Вестник Сибирского юридического
института МВД России

УДК 343.95

Елена Викторовна ХРИСТИНИНА,
доцент кафедры государственного,
муниципального управления и таможенного
дела Омского государственного технического
университета,
доцент факультета очного обучения
Сибирского института бизнеса
и информационных технологий (г. Омск),
кандидат юридических наук
elena.nikitina83@mail.ru

КРИПТОВАЛЮТА КАК ПРЕДМЕТ ВЗЯТОЧНИЧЕСТВА В СФЕРЕ ВЫСШЕГО ОБРАЗОВАНИЯ

CRYPTOCURRENCY AS A SUBJECT MATTER OF BRIBERY IN HIGHER EDUCATION

В статье рассмотрены понятие и виды предмета взятки в сфере высшего образования с основным акцентом на криптовалюте в качестве преступного предмета. Представлена авторская классификация предмета взятки в сфере высшего образования. Констатируется, что в связи с развитием информационных технологий, электронных платежей все больше распространенным становится получение взятки в виде криптовалюты.

С криминалистической стороны изучается понятие и виды цифровых следов, которые могут остаться при совершении взяточничества в сфере высшего образования, с использованием предмета взятки в виде криптовалюты, виды следственных действий, которые могут проводиться по анализируемым уголовным делам.

The concept and types of the subject matter of bribery in the field of higher education are considered in the article, whereby great emphasis is placed on cryptocurrencies as a subject matter of crime. The author's classification of the subject matter of bribery in the field of higher education is presented in the article. It is stated that due to the development of information technologies and electronic payments acceptance of a bribe in the form of crypto currencies is becoming more common.

A forensic approach is used in studying the concept and types of digital footprints that can be left when committing bribery in the field of higher education using cryptocurrency as a subject matter of crime. The types of investigative actions that can be carried out in the analyzed criminal cases are studied as well.

Ключевые слова: взяточничество в сфере высшего образования, взяткополучатель, коррупция, расследование уголовных дел, взяткодатель, криптовалюта, биткоины, фиатная валюта, криптобиржа, предмет взяточничества, криптосчет, криптокошелек.

Keywords: *bribery in higher education, bribe taker, corruption, criminal investigation, bribe giver, cryptocurrency, bitcoins, fiat currency, cryptocurrency exchange, subject matter of bribery, crypto account, crypto wallet.*

Предмет взятки учеными-криминалистами рассматривался с различных сторон – как денежные средства, любые материальные вещи, услуги имущественного характера, которые имеют определенную ценность для их получателя.

Значение предмета взятки как элемента криминалистической характеристики состоит

в том, что при помощи него возможно установить другие элементы (способ, обстановка совершения преступления, механизм следообразования, личность взяткополучателя).

Говоря о предмете взяточничества, следует отметить, что ученые-криминалисты выделяют различные классификации предметов взяточничества исходя из разных критериев их деления.

К примеру, А.А. Черкесова предмет взятки разделяет по ее цели на следующие виды: ценные подарки при получении взятки-благодарности и денежные средства при получении взятки-подкупа [11, с. 24].

А.Н. Халиков справедливо указывает, что особенность предмета взятки чаще всего обусловлена той сферой, в которой совершается анализируемое преступление [8, с. 69].

Е.Ю. Фролова, говоря о предмете взяточничества в правоохранительной и судебной сферах, указывает в качестве такового денежные средства, подарки, услуги имущественного характера [7, с. 47].

И.С. Башмаков, изучая предмет взяточничества, совершаемого в органах местного самоуправления, приходит к выводу о том, что предметом взятки являются не только денежные средства, ценные подарки и услуги имущественного характера, но и оказываемая спонсорская помощь [2, с. 68].

Т.Б. Хачатурян, рассматривая взяточничество, совершаемое в органах исполнительной власти, полагает, что предмет взятки может быть различным: денежные средства, ценные бумаги, продукты питания, спиртные напитки, имущество, оказание услуг или выгод имущественного характера [9, с. 48].

Проведенное эмпирическое исследование предмета взятки в сфере высшего образования позволило выделить следующие виды:

1) денежные средства (65,6%), в том числе:

– в иностранной валюте (1,2%);

– в криптовалюте (6,3%);

2) имущество (21,3 %) случаев:

– имущество, стоимость которого приравнивается к «обычной взятке», то есть до 25 тысяч рублей (66,5%). К такому имуществу относились продукты питания, книги, канцелярские принадлежности;

– имущество, стоимость которого приравнивается к взятке значительного размера, то есть свыше 25 тысяч рублей (31,2%). К такому имуществу относились: строительные материалы, мебель, бытовая техника и т.д.;

– имущество, стоимость которого приравнивается к взятке крупного и особо крупного размера, то есть свыше 150 тысяч рублей (2,3%);

3) услуги имущественного характера (11,9%). К таким услугам относятся, например, оплата счетов телефонных переговоров, предоставление туристических путевок, подарочных сертификатов и т.д.

