Научная статья
УДК 343.98
DOI: 10.37973/VESTNIKKUI-2024-58-20

ХИЩЕНИЯ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТЫ В СТРУКТУРЕ КИБЕРПРЕСТУПЛЕНИЙ: ВИДЫ, ПРОБЛЕМЫ РАССЛЕДОВАНИЯ (БЕЛОРУССКИЙ ОПЫТ)

Дарья Игоревна Шнейдерова,
Могилевский институт МВД Республики Беларусь,
Могилев, Республика Беларусь,
shneidmimvd@mail.ru

Аннотация

Введение: статья посвящена анализу хищений в сфере оборота криптовалюты в структуре киберпреступности Республики Беларусь, направленному на выявление проблем тактического и процессуального характера, с которыми сталкиваются белорусские правоохранительные органы при расследовании указанной категории преступлений. Актуальность исследования обусловлена необходимостью поиска научно обоснованных способов решения выявленных проблем, способствующих повышению эффективности процесса расследования хищений в сфере оборота криптовалюты.

Материалы и методы: автором статьи изучены нормативные правовые акты, регулирующие оборот криптовалюты на территории Республики Беларусь и деятельность правоохранительных органов по расследованию преступлений, материалы судебной и следственной практики. При подготовке статьи, наряду с всеобщим методом познания, использовались общенаучные и частнонаучные методы: статистический метод, формально-юридический, системно-структурный метод, формально-логический метод и иные.

Обзор литературы: изучены труды белорусских и российских авторов, посвященные правовым вопросам оборота криптовалюты и отдельным аспектам методики расследования хищений в сфере оборота криптовалюты.

Результаты исследования: автором предложена система способов совершения хищений в сфере оборота криптовалюты на территории Республики Беларусь; определены проблемы получения криминалистически значимой информации по делам указанной категории, а также проблемы организационно-методического характера, влияющие на эффективность процесса расследования хищений криптовалют.

Обсуждение и заключение: определены способы повышения эффективности методики расследования хищений в сфере оборота криптовалюты за счет изменения белорусского подхода к правовому регулированию оборота криптовалюты, внедрения новых каналов получения криминалистически значимой информации из зарубежных источников, совершенствования тактики производства отдельных следственных и процессуальных действий.

Ключевые слова: криптовалюта; транзакции; хищение; владельцы криптовалюты; киберпреступность; проблемы расследования

Для цитирования: Шнейдерова Д.И. Хищения в сфере оборота криптовалюты в структуре киберпреступлений: виды, проблемы расследования (белорусский опыт) // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 4 (58). С. 161 – 170. DOI: 10.37973/VESTNIKKUI-2024-58-20

Scientific article
UDC 343.98
DOI: 10.37973/VESTNIKKUI-2024-58-20

THEFT IN THE SPHERE OF CRYPTOCURRENCY TURNOVER IN THE STRUCTURE OF CYBERCRIME: TYPES, PROBLEMS OF INVESTIGATION (BELARUSIAN EXPERIENCE)

Daria Igorevna Shneiderova
Mogilev Institute of the Ministry of Internal Affairs of the Republic of Belarus,
Mogilev, Republic of Belarus,
shneidmimvd@mail.ru

Abstract

Introduction: the article presents an analysis of the phenomenon of cryptocurrency theft within the context of cybercrime in the Republic of Belarus. The objective is to identify the tactical and procedural challenges encountered by Belarusian law enforcement agencies in investigating this category of crimes. The necessity for this research is determined by the requirement to identify scientifically sound methods of solving the problems identified, with the aim of improving the effectiveness of the investigation process of theft in the sphere of cryptocurrency turnover.

Materials and Methods: the author of the article has conducted a comprehensive investigation into the regulatory framework governing the turnover of cryptocurrency in the territory of the Republic of Belarus, as well as the activities of law enforcement agencies in investigating crimes. This involved a detailed analysis of relevant legal instruments and materials from judicial and investigative practice. In preparing this article, a variety of methods were employed, including the general method of cognition, as well as general and particular scientific methods. These included the statistical method, the formal-legal method, the system-structural method, the formal-logical method, and others.

Literature Review: a review of the literature was conducted, focusing on works by Belarusian and Russian authors that address legal issues related to cryptocurrency turnover and the methodology of investigating theft in this context.

Results revealed that the author proposed a system of methods for committing theft in the sphere of cryptocurrency turnover in the territory of the Republic of Belarus. Furthermore, the research identified the problems of obtaining criminalistically significant information in cases of this category, as well as organisational and methodological problems affecting the effectiveness of the investigation process of cryptocurrency theft.

