Научная статья
УДК 343.352.4
DOI: 10.37973/VESTNIKKUI-2025-59-15

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ПРОТИВОДЕЙСТВИИ ВЗЯТОЧНИЧЕСТВУ, СОВЕРШАЕМОМУ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ФИНАНСОВЫХ И КРИПТОВАЛЮТНЫХ АКТИВОВ

Динар Минзеферович Фарахиев,
Академия управления МВД России, Москва, Россия,
dfarakhiev@mail.ru

Аннотация

Введение: статья посвящена изучению особенностей оперативно-розыскной деятельности органов внутренних дел в противодействии взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов.

Материалы и методы: материалами исследования послужили доктринальные положения права, посвященные оперативно-розыскной деятельности органов внутренних дел, в контексте противодействия взяточничеству. Основными источниками выступили положения, затрагивающие вопросы противодействия взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов. В процессе исследования были использованы общенаучные (анализа, дедукции, индукции) и частнонаучные (структурно-логический, диалектический, формально-юридический) методы познания.

Обзор литературы: проанализированы труды ученых в области оперативно-розыскной деятельности и криминологии, а также рассмотрены исследования, посвященные использованию информационно-телекоммуникационных технологий в противодействии взяточничеству. Наиболее значительный вклад в исследование данной проблемы внесли Х.А. Асатрян, А.П. Дмитриенко, М.Г. Жигас, В.С. Ишигеев, А.В. Куликов, А.И. Овчинников, А.Л. Репецкая и другие.

Результаты исследования: в процессе написания статьи проанализированы проблемные аспекты выявления и документирования взяточничества, совершаемого с использованием цифровых финансовых и криптовалютных активов; рассмотрены наиболее распространенные способы идентификации криптокошельков и их пользователей, которые могут быть применены сотрудниками органов внутренних дел, а также представлена схема совершения преступных транзакций, связанных со взяточничеством; определена закономерность в использовании органами внутренних дел информационно-телекоммуникационных технологий в процессе оперативно-розыскного противодействия взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов.

Обсуждение и заключение: выявлена тенденция к распространению обращения цифровых финансовых и криптовалютных активов при совершении взяточничества; предлагается авторская вариация текста запроса, подготавливаемого в адрес криптовалютной биржи в целях получения оперативно-значимой информации; сформулированы меры, направленные на повышение эффективности оперативно-розыскной деятельности органов внутренних дел в противодействии взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов.

Ключевые слова: оперативно-розыскная деятельность; органы внутренних дел; взяточничество; цифровые финансовые активы; криптовалютные активы; противодействие взяточничеству; информационно-телекоммуникационные технологии; система блокчейн

Для цитирования: Фарахиев Д.М. Оперативно-розыскная деятельность органов внутренних дел в противодействии взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов // Вестник Казанского юридического института МВД России. 2025. Т. 16. № 1 (59). С. 127 – 137. DOI: 10.37973/VESTNIKKUI-2025-59-15

Scientific article
UDC 343.352.4
DOI: 10.37973/VESTNIKKUI-2025-59-15

INVESTIGATION ACTIVITIES OF INTERNAL AFFAIRS BODIES IN THE FIGHT AGAINST BRIBERY COMMITTED USING DIGITAL FINANCIAL AND CRYPTOCURRENCY ASSETS

Dinar Minzeferovich Farahiev,
Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia,
dfarakhiev@mail.ru

Abstract

Introduction: the study covers features of investigation activities of internal affairs in countering bribery committed with the use of digital financial and cryptocurrency assets.

Materials and Methods: the doctrinal law provisions on the investigation activities of the internal affairs in the light of the fight against corruption became the study materials. Regulations on countering bribery committed with digital financial and cryptocurrency assets were the basic study sources. The author used universal (analysis, deduction, and induction) and special (structure logic, dialectical, and legal) methods of cognition.

Literature review: the author analyzed investigation and criminology scientific works, as well as considered studies on informational and telecommunication technologies in countering bribery. Thus, he came to the conclusion that H.A. Asatryan, A.P. Dmitrienko, M.G. Zhigas, V.S. Ishigeev, A.V. Kulikov, A.I. Ovchinnikov, A.L. Repetskaya and others contributed substantially to the study.

Results: the following conclusions were drawn from the research:

- The most challenging issues concerning the detection and documentation of bribery committed using digital financial and cryptocurrency assets were analysed by the author.
- The most common ways to identify crypto wallets and their users, which can be used by internal affairs bodies, were considered.
- The scheme of criminal transactions related to bribery was presented.
- The regularity in the use of information and telecommunication technologies by internal affairs bodies in combating bribery committed using digital financial and cryptocurrency assets was defined.

Discussion and Conclusions: there are signs of circulation of digital financial and cryptocurrency assets in bribery. The author presents his own variant of the inquiry for crypto platform to receive necessary information for the investigation; measures to improve investigation efficiency in internal affairs bodies when combating bribery committed with digital financial and cryptocurrency assets.