Причинами совершения взяточничества с использованием информационно-телекоммуникационных технологий могут выступать информатизация всех систем, применение в качестве предмета взятки электронных денег, усложняющих процесс изобличения преступника. Кроме того, средством для передачи электронных денег может выступать электронная почта, принадлежащая взяткополучателю, с помощью которой последний узнает код, на основании которого можно обналичить денежные средства. Отдельный интерес представляет использование взяткополучателем определенного предмета преступления – криптовалюты. Ее появление было обусловлено развитием блокчейн-технологии для того, чтобы электронная валюта была не контролируема государством.

Получение взятки в виде криптовалюты – быстрый и достаточно простой способ преступного обогащения. Во-первых, бывает достаточно сложно отследить перемещение данных денежных средств с одного криптосчета на другой. Во-вторых, перемещение денежных средств имеет бесконтактный способ, незаметный для окружающих. В-третьих, данный предмет взятки, как правило, легко скрыть, например взяткодатель может деньги обналичить и приобрести на них имущество либо иначе реализовать преступный источник дохода.

В настоящее время законодатель ввел понятие криптовалюты в ч. 3 ст. 1 Федерального закона от 31 июля 2020 г. N 259-ФЗ «О цифровых финансовых активах, цифровой валю-

те и о внесении изменений в отдельные законодательные акты Российской Федерации».

Согласно закону 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.

К сожалению, законодатель в ст. 290 УК РФ в качестве предмета взятки включил лишь деньги, ценные бумаги, иное имущество, незаконное оказание услуг имущественного характера, иные имущественные права. Криптовалюта в виде биткоина в качестве предмета преступления не упоминается.

Однако следует обратиться к постановлению Пленума Верховного Суда РФ от 9 июля 2013 г. N 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях», в п. 10 которого говорится о том, что получение взятки считается оконченным преступным деянием с момента зачисления с согласия должностного лица на указанный им банковский счет, «электронный кошелек». Тем самым законодатель косвенно относит к предмету взятки криптовалюту.

Для получения незаконного вознаграждения в виде криптовалюты взяткополучатель создает специальный криптокошелек через специализированные сайты (Blockchain.info) либо специально установленные приложения на компьютере и мобильном устройстве. Представляется, что криптокошелек может действовать в режиме анонимности пользователя, поскольку дополнительной верификации или предоставления документов, удостоверяющих личность пользователя, не требуется. После создания криптокошелька взткополучатель отправляет его идентификатор, состоящий из одномерного цифрового кода или QR-кода взяткодателю, который в будущем будет переводить виртуальные деньги. После перечисления виртуальных денег взяткополучатель может обменять биткоины на фиатную валюту на криптобирже, после чего денежные средства могут быть зачислены на банковский счет как самого преступника, так и его родственников и знакомых.

Исходя из преступного механизма перечисления денежных средств, следует сделать вывод о том, что довольно сложно идентифицировать участников преступления, это возможно только в том случае, если известны сведения об идентификаторе криптокошелька взяткополучателя и установлены преступная связь между взяткополучателем и взяткодателем посредством перечисления виртуальных денежных средств на криптокошелек и выполнение определенных действий в интересах дающего.

Таким образом, применение информационно-телекоммуникационных технологий при совершении взяточничества влечет изменение механизма преступления за счет отсутствия прямого контакта между взяткодателем и взяткополучателем, в результате чего появляется термин «дистанционное взяточничество». В результате появляются сложности в расследовании преступления и установлении виновного лица. К примеру, эти сложности обусловлены тем, что IP-адреса, серверы и ресурсы, с которых совершаются преступные деяния, могут находиться вне юрисдикции нашего государства. Следовательно, основная задача органов расследования – своевременно получить криминалистически важную информацию о совершении «дистанционных» взяточничеств из анализа цифровых следов преступления.

В научной литературе существует множество определений понятий «виртуальные следы» (В.Ю. Агибалов, В.А. Мещеряков, А.Б. Смушкин и др. [1; 4; 6], «электронно-цифровые следы» (В.Б. Вехов [3]), «цифровые следы» (Е.Р. Россинская и И.А. Рядовский, М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин [5; 10]).

В.А. Мещеряков справедливо указывает, что виртуальные следы представляют собой «любые изменения состояния автоматизированной информационной системы («кибернетического пространства»), связанные с событием преступления и зафиксированные в виде компьютерной информации на материальном носителе, в том числе электромагнитном поле» [4, с. 74].

