УГОЛОВНО-ПРАВОВЫЕ НАУКИ

CRIMINAL LEGAL SCIENCES

DOI: 10.18287/2542-047X-2023-9-3-81-90

НАУЧНАЯ СТАТЬЯ

УДК 343

Дата поступления : 20.04.2023
рецензирования: 21.05.2023
принятия: 25.07.2023

Деятельность органов внутренних дел в процессе раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий (на примере криптовалютных активов)

Д. М. Фарахиев
Управление экономической безопасности и противодействия коррупции
МВД по Республике Татарстан, г. Казань, Российская Федерация
E-mail: dfarakhiev@mail.ru

Аннотация: В настоящей статье рассматриваются актуальные вопросы деятельности сотрудников органов внутренних дел в процессе раскрытия и расследования преступлений, совершаемых с криптовалютными активами. В процессе глобальной цифровизации общество перешло на применение информационно-телекоммуникационных технологий в различных сферах жизнедеятельности. Тенденция использования информационно-телекоммуникационных технологий набирает оборот и в противоправных слоях общества. Преступники все чаще используют инновационные технологии в целях совершения преступлений. В исследовании комплексному анализу подвергается понятие и особенности криптовалюты, а также наиболее распространенные преступления, посягающие на криптовалютные активы и (или) совершаемые с их использованием. Эффективность деятельности органов внутренних дел в процессе раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий (на примере криптовалютных активов), строится на организационных формах взаимодействия между подразделениями органов внутренних дел. В заключение предлагается алгоритм действий, направленных на повышение эффективности оперативно-служебной деятельности по линии борьбы с противоправным использованием информационно-коммуникационных технологий, в частности криптовалютных активов.

Ключевые слова: информационно-телекоммуникационные технологии; криптовалютные активы; криптовалютные биржы; раскрытие; расследование; органы внутренних дел; деанонимизация; подготовительные и процессуальные документы.

Цитирование. Фарахиев Д. М. Деятельность органов внутренних дел в процессе раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий (на примере криптовалютных активов) // Юридический вестник Самарского университета. 2023. Т. 9, № 3. С. 81–90. DOI: https://doi.org/10.18287/2542-047X-2023-9-3-81-90.

Информация о конфликте интересов: автор заявляет об отсутствии конфликта интересов.

Динар Минзеферович Фарахиев – оперуполномоченный Управления экономической безопасности и противодействия коррупции МВД по Республике Татарстан, 420012, Российская Федерация, г. Казань, ул. Лобачевского, 9/30.

SCIENTIFIC ARTICLE

Submitted: 20.04.2023
Revised: 21.05.2023
Accepted: 25.07.2023

Activities of internal affairs bodies in the process of detection and investigation of crimes committed with the use of information and communication technologies (on the example of cryptocurrency assets)

D. M. Farakhiev
Department of Economic Security and Anti-Corruption of the Ministry of Internal Affairs for the Republic of Tatarstan, Kazan, Russian Federation
E-mail: dfarakhiev@mail.ru

Abstract: This article discusses topical issues of the activities of employees of the internal affairs bodies in the process of disclosing and investigating crimes committed with cryptocurrency assets. In the process of global digitalization, society has switched to the use of information and telecommunication technologies in various spheres of life. The trend of using information and telecommunication technologies is gaining momentum in the illegal strata of society. Criminals are increasingly using innovative technologies to commit crimes. The study provides a comprehensive analysis of the concept and features of cryptocurrency, as well as the most common crimes that infringe on cryptocurrency assets and (or) are committed with their use. The effectiveness of the activities of internal affairs bodies in the process of detecting and investigating crimes committed using information and communication technologies (on the example of cryptocurrency assets) is based on organizational forms of interaction between departments of internal affairs bodies. In conclusion, an algorithm of actions is proposed aimed at improving the efficiency of operational activities in the fight against the illegal use of information and communication technologies, in particular, cryptocurrency assets.
Key words: information and telecommunication technologies; cryptocurrency assets; cryptocurrency exchanges; disclosure; investigation; law enforcement agencies; deanonymization; preparatory and procedural documents.
Citation. Farakhiev D. M. *Deyatel'nost' organov vnutrennikh del v protsesse raskrytiya i rassledovaniya prestuplenii, sovershaemykh s ispol'zovaniem informatsionno-kommunikatsionnykh tekhnologii (na primere kriptovalyutnykh aktivov)* [Activities of internal affairs bodies in the process of detection and investigation of crimes committed with the use of information and communication technologies (on the example of cryptocurrency assets)]. *Iuridicheskii vestnik Samarskogo universiteta* [Juridical Journal of Samara University], 2023, vol. 9, no. 3, pp. 81–90. DOI: https://doi.org/10.18287/2542-047X-2023-9-3-81-90 [in Russian].
Information about the conflict of interests: author declares no conflict of interests.

Dinar M. Farakhiev – criminal intelligence detective of the Department of Economic Security and Anti-Corruption of the Ministry of Internal Affairs for the Republic of Tatarstan, 9/30, Lobachevsky Street, Kazan, 420012, Russian Federation.

Борьба с преступлениями, которые совершаются с использованием информационно-телекоммуникационных технологий, является наиболее приоритетным направлением в деятельности органов внутренних дел [1, с. 60]. Оперативное и своевременное принятие мер по предупреждению преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, эффективно отражается на общей обстановке в стране и повышает авторитет органов внутренних дел. На наш взгляд, эффективность проводимых предупредительных мероприятий зависит от комплексного подхода к решению исследуемой проблемы.

На протяжении нескольких лет на территории России отмечается увеличение количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий (рис. 1). Число преступлений из года в год увеличивается прямо пропорционально числу пользователей сети Интернет. Как справедливо отмечает К. О. Карабеков: «Темпы роста преступности в глобальной сети Интернет являются самыми быстрыми на планете» [2, с. 25].