Keywords: investigative activities; internal affairs agencies; bribery; digital financial assets; cryptocurrency assets; fight against bribery; information and telecommunication technologies; blockchain system

For citation: Farahiev D.M. Investigation Activities of Internal Affairs Bodies in the Fight Against Bribery Committed Using Digital Financial and Cryptocurrency Assets. Bulletin of the Kazan Law Institute of MIA of Russia. 2025;16(1):127-137. (In Russ.). DOI: 10.37973/VESTNIKKUI-2025-59-15

Введение

Взяточничество является запрещенным уголовным законом деянием, подрывающим авторитет органов власти страны. Соответствующие антикоррупционные запреты существовали как в дореволюционные, так и в советско-российские времена. В настоящее время на территории Российской Федерации преступления коррупционной направленности представляют собой значительную проблему, затрагивающую функционирование органов государственной и муниципальной власти, правоохранительных органов, системы здравоохранения, образования и других немаловажных сфер и областей жизнедеятельности общества.

Согласно статистическим данным МВД России, за январь – декабрь 2023 года на территории страны зарегистрировано 20 279 преступлений, связанных со взяточничеством (4%), из них: получение взятки – 5 960 (7,6%), дача взятки – 5 657 (20%), посредничество во взяточничестве – 2 256 (19,9%), мелкое взяточничество – 6 406 (-12,9%).

Кроме того, следует отметить, что в России за последние два года количество судебных дел, связанных с цифровыми финансовыми и криптовалютными активами, увеличилось в пять раз: с 510 в 2021 году до 2653 в 2023 году[1]. В результате анализа статистических данных установлено, что в процентном соотношении уголовные дела составили 34%. Вместе с тем глава Федеральной службы по финансовому мониторингу Российской Федерации (далее – Росфинмониторинг) Ю.А. Чиханчин заявил, что «криптовалютой активно пользуются … коррупционеры»[2].

Общественная опасность взяточничества проявляется в деформации деятельности должностных лиц органов власти, нарушении законных прав и интересов граждан и организаций. Следует отметить, что взяточничество играет роль извращенного неправомерного стимула в служебной деятельности [1, с. 84] в целях получения незаконного вознаграждения и улучшения материального состояния и положения должностных лиц.

Согласно постановлению Пленума Верховного Суда Российской Федерации: «Получение и дача взятки, а равно незаконного вознаграждения при коммерческом подкупе считаются оконченными с момента принятия должностным лицом либо лицом, выполняющим управленческие функции в коммерческой или иной организации, хотя бы части передаваемых ему ценностей (например, с момента передачи их лично должностному лицу, зачисления с согласия должностного лица на указанный им счет, «электронный кошелек»). При этом не имеет значения, получили ли указанные лица реальную возможность пользоваться или распоряжаться переданными им ценностями по своему усмотрению»[3].

Сферами, наиболее подверженными коррупции, в том числе взяточничеству, являются медицина, образование, кадастровая деятельность, строительство, жилищно-коммунальное хозяйство. Вышеперечисленные направления профессиональной деятельности широко распространены в России и пользуются наибольшим спросом у общества, а также соприкасаются с иными общественными сферами, в которых имеются коррупционные проявления.

В настоящее время в условиях цифровизации финансовые средства, как правило, обращаются в безналичной форме, что, в свою очередь, актуализирует вопросы использования цифровых финансовых активов, цифровой валюты и криптовалютных активов в качестве предмета взяточничества, что непосредственно влияет на эффективность противодействия исследуемым видам преступлений.

Обзор литературы

Изучены научные труды профессоров В.С. Ишигеева [1] и М.Г. Жигас [2], А.П. Дмитриенко [3], А.Л. Репецкой [4], Х.А. Асатряна [5] и иных авторов, занимавшихся исследованием вопросов использования информационно-телекоммуникационных технологий в противодействии взяточничеству.

Вместе с тем мы согласны с мнением авторов, считающих, что криптовалютные активы являются наиболее распространенными видами валют, обладающими преимуществом анонимности при использовании их в качестве предмета преступления [3, с. 52; 6, с. 160; 7, с. 36]. Общественная опасность взяточничества увеличивается, когда предметом взятки выступают криптовалютные активы [8, с. 15-16]. В настоящее время представляется, что тенденция к цифровизации коррумпированных «сервисов» – это реальность «ближайшего будущего» [4, с. 67].

Материалы и методы

Методологическую основу исследования составили диалектический и структурно-логический методы научного познания. В процессе исследования автором использовались методы сравнения, анализа, дедукции и индукции. Эмпирической основой исследования послужили материалы уголовных дел и правоприменительной практики по преступлениям, предусмотренным ст. 290-291[2] УК РФ, совершаемым с использованием цифровых финансовых и криптовалютных активов.

Результаты исследования

Цифровые финансовые и криптовалютные активы – это новые явления в экономике и праве. В настоящее время государство уделяет значительное внимание 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 за-

[1] Состояние преступности на территории Российской Федерации. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 05.09.2024).

[2] Росфинмониторинг: число операций с криптовалютой с начала года увеличилось втрое. URL: https://www.vedomosti.ru/finance/news/2023/11/01/1003641-rosfinmonitoring (дата обращения: 05.09.2024).

[3] О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях: постановление Пленума Верховного Суда РФ от 09.07.2013 № 24 // Российская газета. 2013. № 154.

конодательные акты Российской Федерации» (далее – ФЗ № 259)[1]. Положения данного закона легализуют криптовалютные активы, но запрещают их использование в России для оплаты товаров и оказанных услуг.