Discussion and Conclusions: the ways of enhancing the efficacy of the investigative methodology for crimes involving cryptocurrency turnover by modifying the Belarusian approach to the legal regulation of cryptocurrency turnover, establishing new channels for acquiring criminologically significant information from foreign sources, and improving the tactics for conducting certain investigative and procedural actions have been identified.

Keywords: cryptocurrency; transactions; theft; cryptocurrency owners; cybercrime; investigation problems

For citation: Shneiderova D.I. Theft in the Sphere of Cryptocurrency Turnover in the Structure of Cybercrime: Types, Problems of Investigation (Belarusian Experience). Bulletin of the Kazan Law Institute of MIA of Russia. 2024;15(4):161-170. (In Russ.). DOI: 10.37973/VESTNIKKUI-2024-58-20

Введение

Киберпреступность – негативная, стремительно набирающая обороты тенденция мирового масштаба, характеризующая информационно-коммуникационную сферу в эпоху глобализации и компьютеризации экономического пространства. Прогрессивность киберпреступности на фоне иных категорий уголовно-наказуемых деяний подтверждается данными статистики, согласно которой пиковый рост зарегистрированных на территории Беларуси кибепреступлений приходится на 2020 г. (с 2 440 в

2015 г. до 25 561 в 2020 г.)[1]. Вместе с тем, несмотря на стабилизирование данной тенденции на протяжении 2021−2022 гг. (15503 в 2021 г. и 13990 в 2022 г.), на конец 2023 г. правоохранительные органы вновь констатировали рост киберпреступлений (за 2023 г. в Беларуси совершено около 20000)[2].

В теории уголовно-правовых наук киберпреступность – понятие собирательное. В связи с этим следует согласиться с мнением К.Н. Евдокимова и К.В. Хобонковой, что «киберпреступность – совокупность преступлений, совершенных с использованием компьютерных и информационно-коммуникационных технологий за определенный период времени в национальном либо международном сегменте сети Интернет» [1, с. 91]. В структуре характерных белорусской правоприменительной практике киберпреступлений выделяется два блока уголовно-наказуемых деяний:

1) преступления против компьютерной безопасности (собственно компьютерные преступления), т.е. те деяния, предметом преступного посягательства при совершении которых выступает компьютерная информация (например, несанкционированный доступ к компьютерной информации; уничтожение, блокирование или модификация компьютерной информации; неправомерное завладение компьютерной информацией и др.);

2) иные виды преступлений, при совершении которых используются информационно-коммуникационные технологии, а именно преступления против: мира и безопасности человечества; жизни и здоровья; уклада семейных отношений и интересов несовершеннолетних; личной свободы, чести и достоинства; конституционных прав и свобод человека и гражданина; собственности; порядка осуществления экономической деятельности; общественной безопасности; здоровья населения; общественного порядка и общественной нравственности; государства; порядка управления и иные. Следует констатировать, что практически в каждой главе Уголовного кодекса Республики Беларусь можно встретить несколько составов преступлений, в механизме которых задействованы продукты IT-индустрии. В свою очередь, более 90% указанных преступлений приходится на долю хищений[3].

С начала развития в Республике Беларусь криптовалютной индустрии в группе киберхищений образовалась новая подкатегория преступлений, в механизме которых криптовалюта выступает либо в качестве предмета преступного посягательства, поскольку обладает имущественной ценностью, либо в качестве средства противоправного завладения фиатными или электронными деньгами. На данный момент наблюдается тенденция увеличения спроса на криптовалюту среди пользователей белорусского сегмента сети Интернет, о чем свидетельствует и количественный прирост криптобирж и криптообменников, зарегистрированных в качестве резидентов Парка высоких технологий Республики Беларусь. Если на конец 2023 г. количество таких криптоплатформ составляло 3, то уже ко второму полугодию 2024 г. достигло 9: IMEX, Secure8, TRADEX, Dzengi.com, Finstore, BYNEX, FREE2EX, Whitebird, FainEX[4]. Из изложенного усматривается следующая закономерность: увеличение спроса на криптовалюту приводит к росту хищений в сфере ее оборота, практика расследования которых столкнулась с рядом проблем организационно-методического, процессуального и тактического характера, вызванных спецификой криптовалют и инструментов их оборота, а также сложностью получения криминалистически значимой информации из зарубежных источников, что в совокупности предопределяет актуальность темы настоящей статьи и ее практическую значимость.