На основе вышеуказанного рисунка мы видим, что количество преступлений, совершенных с использованием компьютерной техники, расчетных (пластиковых) карт, сети Интернет и средств мо-

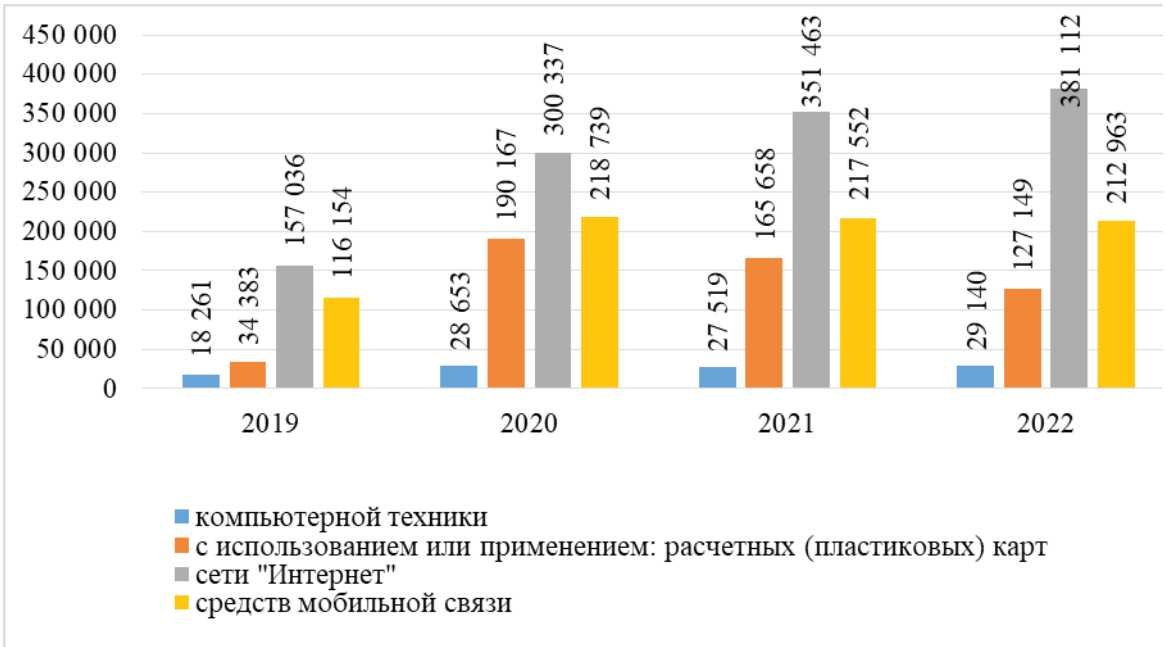

Рисунок 1 – Количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий за период времени с 2019 по 2022 г. на территории Российской Федерации
Figure 1 – Number of registered crimes committed using information and telecommunication technologies for the period from 2019 to 2022 on the territory of the Russian Federation

бильной связи за период времени с 2019 по 2022 г. увеличивается, что, в свою очередь, порождает использование цифровых финансовых активов при совершении преступлений.

Цифровые финансовые активы и криптовалюта – это новые явления в экономике и праве. Ежедневно в мире и в стране совершается множество транзакций с применением виртуальных валют. В одном из своих выступлений Президент РФ В. В. Путин справедливо заявил, что: «Прежде всего это возможность отмывания капиталов, полученных преступным путем, ухода от налогов и финансирование даже терроризма, ну и, конечно, распространение мошеннических схем, жертвами которых, безусловно, могут стать рядовые граждане» [3].

В настоящее время большое внимание государства уделяется правовому регулированию цифровых финансовых активов, в частности криптовалютных активов, что подтверждается принятием Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ № 259) [4]. Положения данного закона легализуют криптовалюту, но запрещают ее использование в России для оплаты товаров и услуг.

Следует отметить, что ФЗ № 259 не содержит в себе четкого определения «криптовалюта». В связи с чем криптовалюту можно рассматривать в качестве электронного имущества, созданного при помощи криптографических средств и учитываемого в реестре цифровых транзакций, в соответствии с закрепленными правилами его ведения. По мнению доктора юридических наук Ю. В. Гаврилина, криптовалюта представляет собой «распределенную, основанную на математических принципах пиринговую виртуальную валюту с открытым исходным кодом, при использовании которой отсутствует централизованный администратор, а также соответствующие контроль и надзор (Bitcoin, LiteCoin, Ripple) со стороны государственных органов или иных третьих лиц» [5, с. 48].

По мнению The Financial Action Task Force (далее – FATF), под виртуальной валютой следует понимать средство, которое выражает стоимость, представленное в электронном виде и выступающее в качестве средства обмена; средство хранения самой стоимости, которое не подпадает под понятие законного платежного средства [6].

По мнению АО «Лаборатория Касперского», под криптовалютой следует понимать: «Любой вид валюты в цифровой или виртуальной форме»; «Криптовалюта – это цифровая платежная система, при проверке транзакций которой не участвуют банки» [7]. Таким образом, можно сделать вывод, что под криптовалютой следует понимать разновидность платежного средства, учет которого обеспечивается децентрализованной платежной системой.

Процесс цифровизации породил появление новых способов совершения преступлений, как с использованием криптовалютных активов, так и в отношении них. Использование криптовалютных активов в процессе совершения преступлений с применением шифрования IP-адресов негативно сказывается на деятельности органов внутренних дел по выявлению, раскрытию и расследованию преступлений, в частности, совершаемых с использованием информационно-телекоммуникационных технологий, затрудняет процесс деанонимизации лиц, совершающих исследуемые преступления [8, с. 250], а также ограничивает возможность использования криптовалютных активов в качестве вещественных доказательств по уголовным делам.