В 2022 году Банк России предложил запретить выпуск, обращение и обмен криптовалютных активов, а также организацию данных операций на территории нашей страны. Помимо прочего, Банк России предлагает привлекать к ответственности лиц, нарушающих запрет на использование криптовалютных активов в качестве средства платежа[2]. В свою очередь, Министерство финансов России (далее – Минфин России) подготовило концепцию регулирования криптовалютных активов в России без их запрета: ведомство предлагает проводить все операции с криптовалютными активами через российские банки, идентифицировать держателей криптокошельков и разделять клиентов на квалифицированных и неквалифицированных инвесторов[3]. Концепцию Минфина России поддержал Росфинмониторинг[4].

Необходимо принимать во внимание, что биржи разграничиваются на централизованные и децентрализованные. Все централизованные криптовалютные биржи (которых большинство на рынке) хранят средства пользователей на своих «горячих» адресах[5], 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[6], при этом многие из них имеют логи активности своих пользователей. Каждая биржа имеет собственный порядок предоставления сведений, некоторые и вовсе не отвечают на запросы органов государственной власти [9, с. 84], что затрудняет противодействие взяточничеству.

В теории права по данному поводу имеется несколько точек зрения. Одни авторы рассматривают криптовалютные активы в качестве предмета преступлений против собственности; предмета преступлений коррупционной направленности. Другие авторы придерживаются мнения о том, что криптовалютные активы подпадают под услуги имущественного характера при совершении взяточничества. Третьи считают, что криптовалютные активы целесообразно относить к имущественному праву [10, с. 48], четвертые – к иному имуществу [11, с. 14; 12, с. 381]. Также существует позиция о том, что сегодня создана «идейная и технологическая база для того, чтобы биткоин из товара смог стать мировой валютой» [13, с. 69].

В настоящее время на территории Российской Федерации формируются преступные механизмы и схемы совершения взяточничества с использованием цифровых финансовых и криптовалютных активов. Так, Генеральный прокурор Российской Федерации И.В. Краснов в интервью ТАСС к Международному дню борьбы с коррупцией в 2022 году заявил, что «есть примеры передачи в качестве взятки криптовалюты, хотя они пока не столь распространены»[7]. Проанализировав материалы правоприменительной практики в части, касающейся привлечения взяточников к ответственности за совершение преступлений с использованием цифровых финансовых и криптовалютных активов, можно сделать вывод о наличии следующей закономерности: исследуемые виды преступления выявляются, документируются и раскрываются благодаря слаженному взаимодействию органов и подразделений, а также при наличии сведений об обналиченных средствах без законного обоснования их происхождения. Следует отметить, что в процессе противодействия взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов, у органов внутренних дел возникают проблемы в области использования информационно-телекоммуникационных технологий в процессе выявления и документирования фактов взяточничества, когда предметом выступают цифровые финансовые и криптовалютные активы.

Так, в 2021 году в Москве в отношении профессорско-преподавательского состава возбуждено уголовное дело по признакам преступлений,

[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 // Российская газета. 2020. № 173.

[2] ЦБ предложил запретить оборот и майнинг криптовалют в России. URL: https://www.rbc.ru/finances/20/01/2022/61e9231a 9a79477 514c2b9ce (дата обращения: 10.09.2024).

[3] Минфин предложил новые правила криптовалютных операций вместо запрета. URL: https://www.rbc.ru/ finances/27/01/2022/61f109cd9a 7947eabe32ce42 (дата обращения: 10.09.2024).

[4] Греф поддержал запрет на использование криптовалют для платежей. URL: https://www.rbc.ru/rbcfree news/61fac9d-c9a79471d479 d3b9a? (дата обращения: 10.09.2024).

[5] 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).

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

[7] Генпрокурор РФ сообщил о выявлении в России первых случаев взяток криптовалютой. URL: https://tass.ru/ ekonomika/16544839 (дата обращения: 12.09.2024).

предусмотренных п. «в» ч. 5 ст. 290 и п. «б» ч. 3 ст. 291[1] УК РФ[1]. Из материалов уголовного дела следует, что предметом взяточничества являлись криптовалютные активы, которые были перечислены на анонимные криптокошельки. Задокументировать факт противоправной деятельности удалось благодаря проведенным оперативно-розыскным мероприятиям, в результате которых установлено, что после возбуждения уголовного дела сотрудниками оперативных подразделений по поручению следователя по адресу проживания фигуранта был осуществлен обыск, в результате которого были выявлены обналиченные денежные средства, расфасованные по конвертам; черновые записи с вопросами, которые необходимо задать при защите диссертационного исследования и др.

В июне 2023 года правоохранительными органами было возбуждено одно из наиболее резонансных уголовных дел по преступлениям коррупционной направленности. Уголовное дело возбуждено в отношении начальника следственного отдела СУ СК РФ по Тверскому району г. Москвы Марата Тамбиева, который по версии ГСУ СК РФ и Генеральной прокуратуры РФ получил от хакеров взятку в виде криптовалютных активов на общую сумму 24 млн долларов. В ходе обыска по месту проживания Тамбиева был изъят компьютер, в котором находилась папка с надписью «Пенсия» с кодами доступа к электронному криптокошельку. Взяткодатели отделались условными сроками, а у Тамбиева надзорные органы рассчитывают конфисковать весь его коррупционный доход. В процессе расследования следователи выдвигают версию, согласно которой Тамбиев 7 апреля 2022 года от хакерской группировки Infraud Organization, а именно ее членов: Марка и Константина Бергмановых, и Кирилла Самокутяева получил взятку за неналожение ареста на их активы[2].