При этом настоящее исследование ставит своими задачами приведение краткого обзора основных положений правового регулирования оборота криптовалюты в Беларуси; структурирование системы видов хищений в сфере оборота криптовалюты и непосредственных способов их совершения; выделение проблем, с которыми сталкиваются правоохранительные органы при расследовании указанных хищений, и предложение оптимальных путей их устранения.

Обзор литературы

В рамках исследования хищений в сфере оборота криптовалюты с позиции уголовно-право-

[1] Киберпреступность в Беларуси. URL: https://www.belta.by/infographica/view/kiberprestupnost-v-belarusi-24963/(дата обращения: 07.11.2024).

[2] В Беларуси за 2023 год совершено около 20 тыс. киберпреступлений. URL: https://belta.by/society/view/gora-v-belarusi-za-2023-god-sovershено-okolo-20-tys-kiberprestuplenij-627270-2024/(дата обращения: 07.11.2024).

[3] В Беларуси в 2023 году зафиксировано более 10 тыс. киберпреступлений. URL: https://www.belta.by/society/view/v-belarusi-v-2023-godu-zafiksirovano-bolee-10-tys-kiberprestuplenij-585322-2023/(дата обращения: 07.11.2024).

[4] Резиденты ПВТ. URL: https://www.park.by/residents/?q=&UNP=&search=Y&STAFF=&EXPER=&TARGET%5B%5D=831&TARGET%5B%5D=832&TARGET%5B%5D=833&TARGET%5B%5D=834&TARGET%5B%5D=835&save=Найти(дата обращения: 07.11.2024).

вых наук обращалось внимание на особенности правового статуса криптовалюты как предмета преступного посягательства и порядка правового регулирования ее оборота, которые нашли отражение в трудах А.Ю. Богданкевич, М.Х. Боранукова, С.С. Вабищевич, С.В. Горбунова, М.М. Долгиевой, Г.Р. Игбаевой, А.Г. Корчагина, И.А. Маньковского, А.В. Токолова, В.Н. Усоского, В.В. Хилюты, Н.В. Шепель, А.А. Яковенко и других авторов. Кроме того, непосредственно вопросам методики расследования преступлений с криптовалютой и ее структурным элементам, тактике производства следственных действий и особенностям получения криминалистически значимой информации по рассматриваемой категории преступлений посвящены работы Н.Н. Беломытцева, Ж.А. Борисовой, А.Д. Валесюк, С.Л. Гамко, М.В. Губич, В.П. Зайцева, И.А. Ишина, А.А. Карпова, И.Б. Колчевского, А.Г. Кузнецова, Э.С. Маркаряна, Л.Л. Мельника, О.А. Никулиной, Н.В. Олиндер, Р.С. Поздышева, Д.А. Романюка, С.В. Рыбака, А.Г. Саакяна, А.А. Титова, В.Н. Усоского, А.Ю. Ушакова и иных белорусских и российских авторов. Особенности и проблемные вопросы международного взаимодействия по уголовным делам о киберпреступлениях рассматривались в работах В.Р. Атнашева и С.Н. Яхъеевой, М.Г. Головенчик, К.Н. Евдокимова и К.В. Хобонковой, К.К. Клевцова, А.О. Миронова, А.Ф. Остряковой и Т.С. Спешиловой, Т.В. Пинкевич, В.Ч. Родевич и С.С. Тупеко, Ш.М. Саргсяна, Я.М. Хаминского, Е.М. Якимовой и С.В. Нарутто и иных.

Материалы и методы

Эмпирическую основу исследования составили положения действующего законодательства, регулирующего оборот криптовалюты на территории Республики Беларусь и деятельность правоохранительных органов по расследованию хищений в сфере оборота криптовалюты, в частности нормы Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики», указа Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)», Уголовно-процессуального кодекса Республики Беларусь (далее – УПК Республики Беларусь); научные труды белорусских и зарубежных авторов; результаты проведенного в рамках исследования анкетирования следователей подразделений Следственного комитета Республики Беларусь. Методологической основой статьи послужили положения материалистической диалектики как всеобщего метода познания. При подготовке статьи использовались общенаучные (анализ, синтез, индукция, дедукция, сравнение, обобщение и другие) и частнонаучные (статистический метод, формально-юридический, системно-структурный метод, формально-логический метод и иные) методы познания.