В своих исследованиях Ю. В. Гаврилин рассматривает использование криптовалют в процессе совершения преступлений в сфере незаконного оборота наркотических средств, психотропных веществ или их аналогов [9]. Так, автор отмечает, что: «если до 2014 года сбыт наркотических средств осуществлялся преимущественно способом «из рук в руки», то с развитием цифровых технологий он стал осуществляться с использованием электронных торговых площадок в теневом сегменте сети Интернет (преимущественно на платформе Hydra), принимающих оплату посредством криптовалюты (обеспечивая тем самым анонимность сделок) и передающих информацию о местонахождении заранее оборудованных тайников – «закладок», в которых находятся запрещенные препараты» [5, с. 7–8].

Согласно результатам проведенного исследования – изучения материалов уголовных дел, следует, что криптовалюта активно используется при совершении следующих преступлений: ст. 158, 159, 159.4, 159.6, 161, 162, 163, 174.1, 210, 228–228.1 228.3, 229.1, 230, 272 УК РФ).

В своих исследованиях В. В. Пушкарев и А. Ю. Терехов выделяют определенную классификацию преступлений с использованием криптовалют в соответствии с различными признаками. К ним авторы относят, в частности, «1. Преступления, связанные с майнингом. 2. Преступления, связанные с обменом криптовалют и фиатных валют. 3. Кража криптовалюты. 4. Мошенничество под предлогом и/или с использованием криптовалют. 5. Мошенничество с использованием криптовалюты в информационно-телекоммуникационном пространстве. 6. Самая большая категория киберпреступлений с криптовалютами связана с хакерскими атаками на обменники криптовалют с помощью создания, использования и распространения вредоносных компьютерных программ и в дальнейшем непосредственно с кражей криптовалют или фишингом» [10, с. 123–125].

На сегодняшний день можно справедливо заявить, что криптовалютные активы все чаще фигурируют в правоприменительной практике. Одним из наиболее нашумевших дел в первой половине 2023 года является «дело Марата Тамбиева», который, по версии ГСУ СКР и надзирающей за ним Генпрокуратуры, получил от подследственных ха-

керов взятку в биткойнах, соответствующую почти $24 млн [11].

На наш взгляд, интерес со стороны общества к криптовалютным активам повышается, в результате чего увеличивается и ее популярность при совершении преступлений. Увеличение количества преступлений, совершаемых с участием криптовалютных активов, порождает проблемы у органов предварительного расследования относительно инновационных способов совершения преступлений в процессе производства следственных действий и оперативно-розыскных мероприятий [12, с. 180–181].

Проведенный анализ материалов уголовных дел о преступлениях рассматриваемой категории показал, что при их расследовании следователи сталкиваются с определенными трудностями в установлении:

а) IP-адресов, сведений о технических устройствах, с которых преступниками осуществлялся выход в сеть Интернет, фактического адреса данных лиц;

б) регистрации доменных имен на территории Российской Федерации, при которых используются хостинговые площадки операторов из-за рубежа;

в) владельцев криптокошельков, поскольку при регистрации необходимо ввести лишь адрес электронной почты и пароль к счету криптовалюты [13, с. 46].

Организационными формами взаимодействия в процессе раскрытия и расследования преступлений, совершенных с использованием криптовалютных активов, являются:

– взаимодействие и координация действий между подразделениями органов внутренних дел: следователями, оперативниками и экспертами-криминалистами;

– взаимодействие при анализе собранных сведений, полученных в рамках производства следственных действий и оперативно-розыскных мероприятий;

– составление плана расследования, в том числе производства следственных действий и оперативно-розыскных мероприятий;

– обмен значимой информацией по материалу проверки или возбужденному уголовному делу;

– разработка и внедрение в практику методических и научно-практических рекомендаций по раскрытию и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий (на примере криптовалютных активов).

Рассматривая практические аспекты раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе с использованием криптовалютных активов, необходимо рассмотреть технологии, позволяющие деанонимизировать лиц, совершающих данные преступления, а также сами криптокошельки. Так, к числу специализированных коммерческих продуктов, которые направлены на деанонимизацию криптокошельков, следует относить: Crystal Blockchain Analytics & Crypto Compliance; Chainalysis: The Blockchain Data Platform; Ciphertrace; Elliptic: Blockchain Analytics & Crypto Compliance Solutions и др. К наиболее распространенным криптовалютам на территории нашей страны относятся Bitcoin Cash, Litecoin, Zcash, Ethereum. В целях анализа данных криптовалют предлагается использовать платформу GraphSense [14, с. 105].

Все централизованные криптовалютные биржи (которых большинство на рынке) хранят средства пользователей на своих «горячих» адресах[1], проводят (в той или иной степени) процедуру идентификации своих пользователей и ведут логи (журнал) активности пользователей. Децентрализованные криптовалютные биржи не хранят средства пользователей и сами пользователи осуществляют транзакции со своих «холодных» адресов[2], при этом многие из них имеют логи активности своих пользователей. Каждая биржа имеет собственный порядок предоставления сведений, некоторые вовсе не отвечают на запросы органов государственной власти.

На основе проведенного исследования нами предлагается классификация способов получения доказательственной базы по уголовным делам:

– показания участников уголовного процесса;

– осмотр устройств, предметов и документов;

– наведение справок;

– осуществление внутреннего и внешнего взаимодействия в целях получения информации, имеющей значение для уголовного дела;

– специальное исследование информации в системе блокчейн.