Таким образом, на основе анализа правоприменительной практики мы можем сделать вывод, что основополагающим инструментом органов внутренних дел в противодействии взяточничеству в рамках выявления должностных лиц, получающих взятки в цифровых финансовых и криптовалютных активах, является взаимодействие с лицами, оказывающими содействие, и проведение комплекса оперативно-розыскных мероприятий, в том числе ограничивающих конституционные права граждан. При осуществлении оперативно-розыскных мероприятий необходимо задокументировать факт противоправной деятельности: получить идентификаторы криптокошельков, с которых происходит перевод средств в фиатные активы, а далее – их вывод на лицевые счета, в том числе электронные кошельки, которые принадлежат (находятся в пользовании) должностным лицам, их родственникам и третьим лицам, которые находятся в непосредственной связи с взяткополучателем, а также идентификаторы транзакций; получить сведения о лицевых счетах должностных лиц, их родственников и третьих лиц, находящихся в непосредственной связи с взяткополучателем и прочее.

Наиболее распространенными механизмами совершения преступлений, предусмотренных ст. 290-291[2] УК РФ, с использованием криптовалютных активов являются:

1. Открытие должностным лицом, его родственником и третьими лицами, находящимися в непосредственной связи с взяткополучателем, электронных кошельков и криптокошельков.

2. Перечисление криптовалютных активов на открытый ранее электронный кошелек и криптокошелек и передача взяткодателю идентификатора электронного криптокошелька (цифровой код или же QR-код).

3. Обмен криптовалютных активов на фиатную валюту с использованием криптовалютных бирж и вывод денежных средств через банкоматы.

В своих исследованиях Х.А. Асатрян и А.А. Христюк справедливо отмечают, что «выявить участников взяточничества можно только при получении взяткополучателем идентификатора криптокошелька» [5, с. 377]. В свою очередь, необходимо отметить, что идентификатор криптокошелька – это открытый ключ – адрес (счет), на который осуществляется перевод средств. Идентификатор могут видеть другие пользователи системы блокчейн, поэтому он и называется публичным. При помощи открытого ключа выполняется процесс шифрования – создание транзакций.

Таким образом, оперативно-розыскная деятельность органов внутренних дел в противодействии взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов, должна быть направлена на установление, в первую очередь, идентификаторов криптокошельков. В целях идентификации криптокошелька необходимо получить общие сведения, которые содержатся в системе блок-

[1] СК завел дело о взятках биткоинами за диссертации в МПГУ. URL: https://www.rbc.ru/society/25/08/2021/61262ebe9a7947383e067c59?ysclid=l85bstytth394934302 (дата обращения: 12.09.2024).

[2] Все, что нажито непосильной взяткой. URL: https://www.kommersant.ru/doc/6026773 (дата обращения: 12.09.2024).

чейн. В системе блокчейн имеются две разновидности обозревателей: обозреватели, представляющие сведения о конкретных криптовалютных активах, и обозреватели, исследующие различные типы криптовалютных активов.

В случаях, когда в идентифицируемом криптокошельке еще не совершались транзакции, органам внутренних дел в рамках организации оперативно-розыскной деятельности рекомендуется осуществлять его мониторинг, который позволит своевременно выявить и задокументировать факт совершения противоправных коррупционных транзакций с криптовалютными активами. Данный мониторинг, как правило, осуществляется в отношении следующих криптокошельков, оформленных (зарегистрированных) в: Bitcoin (BTC), Ethereum (ETH), Bitcoin Cash (BCH), Litecoin (LTC), с использованием мониторинговых сервисов.

В вышеуказанном направлении органам внутренних дел в рамках организации оперативно-розыскной деятельности необходимо в кратчайшие сроки установить идентификатор кошелька (криптокошелька). Каждый криптокошелек, как ранее отмечалось, имеет уникальный идентификатор, при этом в процессе создания криптокошелька идентификатор пользователя направляется на электронную почту, указанную при верификации, после чего происходит процедура подтверждения.

Наиболее простым способом получения идентификатора криптокошелька, возможно находящегося в пользовании должностного лица, которым могут воспользоваться органы внутренних дел в рамках организации оперативно-розыскной деятельности, является использование операторов расширенных поисковых запросов. На наш взгляд, их использование позволит устранить из поискового запроса сведения, которые не относятся к оперативно-значимой информации в отношении проверяемого (разрабатываемого) должностного лица, и оперативным путем выявлять и документировать факты противоправной деятельности со стороны должностных лиц.

Следующий способ получения сведений о криптокошельке – применение «сайтов-отзовиков» и скоринговых сервисов. При этом скоринговые сервисы осуществляют сбор сведений о применении криптокошелька в преступных целях, а «сайты-отзовики» дополнительно содержат в себе электронные адреса и информацию о веб-ресурсах, которыми пользуются преступники-взяточники.