Результаты исследования

В Республике Беларусь правовой статус криптовалюты нормативно закреплен Декретом Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» (далее – Декрет № 8), согласно п. 4 приложения № 1 которого под *криптовалютой* следует понимать биткоин, иной цифровой знак (токен), используемый в международном обороте в качестве универсального средства обмена[1]. При этом белорусский законодатель, закрепив за криптовалютой статус универсального средства обмена (т.е. ее конвертируемость на иные токены, криптовалюту, белорусские рубли и иностранную валюту), в то же время не рассматривает ее как средство платежа, т.е. расчеты криптовалютой в Беларуси запрещены. Исключение составляют лишь расчеты с операторами криптоплатформ, которые получают криптовалюту в качестве комиссии (вознаграждения) за проведенные транзакции (п. 2.4 Декрета № 8).

Владельцами криптовалюты в Республике Беларусь признаются субъекты гражданского права (физические и юридические лица, индивидуальные предприниматели), которым криптовалюта принадлежит на праве собственности или на ином вещном праве (п. 3 приложения № 1 к Декрету № 8). Пунктами 2.1 и 2.2 Декрета № 8 установлен и перечень правомочий владельцев криптовалют. Так, владельцы криптовалюты вправе совершать следующие операции с ней: хранение в виртуальных кошельках, майнинг, обмен на иные токены, приобретение, отчуждение за белорусские рубли, иностранную валюту, электронные деньги. Кроме того, физические лица также вправе дарить и завещать криптовалюту, а юридические лица и индивидуальные предприниматели создавать и размещать собственную криптовалюту в Республике Беларусь и за рубежом через операторов – резидентов Парка высоких технологий.

Легализация белорусским законодателем правового статуса криптовалюты позволила правоохранительным органам возбуждать уголовные дела по фактам ее хищений по статьям 208, 209

[1] О развитии цифровой экономики: Декрет Президента Респ. Беларусь от 21.12.2017 № 8 (в ред. Декрета Президента Респ. Беларусь от 18.03.2021 № 1). НЦПИ Респ. Беларусь «ЭТАЛОН – ONLINE» (дата обращения: 07.11.2024).

и 212 Уголовного кодекса Республики Беларусь (далее – УК). Несмотря на незначительность по количественному показателю фактов хищений в сфере оборота криптовалюты по отношению к иным видам хищений и киберпреступлений в целом (чуть более 1,5 % от общего количества), доля раскрываемости таких преступлений крайне мала (чуть более 3 %). Из общего количества зарегистрированных и расследуемых белорусскими правоохранительными органами хищений в сфере оборота криптовалюты только по 11 фактам удалось установить лиц, совершивших преступления, и направить уголовные дела в суд. Все остальные уголовные дела либо в подавляющем большинстве приостановлены в связи неустановлением лица, подлежащего привлечению в качестве обвиняемого, либо находятся в процессе расследования.

В Беларуси хищения в сфере оборота криптовалюты представлены такими формами, как вымогательство (ст. 208 УК), мошенничество (ст. 209 УК) и хищение путем модификации компьютерной информации (ст. 212 УК), каждой из которых присущи свои способы непосредственного совершения преступления:

1) способы совершения вымогательства: путем распространения вирусных программ-блокираторов; путем направления текстовых сообщений по электронной почте, в социальных сетях или мессенджерах с требованием выкупа под угрозой распространения клеветнических сведений о потерпевшем и / или сведений о его личной жизни, которые последний желает сохранить в тайне либо под угрозой уничтожения имущества потерпевшего или юридического лица;

2) способы совершения мошенничества: путем обмана под предлогом совершения гражданско-правовых сделок – потребительское мошенничество (связано с осуществлением сделок по купле или продаже криптовалюты (обменные операции) потерпевшему либо продаже товара, сдаче в аренду объектов недвижимости под условием расчета в криптовалюте); путем обмана под предлогом оказания посреднических услуг (сопровождение (осуществление в интересах потерпевшего) процедуры регистрации криптокошелька (аккаунта на бирже) и / или покупки криптовалюты с зачислением на созданный либо ранее зарегистрированный потерпевшим кошелек; обучение и сопровождение трейдинга криптовалютой, т.е. совершение периодических обменных операций и биржевых торгов криптовалютой с целью получения дохода на курсовых разницах; обеспечение возврата похищенной криптовалюты);

3) способы совершения хищения путем модификации компьютерной информации: посредством несанкционированного доступа к криптовалютному кошельку, полученного путем подбора (неправомерного получения) данных авторизации криптокошелька; путем неправомерного использования данных авторизации, установленных через фишинговые веб-страницы; путем неправомерного использования данных авторизации, установленных через вредоносное программное обеспечение; посредством несанкционированного доступа к счету криптобиржи, полученного путем неправомерного использования реквизитов подарочной карты криптовалютной биржи; посредством несанкционированного доступа к банковскому счету потерпевшего, полученного путем неправомерного использования реквизитов банковской платежной карты, установленных через фишинговые веб-страницы или вишинг.