При допросе участников уголовного дела мы выделяем следующие характерные черты:

– при отправке криптовалюты с биржи – максимально полно зафиксировать данные аккаунта на бирже, отразив их в протоколе;

– по возможности приложить скриншоты совершения исходящих платежей с биржи, историю пополнения средств на этой бирже;

– при отправке криптовалюты с «холодного» кошелька – отразить в протоколе, каким программным обеспечением пользовалось лицо;

– отразить в протоколе, каким образом осуществлялась транзакция (само лицо отправило активы или доступ к управлению активами был получен третьими лицами незаконно);

– зафиксировать суммы транзакций с указанием криптовалюты платежей, даты, времени, криптовалютного адреса получателя средств, а также, по возможности, указать хеш-идентификатор и криптовалютный адрес отправителя средств.

[1] Горячий адрес/кошелек – такой адрес, приватные ключи от которого хранятся у какого-то доверенного лица, не являющегося владельцем активов на адресе (например, у криптовалютной биржи или онлайн-кошелька криптовалют).

[2] Холодный адрес/кошелек – такой адрес, приватные ключи от которого (и, как следствие – право распоряжаться активами на адресе) хранятся у самого пользователя.

После допроса необходимо назначить специальное исследование, к особенностям которого следует относить следующее:

– точное указание реквизитов (криптовалютные адреса, хеш-идентификаторы транзакций и прочее);

– наличие вопросов по интересующему периоду, за который нужно изучить технологию блокчейн;

– наличие вопроса о поступлении средств на криптовалютные адреса, ассоциируемые с централизованными криптовалютными биржами;

– запрос на информацию о программном обеспечении, используемом при проведении специального исследования? и номере его лицензии;

– указание на необходимость предоставления визуализации предоставленной информации при наличии к тому технической возможности.

При составлении процессуальных документов по уголовным делам, связанным с обращением цифровых финансовых активов, в частности криптовалютных активов (на примере хищений), необходимо обращать внимание на определенные этапы и аспекты, указанные ниже (рис. 2).

Рисунок 2 – Этапы и условия при составлении процессуальных документов по уголовным делам, связанным с обращением цифровых финансовых активов

Figure 2 – Stages and conditions in the preparation of procedural documents in criminal cases related to the circulation of digital financial assets

1. В процессе принятия решения о возбуждении уголовного дела необходимо опросить лицо, у которого были похищены криптовалютные активы, и:

1.1. Определить, был ли осуществлен перевод средств преступникам с криптовалютной биржи: 1.1.1. Если да, то какой и на какие персональные данные верифицирован аккаунт потерпевшего, зафиксировав ФИО, номер телефона, наименование электронной почты, идентификатор аккаунта и прочее); 1.1.2. В случае перевода средств с внебирже-

вых кошельков необходимо установить, каким программным обеспечением пользовался потерпевший и каким образом происходила транзакция.

1.2. Задокументировать суммы транзакций с указанием криптовалюты платежей, даты, времени, криптовалютного адреса получателя, а также по возможности получить хеш-идентификатор (Txid, ID) и криптовалютный адрес отправителя средств.

1.3. Если средства были перечислены непосредственно преступникам в результате обмена, то необходимо получить информацию о том, какой обменник совершил эту транзакцию, его максимально полные данные и контакты, а также получить сведения о том, почему потерпевший обратился именно в этот обменник.

1.4. К объяснению, протоколу или иным процессуальным документам по возможности необходимо приложить скриншоты совершения исходящих платежей с биржи, историю пополнения средств на этой бирже.

1.5. В настоящий момент наиболее часто встречаются следующие криптоактивы:

1.5.1. Биткоин (Bitcoin, BTC), транзакции осуществляются в сети (блокчейне) Биткоин.

1.5.2. Эфириум (Эфир, Ethereum, Ether, ETH), транзакции осуществляются в сети (блокчейне) Эфириум.

1.5.3. Тезер (ЮСТД, Tether, USDT), транзакции чаще всего осуществляются в сети (блокчейне) Tron (TRC20, Tron Request for Comments 20, трон), но также может встречаться в сети (блокчейне) Эфириум (ERC20, Ethereum Request for Comments 20).

Важно верно указать сеть (блокчейн), в которой осуществляется транзакция, во всех оперативно-розыскных и процессуальных документах. В качестве примера предлагаем возможную формулировку, которая может быть использована в указанных документах:

Криптовалютные активы в количестве 1,2 биткоина были похищены у гр. А. с криптовалютной биржи Binance, где ранее находились у гр. А. на аккаунте ID 111, верифицированном на имя гражданина Российской Федерации – гр. А. с номером мобильного телефона +79998887766 и адресом электронной почты 111@mail.ru.

Перевод средств гр. А. осуществил путем отправки средств неустановленному лицу из личного кабинета криптовалютной биржи Binance. Перевод осуществлялся двумя транзакциями в сети Биткоин:

... на адрес … ДД.ММ.ГГ в ЧЧ.ММ.СС. в сумме 0,3 биткоина;

... на адрес … ДД.ММ.ГГ в ЧЧ.ММ.СС. в сумме 0,9 биткоина.

2. В процессе назначения специального исследования информации в системе блокчейн следует концентрироваться на конкретную и правильную описательную часть, включая постановку вопроса перед специалистом.

В описательной части запроса необходимо привести ранее полученную информацию о фактических обстоятельствах дела, имеющихся транзакциях и криптовалютных адресах.

В качестве примера предлагаем возможную формулировку описательной части:

Старший следователь ГСУ МВД по Республике Татарстан, майор юстиции ФИО, рассмотрев материалы уголовного дела № 111, возбужденного ДД.ММ.ГГ. в отношении неустановленных лиц, по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ.

