личная идентификационная информация: полное имя, дата рождения, национальность, пол, подпись, счета за коммунальные услуги, фотографии, номер телефона, домашний адрес и/или адрес электронной почты;

– официальная идентификационная информация: выданный государственным органом документ, удостоверяющий личность, такой как паспорт, водительские права, национальное удостоверение личности, удостоверение личности штата, идентификационный номер налогоплательщика, номер паспорта, данные водительских прав, данные национального удостоверения личности, информация о визе и/или любая другая информация, которая будет сочтена необходимой для соблюдения юридических обязательств компании в соответствии с законодательством;

– институциональная информация: идентификационный номер работодателя (или аналогичный номер, выданный правительством), подтверждение юридического образования (например, устав), личная идентификационная информация для всех существенных бенефициарных владельцев;

– финансовая информация: информация о банковском счете, основной номер счета платежной карты (PAN), история транзакций, торговые данные и/или налоговая идентификация;

– информация о транзакции: информация о транзакциях, которые клиент совершает в сервисах компании, такая, как имя получателя, имя пользователя, сумма, отметка о времени;

– информация о занятости: местонахождение офиса, должность и/или описание должности;

– переписка: ответы на опросы, информация, предоставленная группе поддержки компании или исследовательской группе пользователей;

– аудио, электронная, визуальная и подобная информация, такая как звонки и видеозаписи внутри сервиса;

– онлайн-идентификаторы: сведения о географическом местоположении, данные браузера, операционная система, личные IP-адреса;

– данные об использовании: данные аутентификации, контрольные вопросы, данные о кликах, общедоступные публикации в соци-

альных сетях и другие данные, собранные с помощью файлов cookie и аналогичных технологий[1].

Yobit – криптовалютная биржа, имеющая достаточно высокую популярность за счет низких требований к пользователю и высокого уровня конфиденциальности. Компания зарегистрирована в Панаме в закрытой юрисдикции, что позволяет сохранять безопасность средств и данных пользователей (YoBiCrypto Corp., 0801−3254 Panama City, Plaza 2000 Tower, Calle 50 Panamá)[2]. Указанный адрес в данный момент является единственным средством связи с компанией. В то же время проверка данного адреса через навигационные и справочные системы показала отсутствие офисов компании Yobit по указанному адресу. На официальном сайте компания гарантирует безопасность сделок, но не придерживается политики борьбы с отмыванием денег и финансированием терроризма. Таким образом, направление запроса и прямое взаимодействие с компанией правоохранительными и судебными органами практически невозможно. Следует отметить, что интернет-ресурс Yobit пользуется достаточно мощной защитой и информация о его успешных взломах отсутствует. Таким образом, работа с пользователем криптовалютного счета в данной компании возможна только напрямую, то есть при наличии его реальных данных. В самой компании таких данных нет.

Еще одна распространенная в России биржа – CryptoLocator. Исходя из опубликованной на официальном сайте компании политики AML/KYC, относящейся к национальным и международным нормам по предотвращению преступной деятельности и отмывания денег, а также финансирования терроризма, данная компания носит официальное название Crypto Technologies LTD и зарегистрирована в Республике Сейшельские острова, компания №: 215792, зарегистрированный офис расположен по адресу: Suite 1, Second Floor, Sound & Vision House, Francis Rachel Str., Victoria, Mahe, Seychelles[3].

Компания достаточно серьезно относится к безопасности проводимых сделок, в связи с чем информирует о том, что будет приостанавливать или прекращать действие любой учетной записи на вебсайте в любое время, если посчитает, что есть разумные основания

---

[1] Coinbase User Agreement. URL: https://www.coinbase.com/legal/user_agreement/kenya (дата обращения: 01.03.2022).

[2] YoBit 2020: Обзор криптовалютной биржи. URL: https://ru.ihodl.com/analytics/2020-05-21/yobit-2020-obzor-kriptovalyutnoj-birzhi/ (дата обращения: 25.03.2022).

[3] AML / KYC Policy. URL: https://cryptolocator.com/en/pages/aml_kyc. (дата обращения: 25.03.2022).

для того, чтобы сделать это по закону или для выполнения рекомендаций, выпущенных соответствующим государственным органом или признанным органом для предотвращения финансового преступления. CryptoLocator категорически запрещает использовать аккаунт пользователя в любых незаконных целях и обязуется сообщать о любой подозрительной деятельности в соответствующие правоохранительные органы. Нестандартным для такого рода компаний предупреждением является то, что она оставляет за собой право немедленно заморозить средства и учетную запись пользователя на веб-сайте в любое время, если он будет осуществлять деятельность по смешиванию криптовалюты на сайте компании, что означает деятельность, когда пользователи вносят украденные средства на платформу или на биржу, чтобы криптовалюта смешивалась в кошельках биржи, а затем отправляет на другую биржу, чтобы не отслеживать кошельки[1].

При подготовке запроса в компанию следует обратить внимание на то, что в соответствии с политикой конфиденциальности компания удаляет данные своих клиентов через 14 дней после последнего посещения сайта (и отсутствия активности соответственно). В то же время отдельные данные, в основном хранящиеся на серверах компании в журналах активности пользователей, могут не удаляться до 12 месяцев. Также в соответствии с политикой конфиденциальности личные данные пользователя компания удаляет через пять лет после удаления его аккаунта[2].