Третий способ идентификации криптокошелька – получение сведений об отнесении криптокошелька к криптовалютным биржам и криптообменникам. Сведения о данных криптокошельках находятся в специализированных сервисах, доступ к которым ограничен. После получения сведений о криптовалютных биржах целесообразно направить соответствующий запрос в рамках ведения дел оперативного учета при проведении оперативно-розыскных мероприятий. Следует отметить, что прежде чем запросить данную информацию, необходимо получить судебное решение на производство оперативно-розыскного мероприятия «Наведение справок». В качестве примера предлагаем возможную формулировку запроса в централизованную криптовалютную биржу.

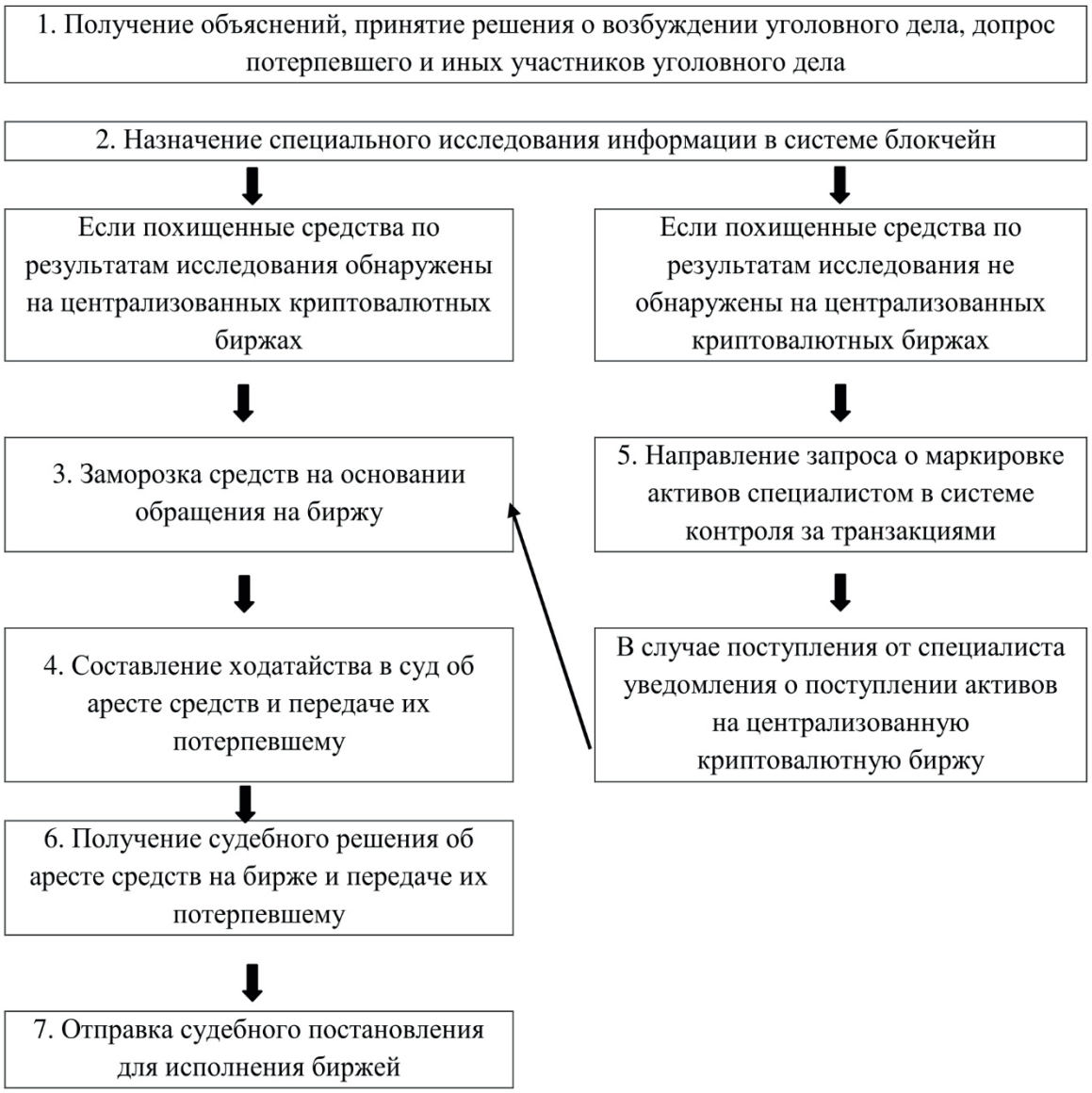
При сопровождении уголовного дела № 111, возбужденного ДД.ММ.ГГ. в отношении гр. ФИО по признакам преступления, предусмотренного ч. 6 ст. 290 УК РФ, имеется необходимость в получении сведений об идентификаторе криптокошелька, принадлежащего гр. П., 01.01.1990 г.р., зарегистрированному по адресу: г. Москва, ул. Мира, д. 1, кв. 1, использовавшему для верификации электронную почту (……@bk.ru), а также сведения о логине и абонентском номере, указанных при регистрации и верификации; копии документов, представленных в процессе верификации; информацию об IP-адресах, с которых осуществлялось обращение; сведения о произведенных операциях по перечислению криптовалютных активов с отражением объема, наименования и дат совершения операций, сведений об остатках криптовалютных активов и прочее.