Согласно материалам дела, ДД.ММ.ГГ. транзакциями с хеш-идентификаторами в сети Биткоин … у гр. А. была похищена криптовалюта в количестве 1,2 биткоина с криптовалютной биржи Binance и переведена на адрес … .

В настоящее время имеется необходимость в получении дополнительных сведений о пути перемещения средств и адресах хранения указанных средств в целях полного и всестороннего исследования обстоятельств данного уголовного дела.

В процессе формулирования вопросов, которые необходимо поставить перед специалистом, следует обращать внимание на следующие составные компоненты:

а) точно перечисленные реквизиты транзакций;

б) конкретная информация о периоде совершения транзакций (как правило, с момента совершения первого преступления по настоящее время);

в) вопрос о поступлении средств на криптовалютные адреса преступников, которые ассоциируются с централизованными криптовалютными биржами;

г) вопрос о текущем порядке взаимодействия с централизованными криптовалютными биржами, которые будут установлены в процессе исследования;

д) запрос информации о программном обеспечении, используемом при проведении специального исследования, и номере его лицензии;

е) дополнительно указать на необходимость предоставления визуализации полученной информации при наличии к тому технической возможности.

В качестве примера предлагаем возможную формулировку вопросов, которые целесообразно ставить перед специалистом:

А. Возможно ли отследить движение криптовалютных активов в сети Bitcoin, переданных транзакциями со следующими хеш-идентификаторами: … и … на адрес: …?

Если да, то какими техническими средствами и/или решениями это осуществляется, какие номера лицензий специализированного программного обеспечения используются при проведении исследования?

Б. Имеется ли техническая возможность установить и задокументировать факт поступления криптовалютных активов, изначально переданных транзакциями, указанными в вопросе № 1, на адреса централизованных криптовалютных бирж (или иных Virtual Asset Service Provider (далее – VASP) в значении, используемом межправительственной организацией с участием Российской Федерации FATF?

Если да, то на каких криптовалютных биржах (или иных VASP) в настоящий момент находятся указанные криптовалютные активы, в каком количестве и какие они имеют реквизиты идентификации внутри криптовалютных бирж (или иных VASP)?

В. В случае невозможности установления факта поступления криптовалютных активов, изначально переданных транзакциями, указанными в вопросе № 1, на адреса централизованных криптовалютных бирж (или иных VASP) полностью или в какой-то части возможно ли установление каких-либо меток (маркировок) на указанные криптовалютные активы с целью установления их последующего движения по биржам?

Г. Осуществляется ли в настоящее время взаимодействие администрации централизованных криптовалютных бирж (или иных VASP) с российскими правоохранительными органами в части замораживания криптовалютных активов и их возврата потерпевшим по уголовным делам?

Если да, то каким образом и в каких формах? Имеются ли рекомендации о порядке взаимодействия с криптовалютными биржами (или иными VASP).

Дополнительно просим предоставить визуализацию указанных сведений при наличии к тому технической возможности.

3. При наличии в исследовании информации о найденных активах на централизованных криптовалютных биржах необходимо с официальной почты ведомства (службы)[1] обратиться к администрации соответствующей централизованной криптовалютной биржи тем способом, который будет указан в специальном исследовании, с требованием временной заморозки вывода криптовалютных активов с ассоциируемых в этой бирже криптовалютных адресов. В зависимости от конкретной криптовалютной биржи может потребоваться изменение формулировок или данных. Этим же запросом следует запрашивать идентификационную и техническую информацию на лиц, связанных с использованием соответствующих аккаунтов криптовалютных бирж.

В качестве примера предлагаем возможную формулировку запроса в централизованную криптовалютную биржу:

«В производстве ГСУ МВД по Республике Татарстан находится уголовное дело № 111, возбужденное ДД.ММ.ГГ. в отношении неустановленных лиц, по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ.

Следствием установлено, что последующие транзакции с похищенной криптовалютой взаимосвязаны со следующим адресом в сети Биткоин, принадлежащим бирже Binance: … .

На основании изложенного и руководствуясь ч. 4 ст. 21 УПК РФ, просим Вас предоставить сведения об аккаунтах, которым предоставлялись указанные криптовалютные адреса, а именно: сведения о логине, телефоне, электронной почте, указанных при регистрации; копии документов, представленных в процессе верификации; информацию об IP-адресах, с которых осуществлялось обращение к указанным криптовалютным кошелькам; сведения о произведенных операциях по покупке (продаже) криптовалюты с отражением объема и наименования криптовалюты, дат совершения операций, сведений об остатках криптовалюты.

На основании вышеизложенного также просим Вас приостановить операции с криптовалютой, находящейся на вышеуказанном адресе, а также иных адресах, принадлежащих лицу или лицам, на срок до рассмотрения судом ходатайства о наложении ареста на имущество и вступления решения в силу, о чем будет сообщено дополнительно.

В настоящее время проводятся следственные действия, оперативно-розыскные и иные мероприятия, направленные на проверку финансовых операций, проведенных с использованием криптовалютных кошельков, и на установление похищенного имущества.

В связи с ограниченными сроками расследования ответ просим предоставить в кратчайшие сроки, направив на адрес служебной электронной почты: ivanov@mvd.ru».

Возможен и такой вариант запроса:

«В связи с рассмотрением материала проверки № 111 от ДД.ММ.ГГ., руководствуясь ст. 6, 13, 15 Федерального закона № 144-ФЗ «Об оперативно-розыскной деятельности» и п. 4, 10 ст. 13 Федерального закона № 3-ФЗ «О полиции», просим Вас предоставить сведения об аккаунтах, которым предоставлялись указанные криптовалютные адреса, а именно: сведения о логине, телефоне, электронной почте, указанных при регистрации; копии документов, представленных в процессе верификации; информацию об IP-адресах, с которых осуществлялось обращение к указанным криптовалютным кошелькам; сведения о произведенных операциях по покупке (продаже) криптовалюты с отражением объема и наименования криптовалюты, дат совершения операций, сведений об остатках криптовалюты.