Несмотря на это, систем связи для правоохранительных органов на сайте компании не предусмотрено. Существует лишь система службы поддержки, через которую в разделе «Другое» имеется возможность направить необходимые материалы и прикрепить отсканированные решения суда. Данный раздел находится по интернет-адресу: https://cryptolocator.com/ru/support/request.

Компания EXMO также достаточно популярна в России. Исходя из данных официального сайта компании, а также ряде других интернет-ресурсов о компании, EXMO имеет офисы в Москве, Киеве. В то же время установить место расположения указанных офисов не представляется возможным. Сама компания указывает следующие кон-

[1] Cryptolocator general terms of use. URL: https://cryptolocator.com/ru/pages/terms_of_use (дата обращения: 25.03.2022).

[2] Privacy policy. URL: https://cryptolocator.com/ru/pages/privacy_policy (дата обращения: 25.03.2022).

тактные данные для связи: England, London, 2 Kingdom Street, W2 6JP[1].

Данный адрес также определяется на электронных картах сервисов Google Карты и Google Планета Земля как офис данной компании.

Контактные данные компании в Литовской Республике в соответствии с опубликованной на сайте лицензией EXMO: Литовская Республика, г. Вильнюс, Гирулиу г. 10-201[2].

В соответствии с пользовательским соглашением компания EXMO может передавать персональные данные своих пользователей правоохранительным органам, а также иным государственным органам в случаях если:

- указанное требуется в соответствии с действующим законодательством;
- передача данных требуется в принудительном порядке на основании повестки в суд, постановления или решения суда или иной юридической процедуры;
- сама компания примет решение, что такое раскрытие необходимо для предотвращения убытков или финансовых потерь;
- раскрытие необходимо для сообщения о предполагаемой незаконной деятельности;
- раскрытие необходимо для расследования нарушений соглашения с клиентом или любого применимого закона[3].

Необходимо обратить внимание, что, согласно информации на официальном сайте, EXMO не принимает клиентов из спорных территорий, так как они не предоставляют общепризнанных официальных документов, т.е. паспортов, выданных Российской Федерацией в Крыму, и паспортов, выданных жителям Донецкой Народной Республики и Луганской Народной Республики. Таким образом, граждане, проживающие на данных территориях, могут быть зарегистрированы на сайте компании только с использованием чужих либо подложных документов[4].

---

[1] Контакты. URL: https://info.exmo.me/ru/contacts/.(дата обращения: 01.03.2022).

[2] Lietuvos Respublikos Juridinių asmenų registro išplėstinis išrašas. URL: https://info.exmo.me/wp-content/uploads/2021/09/UAB-Exmo-Exchange-Registre-Extract.pdf (дата обращения: 25.03.2022).

[3] Пользовательское соглашение. URL: https://info.exmo.me/ru/user-agreement/ (дата обращения: 25.03.2022).

[4] Политика по предотвращению легализации доходов, добытых преступным путем, финансирования терроризма и Политика «Знай своего клиента». URL:https://info.exmo.me/ru/aml-ctf-kyc-policy/ (дата обращения: 25.03.2022).

Вопросы для самоконтроля

1. Какие криптовалютные биржи наиболее распространены в мире? Какие биржи рассматриваемого типа пользуются популярностью в России?

2. Какое отношение к Binance имеет компания Bifinity UAB? В какой стране зарегистрирована данная компания?

3. В течение какого срока Binance обеспечивает возможность сохранения доказательств при поступлении запроса от правоохранительных органов?

4. Что подразумевается под международными принципами KYC и AML?

5. Какие данные необходимо представить Binance при направлении запроса от правоохранительных органов, кроме соответствующего решения суда?

6. Могут ли в соответствии с политикой конфиденциальности Huobi быть представлены личные данные пользователя по запросу правоохранительных органов?

7. Услугами какого американского агента (трастовой компании) пользуется биржа Coinbase? В каком штате располагается данный агент?

8. В какой стране зарегистрирована компания Yobit?

9. Осуществляется ли Yobit взаимодействие с правоохранительными органами?

10. В какой стране зарегистрирована компания CryptoLocator?

11. В каких странах расположены официальные офисы компании EXMO?

ГЛАВА 7.
ОБЗОР СУДЕБНОЙ ПРАКТИКИ ПО УГОЛОВНЫМ ДЕЛАМ В ОТНОШЕНИИ КРИПТОВАЛЮТ И ДРУГИХ ВИРТУАЛЬНЫХ АКТИВОВ

Согласно позиции ученых, самое распространенное преступление в России с использованием криптовалют на данный момент - незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества[1]. При приобретении или сбыте наркотиков в большинстве случаев наркоторговцы применяют криптовалюту. Указанное находит свое отражение лишь в описательно-мотивировочной части приговоров и существенно не влияет на окончательный приговор. В то же время сегодня начинает складываться и иная практика. Так, при рассмотрении дел о наркоторговле, когда перевод денежных средств осуществляется через криптовалюту, лица, привлекаемые к ответственности за указанное, привлекаются и за легализацию преступных доходов.

В качестве примера следует рассмотреть часть решения Новотроицкого городского суда Оренбургской области по делу № 1-259/2019[2].

Подсудимый Ю.А. Волков, действуя в составе организованной группы, дважды покушался на незаконный сбыт наркотических средств с использованием информационно-телекоммуникационных сетей (Интернет) в крупном размере, а также, действуя в составе организованной группы, 16 раз покушался на незаконный сбыт нарко-

[1] Иванцов С. В. и др. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции //Всероссийский криминологический журнал. – 2019. Т. 13. №. 1. С. 85-93.