На основании вышеизложенного, в связи с ограниченными сроками расследования, а также 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», решением Головинского районного суда г. Москвы, просим Вас предоставить вышеуказанные сведения в кратчайшие сроки, направив на адрес служебной электронной почты ….@mvd.ru

При выявлении и документировании исследуемых видов преступлений необходимо обращать внимание на следующие определенные аспекты (см. таблицу).

Принимая во внимание специфику противоправной деятельности, мы выявили возможную схему совершения преступных транзакций, связанных со взяточничеством:

– денежные средства переводятся с электронного кошелька или лицевого счета взяткодателя (посредника) на платежные реквизиты обменника (биржи);



– в обменнике (на бирже) происходит конвертация российских рублей в криптовалютные активы;

– с криптовалютного кошелька обменника (биржи) криптовалютные активы поступают на криптовалютный кошелек взяткополучателя (посредника);

– взяткополучатель (посредник) осуществляет перевод криптовалютных активов с криптовалютного кошелька на криптовалютный соответствующий кошелек обменника (биржи);

– в обменнике (на бирже) происходит конвертация криптовалютных активов в фиатные денежные средства (российские рубли, доллары США и прочее);

– с обменника (биржи) на лицевой счет взяткополучателя (посредника) (либо электронный кошелек) зачисляются конвертированные денежные средства.

После конвертации криптовалютных активов в фиатные денежные средства они включаются в законный гражданско-правовой оборот, им придается правомерный вид владения, а также пользования и распоряжения ими.

Сотрудники органов внутренних дел, осуществляющие оперативно-розыскную деятельность, должны обладать достаточными познаниями в области использования информационно-телекоммуникационных технологий в процессе противодействия взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов. В данном направлении использование системы блокчейн может стать эффективным механизмом антикоррупционной деятельности. Система блокчейн представляет собой сложный, высокотехнологичный и многофункциональный механизм, способствующий быстрой и эффективной обработке значительного объема сведений, в том числе связанных со взяточничеством. Основными особенностями блокчейн-систем являются: прозрачность сведений и информации, доверие (запись в системе блокчейн

не может быть изменена), отсутствие посредников (информация записывается и проверяется без третьих лиц) [14, с. 84-85]. В своих исследованиях М.Г. Жигас справедливо отмечает, что «система дает пользователям возможность осуществлять безопасные расчеты друг с другом по всему миру без вмешательства третьих лиц, при этом все расчеты обеспечены криптографической цифровой защитой, подтверждающей собственность правообладателя» [2, с. 84].

Следует отметить, что в 2021 году Росфинмониторинг совместно с Министерством цифрового развития, связи и массовых коммуникаций (далее – Минцифры России) разработали систему «Прозрачный блокчейн»[1]. Основная цель системы – противодействие криминализации цифровых финансовых и криптовалютных активов и совершению преступлений с их использованием. Задачами «Прозрачного блокчейна» выступают:

1) выявление и отслеживание проводимых транзакций с использованием цифровых финансовых и криптовалютных активов;

2) ведение баз данных с криптовалютными активами и криптокошельками;

3) мониторинг поведения участников криптовалютных бирж для идентификации;

4) прогнозирование возможности участия владельцев цифровых финансовых и криптовалютных активов в противоправной деятельности.

Данная система позволяет органам внутренних дел направлять запрос в Росфинмониторинг и получать информацию о совершенных и (или) совершаемых транзакциях с цифровыми финансовыми и криптовалютными активами конкретным лицом и предотвратить процесс перечисления средств должностному лицу за действия или бездействие в пользу взяткодателя – владельца криптокошелька. Поскольку должностные лица обязаны сообщать о наличии цифровых финансовых и криптовалютных активов наряду с другими доходами, имеется возможность осуществлять проверку для отслеживания транзакций с их использованием, чтобы предотвратить и (или) минимизировать факты взяточничества. Однако следует отметить, что система «Прозрачный блокчейн» – это инструмент, который осуществляет сбор и анализ сведений о криптокошельках и совершаемых транзакциях с использованием цифровых финансовых и криптовалютных активов.

Внедрение в подразделения органов внутренних дел, осуществляющих оперативно-розыскную деятельность, информационно-телекоммуникационных технологий должно носить комплексный характер, например, систему блокчейн, BigData необходимо использовать в неразрывной связи с государственной информационной системой «Посейдон», которая представляет собой эффективную инновационную систему, направленную на информационно-аналитическую деятельность правоохранительных органов в противодействии экономическим и коррупционным преступлениям, структура которой обусловлена тремя элементами (Посейдон, Посейдон-Р, Справки БК) [15, с. 253].

Обсуждение и заключение

По результатам проведенного исследования автор приходит к выводу, что к наиболее распространенным оперативно-розыскным мероприятиям, направленным на противодействие органов внутренних дел взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов, необходимо относить:

– наведение справок в банковских организациях по лицевым счетам фигурантов и их близких родственников; в централизованных криптовалютных биржах, в Федеральной службе государственной регистрации, кадастра и картографии; в налоговых органах, по месту осуществления трудовой деятельности;

– прослушивание телефонных переговоров и снятие информации с технических каналов связи;

– иные оперативно-технические мероприятия, проводимые сотрудниками подразделений специальных технических мероприятий и оперативно-поисковых подразделений;

– оперативно-розыскные и иные мероприятия в сети Интернет: мониторинг интернет-ресурсов, открытых баз данных; специальное исследование информации в системе блокчейн.