В связи с ограниченными сроками проверки ответ просим предоставить в кратчайшие сроки, направив на адрес служебной электронной почты: ivanov@mvd.ru».

4. В случае отсутствия в исследовании информации о наличии похищенных активов на криптовалютных адресах, связанных с централизованными криптовалютными биржами, или в случае частичного нахождения средств на таких адресах, необходимо направить запрос к специалисту в целях маркировки указанных криптовалютных адресов для установления дальнейшего движения данных средств.

В качестве примера предлагаем возможную формулировку запроса к специалисту:

«В производстве ГСУ МВД по Республике Татарстан находится уголовное дело № 111, возбужденное ДД.ММ.ГГ. в отношении неустановленных

[1] К примеру, через сервис электронной почты МВД России (ivanov@mvd.ru).

лиц, по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ.

Специальным исследованием № 1 от ДД.ММ. ГГ. установлено, что похищенные транзакциями со следующими хеш-идентификаторами в сети Биткоин … и … средства, после поступления на криптовалютный адрес преступников … были в последующем распределены по криптовалютным адресам … и …, которые в настоящий момент не ассоциируются с какими-либо централизованными криптовалютными биржами.

На основании вышеизложенного просим Вас надлежащим образом маркировать указанные криптовалютные адреса и незамедлительно сообщить о движении криптовалютных активов с указанных криптовалютных адресов по электронной почте: ivanov@mvd.ru».

Другой вариант запроса:

«В рамках рассмотрения материала проверки № 111 от ДД.ММ.ГГ. проведено исследование, по результатам которого установлено, что похищенные транзакциями со следующими хеш-идентификаторами в сети Биткоин … и … средства, после поступления на криптовалютный адрес преступников … были в последующем распределены по криптовалютным адресам … и …, которые в настоящий момент не ассоциируются с какими-либо централизованными криптовалютными биржами.

Таким образом, на основании вышеизложенного, руководствуясь ст. 6, 13, 15 Федерального закона № 144-ФЗ «Об оперативно-розыскной деятельности» и п. 4, 10 ст. 13 Федерального закона № 3-ФЗ «О полиции», просим Вас надлежащим образом маркировать указанные криптовалютные адреса и незамедлительно сообщить о движении криптовалютных активов с указанных криптовалютных адресов по электронной почте: ivanov@mvd.ru».

5. В случае успешной заморозки криптовалютных активов на централизованной криптовалютной бирже необходимо подготовить постановление об аресте вышеуказанных средств.

При составлении ходатайства необходимо указывать на то, какие криптовалютные адреса на основании специального исследования были выявлены и к каким централизованным криптовалютным биржам они отнесены.

В качестве примера предлагаем возможную формулировку для включения в ходатайство:

В производстве ГСУ МВД по Республике Татарстан находится уголовное дело № 111, возбужденное ДД.ММ.ГГ. в отношении неустановленных лиц, по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ.

Следствием установлено, что похищенные средства, принадлежащие гр. А., были выведены транзакциями со следующими хеш-идентификаторами в сети Биткоин: … и … на криптовалютный адрес: … .

Специальным исследованием № 1 от ДД.ММ. ГГ. установлено, что указанные средства поступили на криптовалютный адрес: …, принадлежащий централизованной криптовалютной бирже Binance.

На основании вышеизложенного, руководствуясь положениями ст. 82, ст. 115 УПК РФ, прошу наложить арест на криптовалютные средства, находящиеся на аккаунте централизованной криптовалютной биржи Binance и ассоциированных с данным аккаунтом адресах иных криптовалютных активов указанной централизованной криптовалютной биржи и передать их гр. А.

6. Судебное постановление должно включать в себя сведения:

1) о проведенном исследовании и его результатах;

2) о хеш-идентификаторах транзакций и криптовалютных адресах преступников;

3) о конечных адресах поступления на централизованную криптовалютную биржу, где ранее были заморожены активы.

При необходимости изложить полный текст описания движения криптоактивов, которое содержится в описательной части специального исследования.

7. После подписания судебного постановления потерпевший должен самостоятельно открыть аккаунты на соответствующих централизованных криптовалютных биржах и пройти там полную верификацию. Данные такого аккаунта должны быть переданы бирже вместе с сопроводительным письмом и судебным постановлением, путем направления письма через официальную электронную почту.

В качестве примера предлагаем возможную формулировку текста для включения его в сопроводительное письмо:

В производстве ГСУ МВД по Республике Татарстан находится уголовное дело № 111, возбужденное ДД.ММ.ГГ. в отношении неустановленных лиц, по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ.

Следствием установлено, что похищенные средства, принадлежащие гр. А., были выведены транзакциями со следующими хеш-идентификаторами в сети Биткоин: … и … на криптовалютный адрес: … .

Специальным исследованием № 1 от ДД.ММ. ГГ. установлено, что указанные средства поступили на криптовалютный адрес: …, принадлежащий централизованной криптовалютной бирже Binance.

На основании вышеизложенного, направляем Вам для исполнения постановление Вахитовского районного суда г. Казани № 333 от ДД.ММ.ГГ. по уголовному делу № 111 и реквизиты аккаунта потерпевшего – гр. А. для перевода ему криптовалютных активов в количестве 1,2 биткоина.