[2] Приговор № 1-259/2019 от 17.07.2019 по делу № 1-259/2019 /Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/suiBk1nZskZh/?regular-txt=%E2%84%96+1-259%2F2019&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=%D0%9D%D0%BE%D0%B2%D0%BE%D1%82%D1%80%D0%BE%D0%B8%D1%86%D0%BA%D0%B8%D0%B9+%D0%B3%D0%BE%D1%80%D0%BE%D0%B4%D1%81%D0%BA%D0%BE%D0%B9+%D1%81%D1%83%D0%B4+%28%D0%9E%D1%80%D0%B5%D0%BD%D0%B1%D1%83%D1%80%D0%B3%D1%81%D0%BA%D0%B0%D1%8F+%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D1%8C%29&regular-judge=&_=1661246646035 (дата обращения: 25.03.2022).

тических средств с использованием информационно-телекоммуникационных сетей (Интернет) в значительном размере и совершил финансовые операции с денежными средствами, приобретенными в результате совершения им преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами.

Так, Ю.А. Волков в период с сентября 2018 года по 3 декабря 2018 года, находясь на территории г. Новотроицка Оренбургской области, действуя незаконно, умышленно, из корыстных побуждений, с целью незаконного обогащения, разработал преступную схему легализации (отмывания) наркодоходов, путем совершения последовательных финансовых операций, направленных на сокрытие и маскировку источника их происхождения, обеспечения возможности их использования под видом собственных легальных доходов, согласно которой вознаграждение за осуществление деятельности, связанной с незаконным оборотом наркотических средств, поступали Ю.А. Волкову на различные криптовалютные адреса (неперсонифицированные мультивалютные кошельки для хранения и переводов различных криптовалют) в виде криптовалют ex.code и bitcoin (пиринговые платежные системы, использующие одноименную единицу для учета операций, при этом конфиденциальность использования криптовалюты достигается путем ограничения доступа к информации, а также отсутствием персонификации владельцев адресов), из которых Ю.А. Волков, реализуя преступный умысел, направленный на придание правомерного вида владению, пользованию и распоряжению денежными средствами, полученными от незаконного сбыта наркотических средств, с целью избежать процедуры банковского контроля, посредством сети Интернет, через онлайн-обмен переводил полученные электронные деньги в фиатные денежные средства (необеспеченные золотом и другими драгоценными металлами деньги, функционирующие как платежное средство на основе государственных законов, обязывающих принимать их по номиналу) - российские рубли на принадлежащие ему счета банковских карт.

Так, Ю.А. Волков в период с 6 сентября 2018 года по 3 декабря 2018 года, находясь на территории г. Новотроицка Оренбургской области, действуя незаконно, умышленно, заведомо зная о запрете свободного оборота наркотических средств на территории Российской Федерации, действуя в составе организованной группы с неустановленными лицами, являясь одновременно ее организатором и оператором, систематически совершал преступления в сфере незаконного

оборота наркотических средств, связанные со сбытом синтетических наркотических средств, за что в указанный период получил от совершения незаконных сбытов наркотических средств денежные средства в общей сумме не менее установленных и зафиксированных в ходе предварительного следствия – 21 352 рубля 41 копейку, конвертируемых в криптовалютах ex.code (экс.код) и bitcoin (биткоин), на различные криптовалютные адреса.

С целью придания правомерного вида владению, пользованию и распоряжению денежными средствами, полученными в результате указанной преступной деятельности, он Ю.А. Волков через различные онлайн-обменные системы электронных денег из интернет-приложений переводил полученные им денежные средства, конвертируемые в криптовалютах ex.code (экс.код) и bitcoin (биткоин) в фиатные денежные средства - российские рубли, после чего полученные денежные средства, согласно разработанному им плану, посредством информационно-телекоммуникационной сети Интернет переводил на электронное средство платежа (ООО НКО «Яндекс.Деньги»), часть которых посредством сети Интернет переводил на открытый на его имя в ПАО «Сбербанк» банковский счет, которые в последующем обналичивал посредством соответствующих указанным счетам банковской карты ПАО «Сбербанка» и карты ООО НКО «Яндекс.Деньги» и использовал их по своему усмотрению.

В результате указанных финансовых операций с денежными средствами, полученными в результате преступной деятельности, направленной на сбыт синтетических наркотических средств, Ю.А. Волков в целях придания правомерного вида владению, пользованию и распоряжению ими легализовал денежные средства на общую сумму 21 352 рубля 41 копейку, зафиксированную в ходе предварительного следствия.

Уголовное дело по обвинению Ю.А. Волкова поступило в суд с представлением заместителя прокурора г. Новотроицка Оренбургской области об особом порядке проведения судебного разбирательства.

В ходе предварительного расследования подсудимый Ю.А. Волков обратился с ходатайством о заключении досудебного соглашения о сотрудничестве. Из материалов уголовного дела следует, что процедура заключения с Ю.А. Волковым досудебного соглашения о сотрудничестве соблюдена.

Предварительное следствие по делу в отношении Волкова Ю.А., с которым было заключено досудебное соглашение о сотрудничестве, проведено с учетом требований ст. 317.4 УПК РФ.