В.А. Мещеряков, исходя из представленного определения, выделяет особенные свой-

ства виртуального следа, благодаря которому следы могут изыматься, исследоваться следственными органами при расследовании многих преступлений. Позиция автора обусловлена тем, что «виртуальные следы» занимают промежуточное межу между видами следов: идеальными и материальными. В.А. Мещеряков объясняет необходимость выделения таких следов тем, что они содержатся на материальном носителе, однако их обнаружение и изъятие возможно только с помощью программно-технических средств, так как по-другому они не могут быть восприняты.

Представляется, что включение «виртуальных следов» в состав материальных следов не является возможным, так как следы содержат субъективную составляющую, зависящую от способа их считывания, и не имеют прочной связи с устройством, которое записывает информацию. Они также являются неустойчивыми, что делает их ближе к идеальным следам. Однако они не могут быть классифицированы как идеальные следы, так как они хранятся на материальных объектах, а не в человеческой памяти.

В.Ю. Агибалов отождествляет термин «цифровой след» с термином «след-модель», включая в его содержание «упорядоченную совокупность электронных цифровых данных, отражающих абстрактную модель и параметры реального объекта, относящегося к расследуемому уголовному делу» [1, с. 353].

Позиция автора основана на том, что при использовании цифровой записи звука или изображения сохраняется абстрактная математическая модель исходного объекта, а не сам объект или его полное отражение. Эта модель определяется видом математической модели и ее параметрами. Таким образом, при цифровой записи информации на материальный носитель фиксируется последовательность чисел, которая представляет параметры абстрактной модели.

А.Б. Смушкин изучает виртуальные следы с позиции совершения определенных действий, определяя, что это «следы совершения действий: включения, создания, открывания, активации, внесения изменений, удаления в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей» [6, с. 43].

Полагаем, что термин «виртуальные следы» сложно использовать при расследовании преступлений, поскольку он активно уже применяется в квантовой теории поля в ходе описания квантовых частиц и относится к виртуальной реальности. В контексте расследования преступлений, где требуется сбор фактических доказательств и установление конкретных фактов, использование термина «виртуальные следы» может вызывать определенную путаницу.

Профессор В.Б. Вехов рассматривает понятие «электронно-цифровой след» как «любую криминалистически значимую компьютерную информацию, зафиксированную на материальном носителе с помощью электромагнитных взаимодействий либо передающуюся по каналам связи посредством электромагнитных сигналов» [3, с. 27].

С теоретической и практической точки зрения мнение В.Б. Вехова считаем логичным, так как данный термин обозначает двойственную природу следов: электронные следы, которые могут оставаться на различных материальных носителях, и цифровые следы, которые представлены в виде цифрового кода или изменений, зафиксированных в цифровом коде в памяти электронных устройств. Такое название позволяет более точно говорить, о каких именно следах идет речь, а также учитывать их электронную и цифровую природу.

Однако полагаем правильнее применять понятие «цифрового следа» при расследовании преступлений.

А.М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин в научных исследованиях применяют термин «цифровые следы», под которым понимают «любую криминалистически значимую компьютерную информацию, содержащую сведения (сообщения, данные), представленную в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [10, с. 130].

С криминалистической точки зрения, как справедливо полагают Е.Р. Россинская и И.А. Рядовский, цифровые следы следует

понимать как «криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [5, с. 7].

Цифровые следы могут находиться на электронных устройствах (компьютерах, планшетах, сотовых телефонах), если при помощи них осуществлялся доступ к криптокошельку или проводились электронные операции с виртуальными деньгами. В сотовом телефоне, планшете правоохранительными органами может быть изъята сим-карта, с помощью которой можно проверить информацию о том, на кого она была зарегистрирована – на взяткополучателя или на постороннее лицо.

Посредством осмотра электронных устройств можно выяснить информацию об общении, взаимодействии взяткодателя и взяткополучателя, а также какие специальные веб-сайты, программное устройство применялось преступником при получении виртуальных денег, а также какие документы были загружены с электронного устройства, например файл с адресом кошелька и QR-кодом для взяткодателя.

Кроме того, анализ трафика от интернет-провайдера, применение сервера VPN, контроль Wi-Fi-сети, применяемой на работе или по месту жительства взяткополучателя, позволяет сделать вывод о том, проводились ли операции посредством криптовалюты или нет. Использование вышеперечисленных информационных технологий не гарантирует пользователю конфиденциальности проведенных электронных операций.