Таким образом, подводя итог исследования, следует отметить, что повышение эффективности деятельности органов внутренних дел в борьбе с преступлениями, совершенными с использованием криптовалютных активов, является первоочередной задачей, которую необходимо решить в максимально короткие сроки. В процессе осуществления своей деятельности сотрудники следственных и оперативных подразделений должны уметь идентифицировать владельцев криптовалютных активов. В связи с чем предлагается внедрить в деятель-

ность органов внутренних дел специализированное информационно-аналитическое программное обеспечение с возможностью взаимодействия с криптовалютными биржами.

Библиографический список

1. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. Москва: Академия управления МВД России, 2019. Ч. 1. 208 с. URL: https://mvd.ru/upload/site120/folder_page/015/122/996/Gavrilin_Ch.1.pdf; https://elibrary.ru/item.asp?id=44836640. EDN: https://elibrary.ru/krepvy

2. Карабеков К. О. Актуальные вопросы исследования киберпреступности в Российской Федерации и Республике Казахстан // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2022. № 22–2. С. 25–27. URL: https://elibrary.ru/item.asp?id=47913900. EDN: https://elibrary.ru/cvocwk.

3. Путин: криптовалюты – это возможность отмывания, ухода от налогов и финансирования терроризма. URL: https://www.kommersant.ru/doc/3435054.

4. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ // Российская газета. 2020. № 173. URL: https://rg.ru/documents/2020/08/06/tsifra-dok.html.

5. Гаврилин Ю. В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях: научно-практическое пособие. Москва: Академия управления МВД России, 2021. 71 с. URL: https://mvd.ru/upload/site120/folder_page/015/122/996/O_nauchnykh_podkhodakh_k_probleme_ispolzovaniya_IT_v_prestupnykh_tselyakh.pdf; https://elibrary.ru/item.asp?id=47334085. EDN: https://elibrary.ru/hpaarh.

6. Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ. URL: https://eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf.

7. Что такое криптовалюта и как она применяется? URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cryptocurrency.

8. Фарахиев Д. М. Способы и методы деанонимизации лиц, совершающих преступления в информационном пространстве // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 249–254. DOI: https://doi.org/10.36511/2078-5356-2022-4-249-254. EDN: https://elibrary.ru/tdhqtk.

9. Гаврилин Ю. В., Бедеров И. С. Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств. Москва: Академия управления МВД России, 2022. 76 с. URL: https://xn--b1aew.xn--p1ai/upload/site120/folder_page/015/122/996/Ustanovlenie_vladeltsev_kriptovalyutnykh_koshelkov.pdf; https://elibrary.ru/item.asp?id=50054103. EDN: https://elibrary.ru/epvrvt.

10. Пушкарев В. В., Техеров А. Ю. Преступления с использованием криптовалюты: актуальные вопросы уголовного преследования // Алтайский юридический вестник. 2021. № 1(33). С. 122–127. URL: https://elibrary.ru/item.asp?id=44867699. EDN: https://elibrary.ru/sfjvlu.

11. Все, что нажито непосильной взяткой. URL: https://www.kommersant.ru/doc/6026773?tg.

12. Курилов С. И., Осипов И. В. Об актуальности организации внутреннего и внешнего взаимодействия органов предварительного следствия, дознания и экспертно-криминалистических подразделений в процессе расследования преступлений с использованием криптовалют // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации: сборник научных статей по материалам международной научно-практической конференции, Москва, 21 мая 2021 года / под ред. Ю. В. Гаврилина, Ю. В. Шпагиной. Москва: Академия управления МВД России, 2021. С. 178–186. URL: https://elibrary.ru/item.asp?id=47439467. EDN: https://elibrary.ru/ezpgei.

13. Пинкевич Т. В. Проблемы уголовно-правового противодействия преступной деятельности с использованием криптовалют // Юристъ-Правоведъ. 2020. № 4 (95). С. 45–48. URL: https://elibrary.ru/item.asp?id=44393427. EDN: https://elibrary.ru/ekolkq.

14. Гаврилин Ю. В., Бедеров И. С. Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России. 2021. № 4 (60). С. 101–108. DOI: https://doi.org/10.24412/2072-9391-2021-460-101-108. EDN: https://elibrary.ru/emalps.

References

1. *Deyatel'nost' organov vnutrennikh del po bor'be s prestupleniyami, sovershennymi s ispol'zovaniem informatsionnykh, kommunikatsionnykh i vysokikh tekhnologii: uchebnoe posobie: v 2 ch.* [Activity of the internal affairs bodies in combating crimes committed using information, communication and high technologies: textbook: in 2 parts]. Moscow: Akademiya upravleniya MVD Rossii, 2019, part 1, 208 p. Available at: https://mvd.ru/upload/site120/folder_page/015/122/996/Gavrilin_Ch.1.pdf; https://elibrary.ru/item.asp?id=44836640. EDN: https://elibrary.ru/krepvy [in Russian].

2. Karabekov K. O. *Aktual'nye voprosy issledovaniya kiberprestupnosti v Rossiiskoi Federatsii i Respublike Kazakhstan* [Topical issues of cybercrime research in the Russian Federation and the Republic of Kazakhstan]. *Aktual'nye problemy bor'by s prestupleniyami i inymi pravonarusheniyami*, 2022, no. 22-2, pp. 25–27. Available at: https://elibrary.ru/item.asp?id=47913900. EDN: https://elibrary.ru/cvocwk [in Russian].

3. *Putin: kriptovalyuty – eto vozmozhnost' otmyvaniya, ukhoda ot nalogov i finansirovaniya terrorizma* [Putin: cryptocurrencies are an opportunity for laundering, tax evasion and financing of terrorism]. Available at: https://www.kommersant.ru/doc/3435054 [in Russian].