В судебном заседании подсудимый Ю.А. Волков согласился с предъявленным обвинением, существо которого ему понятно, пояснил, что осознает характер и последствия ходатайства о постановлении приговора без проведения судебного разбирательства, заявленного им добровольно, после проведения консультации с защитником. Указал на выполнение им условий заключенного с прокурором досудебного соглашения о сотрудничестве.

Суд квалифицировал действия подсудимого Ю.А. Волкова следующим образом.

- ч. 3 ст. 30, п. «а, г» ч. 4 ст. 228.1 УК РФ (N-метилэфедрон массой 12,02 г.) как покушение на незаконный сбыт наркотического средства, совершенное с использованием информационно- телекоммуникационных сетей (сеть Интернет), организованной группой, в крупном размере;

- ч. 1 ст. 174.1 УК РФ как совершение финансовых операций с денежными средствами, приобретенными лицом в результате совершения им преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами.

По данному уголовному делу было установлено, что для совершения своих преступлений подсудимый использовал сотовый телефон марки Xiaomi Redmi 4X, системный блок марки Culer Master. На них на основании постановления Новотроицкого городского суда Оренбургской области от 23 марта 2019 года наложен арест. Данные предметы были признаны средством совершения преступлений и суд в соответствии с п. «г» ч. 1 ст. 104.1 УК РФ посчитал необходимым их конфисковать.

Арест, наложенный на ноутбук марки ASER, сотовый телефон марки Samsung модели S7, сотовый телефон марки LeEco Inside Coolpad, планшет в корпусе черного цвета китайского производства с надписью QS PASS, расчетные счета банковской карты ПАО «Сбербанк России» банковской карты АО «Газпромбанк», банковской карты ООО НКО «Яндекс Деньги» на основании постановления Новотроицкого городского суда Оренбургской области от 23 марта 2019 года, в соответствии с ч. 9 ст. 115 УПК РФ был отменен, поскольку необходимость в его сохранении отпала.

Следует обратить внимание также на следующее решение суда. Дело № 2а-218/2020[1] рассматривалось Устьянским районным судом Архангельской области 17 июля 2020 года.

Судом установлено, что прокуратурой Устьянского района Архангельской области осуществлен мониторинг сети Интернет, по результатам которого на страницах сайтов, указанных в административном иске, в сети Интернет выявлено наличие информации, распространение которой в Российской Федерации запрещено.

Информация, размещенная на данных страницах, распространяется бесплатно и содержит сведения об электронной валюте bitcoin (биткоин), представляющей собой виртуальное средство платежа и накопления, предложение об использовании данного средства платежа. Доступ к сайтам открыт для неопределенного круга лиц, не требует предварительной регистрации и пароля, возможность просмотра сайтов не ограничена, какое-либо ограничение на передачу, копирование и распространение данной информации также отсутствует, что подтверждено заинтересованным лицом.

В соответствии с ч. 1, 2 ст. 75 Конституции Российской Федерации[2] денежной единицей в Российской Федерации является рубль. Денежная эмиссия осуществляется исключительно Центральным банком Российской Федерации. Введение и эмиссия других денег в Российской Федерации не допускаются. Защита и обеспечение устойчивости рубля - основная функция Центрального банка Российской Федерации, которую он осуществляет независимо от других органов государственной власти.

В соответствии со ст. 27 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации» (далее За-

---

[1] Решение № 2А-218/2020 2А-218/2020~М-187/2020 М-187/2020 от 17.07.2020 по делу № 2А-218/2020 / Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/6LuSvc3YypZX/?regular-txt=%E2%84%96+2%D0%B0-218%2F2020&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=%D0%A3%D1%81%D1%82%D1%8C%D1%8F%D0%BD%D1%81%D0%BA%D0%B8%D0%B9+%D1%80%D0%B0%D0%B9%D0%BE%D0%BD%D0%BD%D1%8B%D0%B9+%D1%81%D1%83%D0%B4+%28%D0%90%D1%80%D1%85%D0%B0%D0%BD%D0%B3%D0%B5%D0%BB%D1%8C%D1%81%D0%BA%D0%B0%D1%8F+%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D1%8C%29&regular-judge=&_=1661246885676 (дата обращения: 25.03.2022).

[2] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). URL: http://www.consultant.ru/document/cons_doc_LAW_28399/4db010c9950baa1d07371f4a0ab352d5a0027d20/ (дата обращения: 25.03.2022).

кон о Центральном банке РФ)[1] официальной денежной единицей (валютой) Российской Федерации является рубль. Один рубль эквивалентен 100 копейкам. Введение на территории Российской Федерации других денежных единиц и выпуск денежных суррогатов запрещаются.

Согласно информации Центрального банка РФ, изложенной в письме от 04.09.2017[2], операции с криптовалютами несут в себе высокие риски как при проведении обменных операций, в том числе из-за резких колебаний обменного курса, так и в случае привлечения финансирования через ICO (Initial Coin Offering – форма привлечения инвестиций граждан в виде выпуска и продажи инвесторам новых криптовалют / токенов). Существуют также технологические риски при выпуске и обращении криптовалют и риски фиксации прав на «виртуальные валюты». Это может привести к финансовым потерям граждан и к невозможности защиты прав потребителей финансовых услуг в случае их нарушения.

Росфинмониторинг указал свою позицию, изложенную в Информационном письме от 06.02.2014 «Об использовании криптовалют»[3], процесс выпуска и обращения наиболее распространенных криптовалют полностью децентрализован и отсутствует возможность его регулирования, в том числе со стороны государства. Еще одной из ключевых особенностей использования криптовалют является анонимность пользователей таких криптовалют. Также криптовалюта не требует ведения специальной отчетной документации.