Кроме того, подразделениям органов внутренних дел, осуществляющим оперативно-розыскную деятельность, в рамках противодействия взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов, необходимо:

– использовать общедоступные программы и сервисы, позволяющие осуществлять сбор оперативно-значимой информации;

– применять технологические решения, обеспечивающие техническую, физическую и юридическую достоверность сведений, содержащихся в информационных системах;

– применять технологии смарт-контрактов;

– активировать взаимодействие с Росфинмониторингом по совершенным и совершаемым сомнительным операциям с использованием ли-

[1] В России создан сервис для отслеживания транзакций с криптовалютой. URL: https://www.rbc.ru/crypto/news/602fb2449a7947 f67080807f (дата обращения: 15.09.2024).

цевых счетов фигурантов и их близких родственников; со следственными органами при решении вопроса о наложения ареста на имущество и его конфискации;

– принимать меры по документированию совершенных и совершаемых транзакций с указанием платежей, дат, времени, криптовалютного адреса получателя средств; по установлению хеш-идентификаторов и криптовалютных адресов отправителя средств.

Таким образом, оперативно-розыскная деятельность органов внутренних дел в процессе противодействия взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов, должна преимущественно основываться на использовании информационно-телекоммуникационных технологий. Применение информационно-телекоммуникационных технологий позволит увеличить эффективность выявления и документирования фактов взяточничества. В целях повышения эффективности оперативно-розыскной деятельности органов внутренних дел в противодействии взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов, необходимо:

1) разработать методические рекомендации по выявлению, документированию и раскрытию фактов взяточничества, совершаемого с использованием цифровых финансовых и криптовалютных активов;

2) внедрить в подразделения органов внутренних дел, осуществляющих оперативно-розыскную деятельность, информационно-телекоммуникационные технологии; предоставить сотрудникам исследуемых подразделений органов внутренних дел расширенный доступ к личным кабинетам на сайте Росфинмониторинга и т.д.;

3) наладить взаимодействие между личным составом соответствующих подразделений Центрального аппарата МВД России и личным составом соответствующих подразделений территориальных органов внутренних дел при выявлении и документировании исследуемых видов преступлений, в том числе при разработке алгоритмов их выявления и документирования; с биржами, в которых происходят транзакции, подпадающие под признаки «сомнительных операций»;

4) выстроить неразрывное и интегративное взаимодействие подразделений экономической безопасности и противодействия коррупции с подразделениями по организации противодействия противоправному использованию информационно-коммуникационных технологий (возможно в рамках отдельных приказов и (или) распоряжений);

5) повышать профессионализм, навыки и умения личного состава посредством проведения учебных занятий, направленных на растолкование (раскрытие) механизмов и процессов применения информационно-телекоммуникационных технологий в целях выявления, установления и документирования всех этапов исследуемой преступной деятельности.

СПИСОК ИСТОЧНИКОВ

1. Ишигеев В.С., Христюк А.А. Квалификации должностных преступлений: монография. Иркутск: БГУЭП, 2011. 148 с.

2. Жигас М.Г., Кузьмина С.Н. Блокчейн и децентрализованная денежная система: принципы построения и пути развития // Известия Байкальского государственного университета. 2020. Т. 30. № 1. С. 79 – 88. DOI 10.17150/2500-2759.2020.30(1).

3. Дмитренко А.П. Криптовалюта как предмет взятки и коммерческого подкупа // Уголовное право и информатизация преступности: проблемы теории, практики и преподавания: сборник статей по материалам Всероссийской научной конференции. Москва: Юриспруденция, 2018. С. 49 – 54.

4. Репецкая А.Л. Криптопреступления как следствие цифровизации преступности // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции: сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 года. Москва: Университет прокуратуры России, 2021. С. 61 – 67.

5. Асатрян Х.А., Христюк А.А. Проблемы определения предмета взяточничества и особенности его выявления в современных реалиях // Всероссийский криминологический журнал. 2022. № 3. С. 374 – 383.

6. Исмайылова А.Т. Цифровой актив как предмет получения взятки // Проблемы совершенствования прокурорской деятельности и правоприменительной практики: сборник статей. Том 8. Иркутск: Иркутский юридический институт (филиал) Университета прокуратуры России, 2019. С. 159 – 162.

7. Грибов И.Г. Криптовалюта как предмет взятки: проблемы квалификации // Вестник научных конференций. 2019. № 5-2(45). С. 35 – 37.

8. Долгиева М.М. Квалификация деяний, совершаемых в сфере оборота криптовалюты // Вестник Восточно-Сибирского института МВД России. 2019. № 1 (88). С. 9 – 20.
9. 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 10.18287/2542-047X-2023-9-3-81-90.
10. Takkal Bataille A., Favier J. Bitcoin, la monnaieacéphale. Paris: CNRS Éditions, 2017. 214 p.
11. Vigna P., Casey M.J. The age of cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic Order. New York, 2015.
12. Куликова А.А., Жмурко Р.Д. Криптовалюта как предмет преступления: проблемы квалификации и защиты // Вестник Алтайской академии экономики и права. 2020. № 11-2. С. 376 – 381. DOI 10.17513/vaael.1436.
13. Волегова А.С. Биткоин: деньги или товар // Пермский финансовый журнал. 2016. № 1. С. 60 – 70.
14. Гумаров И.А., Фарахиев Д.М. Технология blockchain как средство противодействия коррупции // Научный компонент. 2022. № 1(13). С. 81 – 87. DOI 10.51980/2686-939X_2022_1_81.
15. Фарахиев Д.М. Государственная информационная система «Посейдон»: современный взгляд на противодействие коррупции // Вестник Московского университета МВД России. 2023. № 1. С. 250 – 254. DOI 10.24412/2073-0454-2023-1-250-254.