По уголовным делам данной категории, где предметом взятки выступает криптовалюта, могут проводиться различные следственные действия, такие как осмотр места происшествия, осмотры электронных устройств и документации, обыски, выемки по месту работы и жительства подозреваемого с обязательным участием специалиста, который может оказать помощь в обнаружении и изъятии цифровых следов, проведение компьютерно-технической экспертизы.

Приведем практический пример, получения взяток преподавателями в виде криптовалюты.

В 2021 г. было возбуждено уголовное дело в отношении преподавателей Московского педагогического государственного университета за получение взяток за защиту диссертаций и получение ученой степени. Механизм совершения преступления был следующий: преподаватели за оказанные услуги получали денежные средства в криптовалюте, переводя их на анонимные кошельки в биткоинах. В ходе проведения групповых обысков по месту работы и жительства преподавателей были обнаружены обналиченные денежные средства в крупных суммах, а также записи о получении сумм взяток и вопросов, которые должны задаваться на защитах научных работ.

Делая вывод, следует отметить, что расследование уголовных дел по взяточничеству в сфере высшего образования, где предметом взятки является криптовалюта, имеет ряд сложностей. Данные сложности связаны с установлением личности владельца криптокошелька, так как чаще всего доступ к нему происходит посредством ввода адреса электронной почты или смс-кода, а сим-карта может быть зарегистрирована на постороннее лицо. В результате этого установить личность преступника, а также доказать связь между переводом виртуальных денег и выполнение должностных полномочий в интересах дающего довольно сложно.

Библиографический список

1. Агибалов, В.Ю. Криминалистическая сущность виртуальных следов / В.Ю, Агибалов // Вестник Воронежского государственного университета. Серия: Право. – 2009. – N 2. – С. 350-355.

2. Башмаков, И.С. Особенности первоначального этапа расследования коррупционных преступлений, совершаемых представителями органов местной власти : дис. … канд. юрид. наук / И.С. Башмаков. – Екатеринбург, 2006. – 211 с.

3. Вехов, В.Б. Основы криминалистического учения об исследования и использовании компьютерной информации и средств ее обработки / В.Б. Вехов. – Волгоград : Волгоградская академия МВД России, 2008. – 404 с.

4. Мещеряков, В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ / В.А. Мещеряков. – Воронеж: Воронежский государственный университет, 2001. – 255 с.

5. Россинская, Е.Р. Концепция цифровых следов в криминалистике / Е.Р. Россинская, И.А. Рядовский // Аубакировские чтения: материалы международной научно-практической конференции. – Алматы: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. – С. 6-9.

6. Смушкин, А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. –2012. – Вып. 8. – С. 43-45.

7. Фролова, Е.Ю. Методика расследования коррупционной деятельности в правоохранительных и судебных органах : дис. … канд. юрид. наук / Е.Ю. Фролова. – Краснодар, 2005. – 217 с.

8. Халиков, А.Н. Особенности расследования получения взяток должностными лицами правоохранительных органов : дис. … канд. юрид. наук / А.Н. Халиков. – Уфа, 2005. – 238 с.

9. Хачатурян, Т.Б. Выявление и расследование взяточничества в органах исполнительной власти : дис. … канд. юрид. наук / Т.Б. Хачатурян. – М., 2004. – 209 с.

10. Цифровые следы преступлений : монография / А.М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин. – М.: Проспект, 2021. – 168 с.

11. Черкесова, А.А. Раскрытие и расследование взяточничества в условиях противодействия : дис. … канд. юрид. наук / А.А. Черкасова. – М, 2007. – 233 с.

8. Фисенко, Д.Ю. О законности привлечения граждан к административной ответственности по ст. 19.3 КоАП РФ за отказ от прохождения медицинского освидетельствования на состояние опьянения / Д.Ю. Фисенко // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2020. – N 6-2. – С. 87-91.

9. Цуканов, Н.Н. Статья 44 Федерального закона от 8 января 1998 г. N 3-ФЗ «О наркотических средствах и психотропных веществах» и статья 27.12.1 КоАП РФ: к вопросу о соотношении оснований направления на медицинское освидетельствование на состояние наркотического опьянения / Н.Н. Цуканов // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XX международной научно-практической конференции: в 2 ч. Красноярск, 20-21 апреля 2017 г. Ч. 1. – Красноярск: СибЮИ МВД России, 2017. – С. 81-84.

10. Чумарова, Е.Ю. Административная ответственность за правонарушение, предусмотренное ст. 20.21 КоАП РФ: особенности доказывания / Е.Ю. Чумарова // Правовые проблемы укрепления российской государственности : сборник статей всероссийской научно-практической конференции. Томск, 28-30 января 2021 г. – Томск: Издательство Томского государственного университета, 2021. – Т. 4. – С. 53-54.