Кроме того, отсутствие в системах криптовалют контролирующего центра влечет невозможность обжалования или отмены несанкционированной транзакции, а фактическое нахождение криптовалют вне правового поля не предоставляет возможность реализации правовых механизмов обеспечения исполнения обязательств сторонами сделки. Например, если оплата произведена, но услуга или товар не получены, то гарантии возврата такого платежа отсутствуют. При

---

[1] О Центральном банке Российской Федерации (Банке России): Федеральный закон от 10.07.2002 № 86-ФЗ (ред. от 30.12.2021). URL: http://www.consultant.ru/document/cons_doc_LAW_37570/8582f82f1cd3de663ddfdf7b65e825f9145958f8/ (дата обращения: 25.03.2022).

[2] Об использовании частных «виртуальных валют» (криптовалют). Пресс-релиз/ Банк России. URL: http://www.cbr.ru/press/pr/?file=04092017_183512if2017-09-04t18_31_05.htm (дата обращения: 25.03.2022).

[3] Информационное сообщение «Об использовании криптовалют»/ Росфинмониторинг. URL: https://www.fedsfm.ru/news/957 (дата обращения: 25.03.2022).

этом криптовалюты в силу децентрализации не имеют субъекта, обеспечивающего их условную платежеспособность.

В соответствии с письмом Центробанка от 04.09.2017, большинство операций с криптовалютами совершается вне правового регулирования как Российской Федерации, так и большинства других государств. Криптовалюты не гарантируются и не обеспечиваются Банком России, выпускаются неограниченным кругом анонимных субъектов. В силу анонимного характера деятельности по выпуску криптовалют граждане и юридические лица могут быть вовлечены в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма. Согласно ст. 3 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[1], под легализацией (отмыванием) доходов, полученных преступным путем, понимается придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления. Статьями 174[2] и 174.1[3] УК РФ предусмотрена уголовная ответственность за совершение финансовых операций и других сделок с денежными средствами или иным имуществом, приобретенными в результате совершения преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом. На интернет-сайтах, осуществляющих торговлю криптовалютой, размещена информация для неопределенного круга лиц об использовании единицы платежа - биткоина. Таким образом, распространение возможности доступа с помощью информационно-телекоммуникационной сети Интернет к информации, побуждающей к использованию при совершении каких-либо сделок и финансовых операций с использованием биткоина как единицы платежа, не яв-

---

[1] О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Федеральный закон от 07.08.2001 № 115-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_32834/7f756f0b351492331efccfd82ac5f928dcf7bbea/

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Ст.174. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/4dfcfc8807c829f92212ce92efe818c4a707a3ca/ (дата обращения: 25.03.2022).

[3] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Ст.174.1 URL: http://www.consultant.ru/document/cons_doc_LAW_10699/c10431f048782e9c62eecc5a90fc102ac7d0e812/ (дата обращения: 25.03.2022).

ляющейся официальной денежной единицей Российской Федерации, а также порядок ее приобретения и майнинга (создания) является распространением запрещенной информации.

В то же время, как это был указано, данная ситуация была отрегулирована Федеральным законом от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[1]. Таким образом, криптовалюта была выведена из разряда запрещенной информации. В настоящее время криптовалюта, имеющая статус цифровой валюты, а также доход с нее подлежит обязательному декларированию в ФНС России.

Вопросы для самоконтроля

1. Какое самое распространенное преступление в России с использованием криптовалют?

2. Какое решение принял Новотроицкий городской суд Оренбургской области в отношении изъятых у подсудимого Ю.А. Волкова сотового телефона марки Xiaomi Redmi 4X и системного блока марки Culer Master? Чем были признаны данные предметы?

3. Какую точку зрения указал Центральный Банк России в отношении торговли криптовалютами 04.09.2017?

4. Что указывал Росфинмониторинг в информационном письме от 06.02.2014 «Об использовании криптовалют»?

5. Как изменилась ситуация с криптовалютой в соответствии с Федеральным законом от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»?

[1] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_358753/(дата обращения: 25.03.2022).

ЗАКЛЮЧЕНИЕ

В пособии продемонстрированы возможности, которыми располагают в настоящее время правоохранительные органы по противодействию преступному использованию криптовалюты. Многие криптовалютные биржи готовы представлять правоохранителям достаточно большое количество данных о своих пользователях и блокировать их счета при получении соответствующих запросов от органов правопорядка либо суда. Кроме того, существуют и иные способы уголовно-процессуального воздействия на держателей криптовалют. Это указывает на перспективы организации работы государственных органов по контролю за оборотом полученных преступным путем денежных средств.

Необходимо отдельно обратить внимание на то, что в связи с динамично меняющейся ситуацией вокруг криптовалют данное пособие является актуальным на момент его издания. Российская Федерация и другие страны предпринимали и продолжают предпринимать все возможные меры по контролю цифровых валют. Прослеживаются положительные перспективы противодействия преступному использованию криптовалют в России и в мире.

ПРАКТИЧЕСКИЕ ЗАДАЧИ

1. В ходе патрулирования парковой зоны сотрудники ППС обнаружили человека, который прятал закладку с наркотическими веществами. Указанное лицо было задержано, ему предъявлено обвинение по ч. 1 ст. 228.1 УК РФ. В ходе следствия установлено, что денежные средства, вырученные в ходе наркоторговли, данное лицо выводило с криптовалютного кошелька на банковский счет.