4. *O tsifrovykh finansovykh aktivakh, tsifrovoi valyute i o vnesenii izmenenii v otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii: Federal'nyi zakon ot 31.07.2020 № 259-FZ* [On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation: Federal Law № 259-FZ as of July 31, 2020]. *Rossiiskaya gazeta*, 2020, no. 173. Available at: https://rg.ru/documents/2020/08/06/tsifra-dok.html [in Russian].

5. Gavrilin Yu. V. *O nauchnykh podkhodakh k probleme ispol'zovaniya informatsionno-telekommunikatsionnykh tekhnologii v prestupnykh tselyakh: nauchno-prakticheskoe posobie* [On scientific approaches to the problem of using information and telecommunication technologies for criminal purposes: research and practice guide]. Moscow: Akademiya upravleniya MVD Rossii, 2021, 71 p. Available at: https://mvd.ru/upload/site120/folder_page/015/122/996/O_nauchnykh_podkhodakh_k_probleme_ispolzovaniya_IT_v_prestupnykh_tselyakh.pdf; https://elibrary.ru/item.asp?id=47334085. EDN: https://elibrary.ru/hpaarh [in Russian].

6. *Virtual'nye valyuty. Klyuchevye opredeleniya i potentsial'nye riski v sfere POD/FT: otchet FATF* [Virtual currencies. Key definitions and potential AML/CFT risks: FATF report]. Available at: https://eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf [in Russian].

7. *Chto takoe kriptovalyuta i kak ona primenyaetsya?* [What is a cryptocurrency and how is it used?]. Available at: https://www.kaspersky.ru/resource-center/definitions/what-is-cryptocurrency [in Russian].

8. Farakhiev D. M. *Sposoby i metody deanonimizatsii lits, sovershayushchikh prestupleniya v informatsionnom prostranstve* [Ways and methods of deanonymization of persons committing crimes in the information space]. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii* [Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia], 2022, no. 4 (60), pp. 249–254. DOI: https://doi.org/10.36511/2078-5356-2022-4-249-254. EDN: https://elibrary.ru/tdhqtk [in Russian].

9. Gavrilin Yu. V., Bederov I. S. *Ustanovlenie vladeltsev kriptovalyutnykh koshelkov pri rassledovanii prestupleniy v sfere nezakonnogo oborota narkoticheskikh sredstv* [Establishment of the owners of cryptocurrency wallets in the investigation of crimes in the field of drug trafficking]. Moscow: Akademiya upravleniya MVD Rossii, 2022, 76 p. Available at: https://xn--b1aew.xn--p1ai/upload/site120/folder_page/015/122/996/Ustanovlenie_vladeltsev_kriptovalyutnykh_koshelkov.pdf; https://elibrary.ru/item.asp?id=50054103. EDN: https://elibrary.ru/epvrvt [in Russian].

10. Pushkarev V. V., Terekhov A. Yu. *Prestupleniya s ispol'zovaniem kriptovalyuty: aktual'nye voprosy ugolovnogo presledovaniya* [Cryptocurrency crimes: current prosecution issues]. *Altaiskii yuridicheskii vestnik* [Altai Law Journal], 2021, no. 1 (33), pp. 122–127. Available at: https://elibrary.ru/item.asp?id=44867699. EDN: https://elibrary.ru/sfjvlu [in Russian].

11. *Vse, chto nazhito neposil'noi vzyatkoi* [Everything that is acquired by an unbearable bribe]. Available at: https://www.kommersant.ru/doc/6026773?tg [in Russian].

12. Kurilov S. I., Osipov I. V. *Ob aktual'nosti organizatsii vnutrennego i vneshnego vzaimodeistviya organov predvaritel'nogo sledstviya, doznaniya i ekspertno-kriminalisticheskikh podrazdelenii v protsesse rassledovaniya prestuplenii s ispol'zovaniem kriptovalyut* [On the relevance of the organization of internal and external interaction of the preliminary investigation, inquiry and forensic units in the process of investigating crimes using cryptocurrencies]. In: *Razvitie ucheniya o protivodeistvii rassledovaniyu prestuplenii i merakh po ego preodoleniyu v usloviyakh tsifrovoi transformatsii: Sbornik nauchnykh statei po materialam mezhdunarodnoi nauchno-prakticheskoi konferentsii, Moskva, 21 maya 2021 goda. Pod red. Yu.V. Gavrilina, Yu.V. Shpaginoi* [Gavrilina Yu. V., Shpagina Yu. V. (Eds.) Development of the doctrine of counteracting the investigation of crimes and measures to overcome it in the conditions of digital transformation: Collection of scientific articles based on the materials of the international research and practical conference, Moscow, May 21, 2021]. Moscow: Akademiya upravleniya MVD Rossii, 2021, pp. 178–186. Available at: https://elibrary.ru/item.asp?id=47439467. EDN: https://elibrary.ru/ezpgei [in Russian].

13. Pinkevich T. V. *Problemy ugolovno-pravovogo protivodeistviya prestupnoi deyatel'nosti s ispol'zovaniem kriptovalyut* [Issues of the criminal-legal counteraction to criminal activity using cryptocurrency]. *Yurist"-Pravoved"* [Jurist-Pravoved], 2020, no. 4 (95), pp. 45–48. Available at: https://elibrary.ru/item.asp?id=44393427. EDN: https://elibrary.ru/ekolkq [in Russian].

14. Gavrilin Yu. V., Bederov I. S. *Ustanovlenie lichnosti vladel'tsev tsifrovoi valyuty: metodologicheskie osnovy* [Identification of digital currency owners: methodological foundations]. *Trudy Akademii upravleniya MVD Rossii* [Proceedings of the Management Academy of the Ministry of Interior of Russia], 2021, no. 4 (60), pp. 101–108. DOI: https://doi.org/10.24412/2072-9391-2021-460-101-108. EDN: https://elibrary.ru/emalps [in Russian].