REFERENCES

1. Ishigeev V.S., Hristyuk A.A. Kvalifikacii dolzhnostnyh prestuplenij: monografiya. Irkutsk: BGUEP, 2011. 148 s.
2. Zhigas M.G., Kuz'mina S.N. Blokchejn i decentralizovannaya denezhnaya sistema: principy postroeniya i puti razvitiya // Izvestiya Bajkal'skogo gosudarstvennogo universiteta. 2020. T. 30. № 1. S. 79 – 88. DOI 10.17150/2500-2759.2020.30(1).
3. Dmitrenko A.P. Kriptovalyuta kak predmet vzyatki i kommercheskogo podkupa // Ugolovnoe pravo i informatizaciya prestupnosti: problemy teorii, praktiki i prepodavaniya: sbornik statej po materialam Vserossijskoj nauchnoj konferencii. Moskow: Yurisprudenciya, 2018. S. 49 – 54.
4. Repeckaya A.L. Kriptoprestupleniya kak sledstvie cifrovizacii prestupnosti // Cifrovye tekhnologii v bor'be s prestupnost'yu: problemy, sostoyanie, tendencii: sbornik materialov I Vserossijskoj nauchno-prakticheskoj konferencii, Moskva, 27 yanvarya 2021 goda. Moskva: Universitet prokuratury Rossii, 2021. S. 61 – 67.
5. Asatryan H.A., Hristyuk A.A. Problemy opredeleniya predmeta vzyatochnichestva i osobennosti ego vyyavleniya v sovremennyh realiyah // Vserossijskij kriminologicheskij zhurnal. 2022. №3. S. 374 – 383.
6. Ismajylova A.T. Cifrovoj aktiv kak predmet polucheniya vzyatki // Problemy sovershenstvovaniya prokurorskoj deyatel'nosti i pravoprimenitel'noj praktiki: sbornik statej. Tom 8. Irkutsk: Irkutskij yuridicheskij institut (filial) Universiteta prokuratury Rossii, 2019. S. 159 – 162.
7. Gribov I.G. Kriptovalyuta kak predmet vzyatki: problemy kvalifikacii // Vestnik nauchnyh konferencij. 2019. № 5-2(45). S. 35 – 37.
8. Dolgieva M.M. Kvalifikaciya deyanij, sovershaemyh v sfere oborota kriptovalyuty // Vestnik Vostochno-Sibirskogo instituta MVD Rossii. 2019. № 1 (88). S. 9 – 20.
9. Farahiev D.M. Deyatel'nost' organov vnutrennih del v processe raskrytiya i rassledovaniya prestuplenij, sovershaemyh s ispol'zovaniem informacionno-kommunikacionnyh tekhnologij (na primere kriptovalyutnyh aktivov) // Yuridicheskij vestnik Samarskogo universiteta. 2023. T. 9, № 3.
S. 81 – 90. DOI 10.18287/2542-047X-2023-9-3-81-90.
10. Takkal Bataille A., Favier J. Bitcoin, la monnaieacéphale. Paris: CNRS Éditions, 2017. 214 p.
11. Vigna P., Casey M.J. The age of cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic Order. New York, 2015.
12. Kulikova A.A., Zhmurko R.D. Kriptovalyuta kak predmet prestupleniya: problemy kvalifikacii i zashchity // Vestnik Altajskoj akademii ekonomiki i prava. 2020. № 11-2. S. 376 – 381. DOI 10.17513/vaael.1436.
13. Volegova A.S. Bitkoin: den'gi ili tovar // Permskij finansovyj zhurnal. 2016. № 1. S. 60 – 70.
14. Gumarov I.A., Farahiev D.M. Tekhnologiya blockchain kak sredstvo protivodejstviya korrupcii // Nauchnyj komponent. 2022. № 1(13). S. 81 – 87. DOI 10.51980/2686-939X_2022_1_81.
15. Farahiev D.M. Gosudarstvennaya informacionnaya sistema «Posejdon»: sovremennyj vzglyad na protivodejstvie korrupcii // Vestnik Moskovskogo universiteta MVD Rossii. 2023. № 1. S. 250 – 254. DOI 10.24412/2073-0454-2023-1-250-254.

Информация об авторе:
Фарахиев Динар Минзеферович, адъюнкт 3 факультета (подготовки научных и научно-педагогических кадров) Академии управления МВД России, dfarakhiev@mail.ru
Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Farahiev Dinar M., Postgraduate of the 3rd Faculty (Training of Scientific and Scientific-Pedagogical Staff) Academy of Management of the Ministry of Internal Affairs of Russia, dfarakhiev@mail.ru
The author has read and approved the final version of the manuscript.

Статья получена: 23.10.2024.
Статья принята к публикации: 25.03.2025.
Статья опубликована онлайн: 27.03.2025.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.