Составьте план следственных действий, которые необходимо провести для возбуждения уголовного дела по ч. 1 ст. 174.1 УК РФ как совершение финансовых операций с денежными средствами, приобретенными лицом в результате совершения им преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами.

2. Составьте протокол принятия устного заявления по факту хищения у гражданина Абова А.А. криптовалюты биткоин с криптовалютного кошелька blockchain.com. Хищение осуществлено получением доступа к приватному ключу злоумышленником путем обмана Абова А.А. через электронную почту (Абов А.А. направил ключ по электронной почте).

Какие вопросы должны быть заданы Абову А.А. по данному преступлению? Какая информация в данной ситуации представляет особую важность? Составьте объяснение Абова А.А.

3. В целях хищения криптовалюты биткоин Бэбов Б.Б. украл из сумки Гэгова Г.Г. Ledger Nano S. После этого Бэбов Б.Б. перевел с криптовалютного кошелька Гэгова Г.Г. 1,2 биткоина на свой криптовалютный кошелек. В дальнейшем Бэбов Б.Б. продал указанную криптовалюту и вырученные деньги перевел себе на Яндекс.Деньги. Каким образом квалифицируется данное деяние?

Как устанавливается размер причиненного ущерба? Что бы изменилось, если бы Бэбов Б.Б. не стал бы переводить с кошелька Гэгова Г.Г. 1,2 биткоина, а просто оставил бы Ledger Nano S Гэгова Г.Г. у себя до изменения курса криптовалют. Вынесите постановление о возбуждении уголовного дела по данному факту.

4. Фабула: В ходе проверки сообщения о совершении мошенничества, оперуполномоченный получил объяснение от гр. Бэбова Б.Б., который сообщил, что преступление было совершено

с использованием криптовалюты. Так, согласно показаниям Бэбова Б.Б., Гэгов Г.Г., в отношении которого осуществлялась проверка по факту мошенничества в отношении Абова А.А., все похищенные денежные средства переводил на криптовалютный кошелек. Оперуполномоченный направил полученные материалы для рассмотрения вопроса о возбуждении уголовного дела в следственную часть УМВД России по г. Энску, однако следователь направил материалы обратно для проведения дополнительных проверочных мероприятий. Так, следователь указал, что необходимо представить подтверждающие материалы о том, существует ли в действительности указанный Бэбовы Б.Б. криптовалютный кошелек.

Задание: Составьте объяснение от имени Бэбова Б.Б. об использовании Грэговым Г.Г. криптовалютного кошелька. Каким образом оперуполномоченный может выполнить в ходе проверки сообщения о преступлении указанные следователем задание?

5. Фабула: Гражданином Абовым А.А. была создана организация, основной целью которой был сбор денежных средств с граждан и осуществление постепенных выплат за счет собранных денежных средств. По данному факту оперативными сотрудникам была организована проверка. В ходе проверки Абов А.А. дал объяснение о том, что с собранных денежных средств он получает доход на криптовалютной бирже Binance, и с этих денег осуществляет выплаты.

Задание: Каким образом осуществить проверку указанной информации? Составьте рапорт о выявлении признаков преступления, включив в него информацию об опровержении позиции Абова А.А.

6. Фабула: В дежурную часть поступило заявление от гр. Абова А.А. о том, что у него похитили денежные средства на сумму 200 000 руб. В заявлении Абов А.А. указал, что денежные средства он перевел на свой криптовалютный кошелек и произвел оплату автомобиля ВАЗ 2114, который находился на момент перевода денег в другом городе. Продавцом, согласно показаниям Абова А.А., являлся Бэбов Б.Б. Он должен был доставить указанный автомобиль после ремонта. Продавец запросил перевести деньги в криптовалюте. После перевода денег продавец на связь не выходил. Абов А.А. представил данные с распечаткой сведений о транзакции с сайта LocalBitcoins, указав, что кошельки, указанные в распечатке, принадлежат Абову А.А. и Бэбову Б.Б.

Задание: проведите анализ поступившей информации. Какие материалы необходимо собрать для возбуждения уголовного дела? Какие первоначальные оперативно-розыскные мероприятия необходимо провести? Подготовьте перечень вопросов, которые необходимо задать Абову А.А.

7. Фабула: В отношении обвиняемого в мошенничестве Абова А.А. принято решение об избрании меры пресечения в виде запрета определенных действий. Имеется информация о том, что у Абова А.А. часть похищенных денежных средств может храниться на криптовалютной бирже Binance.

Задание: Каким образом должна быть организована работа по избранию данной меры пресечения? Какие еще меры пресечения могут быть избраны?

ТЕСТОВЫЕ ЗАДАНИЯ

1. Правоприменительная практика сформировала подход, при котором криптовалюта получила статус

а) иного имущества.

б) денежного суррогата.

в) электронных денег.

г) нематериального финансового актива.

2. Цифровые активы по факту признаны

а) законным имуществом для целей налогообложения и учета при расчетах с кредиторами в процедурах банкротства.

б) законным имуществом для совершения сделок с ним в любой форме.

в) незаконным имуществом.

г) несуществующим объектом.

3. Криминальное использование виртуальной валюты объясняется:

а) всеобщей доступностью и отсутствием ее регуляторов.

б) ее технологическими особенностями и трудностями квалификации преступлений.

в) скоростью транзакций криптовалют.

г) возможностями быстрого сокрытия доходов, полученных при совершении преступлений.

4. В соответствии с постановлением Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений п. 1 примечаний к ст. 158 УК РФ и ст. 128 ГК РФ содеянное должно рассматриваться как:

а) присвоение или растрата чужого имущества.

б) гражданско-правовые отношения.

в) хищение чужого имущества.

г) утрата прав на имущество либо его утеря.

5. Наиболее частые преступления, связанные с майнингом криптовалют – это

а) наркопреступления.

б) хищение ключей от криптокошельков;

в) хищение средств в криптовалюте под видом совершения законных сделок.

г) мошенничества при купле-продаже ферм и их комплектующих.

6. Следует ли считать явку с повинной о совершении хищений электронных денежных средств достаточным для возбуждения уголовного дела?

а) Да, при установлении факта перевода денег после признания.

б) Да, при наличии данных о потерпевшем и подаче им заявления.

в) Нет, такого хищения не предусмотрено законом.

г) Нет, такое дело может быть возбуждено только при хищении реальных денег с банковского счета.

7. Достаточно ли наличия данных в переписке соцсети «Телеграмм» наркокурьера о переводе денег в криптовалюте для возбуждения уголовного дела по легализации?

а) Да, достаточно при указанных условиях.

б) Да, но только если наркокурьер признается, что переводил деньги в криптовалюте.

в) Нет, для легализации нужно доказать получение денег с продажи наркотиков в законной форме.

г) Нет, легализация при наркоторговле невозможна в целом.

8. Возможно ли оперуполномоченному по поручению следователя произвести выемку ключей с криптовалютных кошельков у их владельца?

а) Да, но только с участием специалиста и в случае, если изъятие само по себе возможно (имеется доступ к компьютеру, известно место нахождения устройств типа Ledger и т.д.).

б) Нет, следователь должен самостоятельно производить данное следственное действие с учетом его специфики.

в) Да, может самостоятельно провести указанное.

г) Нет, выемка ключей криптовалютных кошельков невозможна.

9. Оперуполномоченный представил в материалах проверки распечатку скопированного изображения экрана с данными криптовалютного кошелька и указал в рапорте, что этот кошелек принадлежит лицу, в отношении которого ведется проверка по факту совершения мошенничества. Достаточно ли указанной информации для использования ее при возбуждении уголовного дела?

а) Да, достаточно. Она подтверждается рапортом.

б) Не в полной мере достаточно, необходимо было также представить изображение сведений о транзакциях с этого кошелька.

в) Нет, указанная информация вообще не должна рассматриваться при возбуждении уголовного дела.

г) Нет, необходимо получить объяснения от лиц, способных подтвердить принадлежность кошелька.

10. Возможно ли получить информацию об использовании криптовалют в ходе совершения преступлений путем проведения оперативно-розыскного мероприятия «Оперативный эксперимент» и приобщить полученные данные к уголовному делу?

а) Нет, для оперативного эксперимента в таком случае будет необходим криптовалютный кошелек, который невозможно легально зарегистрировать на оперативное подразделение.

б) Да, указанное вполне возможно провести.

в) Не совсем. Полученные данные не могут быть в итоге представлены следствию.

г) Да, но только если оперативный эксперимент проводится по уже возбужденному уголовному делу.

11. При осмотре изъятых в ходе обыска предметов и документов следователь обнаружил лист бумаги с записью данных криптокошелька. Что необходимо предпринять в данной ситуации?

а) Провести осмотр сайтов, представляющих доступ к криптокошелькам и проверить, подходят ли установленные данные к какому-либо из них. Установленное занести в протокол.

б) Провести допрос специалиста в области криптовалюты с предъявлением указанного листа бумаги, сформировать вопросы для экспертизы в данной области и направить лист бумаги для установления, подходит ли ключ к криптокошельку.

в) Провести следственный эксперимент с участием специалиста, в ходе которого проверить, подходят ли полученные данные к какому-либо кошельку.

г) Совместно с экспертом осмотреть и проверить сайты, на которых может быть данный кошелек.

12. В ходе допроса свидетеля по делу установлено, что подозреваемый использовал для совершения преступления криптовалюту. Что из перечисленного имеет большее значение из того, что следует уточнить у свидетеля?

а) Где подозреваемый научился пользоваться криптовалютой.

б) Что свидетель понимает под криптовалютой.

в) Какой именной криптовалютой пользовался и на каких интернет-ресурсах действовал подозреваемый.

г) Когда подозреваемый осуществлял последнюю транзакцию.

13. При производстве обыска в жилище обнаружена работающая в одной из комнат майнинговая ферма. Какие действия следует предпринять?

а) Сфотографировать и описать ферму.

б) Включить основной компьютер фермы и проверить, куда и как осуществляется майнинг.

в) Срочно выключить ферму, возможно короткое замыкание и пожар из-за перегрузки электросети.

г) Привлечь специалиста к осмотру, при необходимости с его участием отключить ферму и изъять ее для экспертизы.

14. При проверке показаний на месте обвиняемый продемонстрировал, что действительно может получать доступ к криптовалютному кошельку, с помощью которого совершалось обналичивание похищенных денег. Что следует делать далее в ходе данного следственного действия?

а) Предложить обвиняемому продемонстрировать, может ли он осуществлять транзакции с криптовалютой.

б) Записать все данные в протокол следственного действия, не давать обвиняемому совершать иных манипуляций с компьютером.

в) Предложить обвиняемому показать, как он осуществлял перевод криптовалюты в рубли.

г) Вызвать специалиста на следственное действие для подтверждения того, что действия обвиняемого соответствуют его показаниям.

15. В ходе следствия установлено, что в гараже обвиняемого в совершении мошенничества на сумму 5 000 000 руб. находится криптовалютная ферма стоимостью порядка 3 000 000 руб. Какие следственные действия необходимо провести в дальнейшем?

а) Допросить обвиняемого, действительно ли в гараже у него майнинг-ферма и как он ее использует.

б) Провести осмотр гаража, в ходе которого описать майнинг-ферму.

в) Провести проверку показаний на месте с участием обвиняемого, чтобы тот показал, как использовал майнинг-ферму.

г) Провести обыск гаража с участием специалиста. При необходимости изъять ферму и отправить ее на экспертизу.

Ключи к тестам

1-а
2-а
3-б
4-в
5-г
6-б
7-в
8-а
9-г
10-а
11-б
12-в
13-г
14-б
15-г

Перечень рекомендуемой к изучению литературы

Учебные и методические пособия

1. Гайдин А.И. Процессуальные и организационно-тактические особенности фиксации доказательственной информации, хранящейся на ресурсах сети Интернет: учебно-методическое пособие / А.И. Гайдин. – Москва: ДГСК МВД России, 2019. – 80 с.

2. Иванов Д.А. Расследование преступлений, совершенных с использованием криптовалюты: учебное пособие / Д.А. Иванов [и др.]. – Москва: Ай Пи Ар Медиа, 2021. – 80 с.

3. Коржова И.В. Юридические основы обращения криптоактивов: учеб. пособие для студ. высш. учеб. заведений / И.В. Коржова; под редакцией В.А. Северина. – Москва: Юр-ВАК, 2020 – 143 с.

Монографии и научные статьи

1. Валеев М.Т. Проблемы и перспективы лишения криптовалюты посредством уголовного наказания / М.Т. Валеев // Уголовная юстиция. – 2020. – №. 15. – С. 17 – 20.

2. Долгиева М.М. Квалификация деяний, совершаемых в сфере оборота криптовалюты / М.М. Долгиева // Вестник Восточно-Сибирского института МВД России. – 2019. – №. 1 (88). – С. 9 – 20.

3. Долгиева М.М. Проблемы квалификации преступлений, совершаемых в сфере оборота криптовалюты / М.М. Долгиева // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2019. – №. 4 (48). – С. 125 – 131.

4. Долгиева М.М. Противодействие легализации преступных доходов при использовании криптовалюты / М.М. Долгиева // Вестник Томского государственного университета. – 2019. – №. 449. – С. 231 – 218.

5. Корчагин А.Г. Криминогенная роль криптовалюты / А.Г. Корчагин, А.А. Яковенко // Юридические исследования. – 2020. – № 2. – С. 9 – 19.

6. Лошкарев А.В. Возмещение ущерба, причиненного преступлением с использованием криптовалют / А.В. Лошкарев, А.Е. Крылова // Международный журнал гуманитарных и естественных наук. – 2020. – №. 10-3. – С. 127 – 130.

7. Лошкарев А.В. К вопросу об обращении взыскания на криптовалюту и электронные денежные средства / А.В. Лошкарев, Ю.В. Кузьмичева // Международный журнал гуманитарных и естественных наук. – 2020. – №. 10-3. – С.131 – 134.

8. Максуров А.А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование: монография / А.А. Максуров. – Москва: Дашков и К°, 2020. – 198 с.

9. Максуров А.А. Криптовалюты и правовое регулирование их обращения: монография / А.А. Максуров. – 2-е изд. – Москва: Дашков и К°, 2019. – 356 с.

10. Михайлишина А.А. Правовой статус криптовалюты в РФ / А.А. Михайлишина // Вопросы российской юстиции. – 2019. – №. 1. – С. 777 – 788.

11. Надысева Э.Х. Проблемы расследования преступлений в сфере оборота криптовалют / Э.Х. Надысева // Вестник экономической безопасности. – 2019. – № 3. – С. 223 – 227.

12. Симаков А.А. Схемы преступлений с использованием криптовалюты / А.А. Симаков, В.В. Неелов // Закон и право. – 2020. – №. 5. – С. 106 – 109.

13. Степанченко А.В. К вопросу о правовой сущности криптовалюты / А.В. Степанченко // Пермский юридический альманах. – 2019. – №. 2. – С. 510 – 519.

14. Тыдыкова Н.В. Криптовалюта как предмет и средство совершения преступлений / Н.В. Тыдыкова, А.А. Коренная // Всероссийский криминологический журнал. – 2019. – Т. 13. – №. 3. – С. 408 – 415.

Учебное издание

Кузнецов Дмитрий Владимирович

УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ВОПРОСЫ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ И ДРУГИХ ВИРТУАЛЬНЫХ АКТИВОВ

Учебное пособие

Корректор М.М. Надыршина
Компьютерная верстка Е.О. Смирнова
Дизайн обложки О.В. Добрыднева
Тиражирование К.О. Фролова
Формат 60*84 1/16
Усл. печ. л. 4
Дата подписания в печать 30.06.2022
Тираж 50 экз.

Типография КЮИ МВД России
420059, г. Казань, ул. Оренбургский тракт, 130