Хищениям в сфере оборота криптовалюты присуща общая специфика киберпреступлений, которая выражается, по мнению А.Ф. Остряковой и Т.С. Спешиловой, в их транснациональном характере, высоком уровне латентности, довольно низких показателях раскрываемости и возможности нанесения значительного материального ущерба при минимальных затратах на подготовку преступления [2, с. 103]. Трансграничность, как основной показатель, характеризуется территориальным разграничением мест совершения преступления и наступления его последствий, нахождением физических носителей цифровых следов и разыскиваемых преступников преимущественно за рубежом. Данное обстоятельство подтверждает востребованность международного сотрудничества в области взаимодействия правоохранительных органов на первоначальном этапе расследования хищений в сфере оборота криптовалюты, которое на сегодняшний день имеет ряд нерешенных вопросов.

Ключевая проблема в данной области заключается в крайне низкой результативности получения необходимой для процесса расследования информации, источниками которой являются зарубежные криптосервисы и иные интернет-ресурсы, провайдеры Сети, мобильные операторы, что также оказывает негативное влияние и на эффективность розыска и задержания лиц, совершивших или причастных к совершению хищений в сфере оборота криптовалюты, территориально находящихся за пределами Беларуси. Как следствие, указанная проблема приводит к приостановлению расследования уголовных дел, порождая отрицательную статистику раскрываемости.

В рамках исследования проводилось анкетирование следователей подразделений Следственного комитета Республики Беларусь относительно проблем, возникающих на этапе получения криминалистически значимой информации из зарубежных источников, по результатам которого анкетируемыми были отмечены следующие отрицательные тенденции в данной области: имеют место частые отказы в предоставлении информации и проведении следственных действий на территории других государств, в отдельных случаях ответы содержат не соответствующие запросу сведения; имеются трудности в получении сведений от зарубежных криптоплатформ, обусловленные особенностями их корпоративной политики; длительное время ожидания ответа на международный запрос, что тормозит процесс расследования и дает возможность преступнику уничтожить цифровые следы; запрос направлен по материалу проверки, тогда как сотрудничество с данной стороной может осуществляться только в рамках возбужденного уголовного дела; хищение криптовалюты не является преступным деянием в соответствии с уголовным законодательством иностранного государства, соответственно, в исполнении запроса отказывается; размер материального ущерба, причиненного хищением криптовалюты на территории Республики Беларусь, недостаточный для наступления уголовной ответственности за аналогичное деяние на территории иностранного государства, которому направлен запрос.

Анализ научной литературы позволил прийти к выводу, что ряд обозначенных проблем характерен и правоохранительной практике Российской Федерации. Так, на проблему отсутствия в уголовном законодательстве ряда зарубежных государств нормы, предусматривающей ответственность за нарушение имущественных отношений, связанных с оборотом криптовалюты, обратила внимание Т.В. Пинкевич. Автор отмечает, что, несмотря на то, что криптовалюта приобрела высокую популярность в ряде стран и активно используется как платежное средство и инвестиционный актив, уголовная ответственность за посягательства в сфере оборота криптовалюты в них по-прежнему не установлена (например, в Германии, Швеции, Великобритании, США, Франции и иных) [3, с. 90-91]. Ш.М. Саргсян указывает, что на территории отдельных государств за деяния, относящиеся к категории киберпреступлений, может быть предусмотрено более мягкое наказанием, чем в стране, где расследуется уголовное дело по факту его совершения, что является препятствием к получению по международному запросу требуемой информации [4, с. 202].

К.К. Клевцов обращает внимание на проблему длительности сроков получения электронной информации в рамках исполнения запроса об оказании правовой помощи, вызванную наличием определенных сроков хранения цифровых данных, которые могут быть превышены при исполнении международного запроса, что, как следствие, приведет к их потере и негативно отразиться на досудебном производстве по уголовным делам о киберпреступлениях [5, с. 679].

Проблемы получения криминалистически значимой информации из зарубежных источников, несомненно, являются ключевыми в вопросах эффективности расследования хищений в сфере оборота криптовалют, но не единственными. Так, следует отметить и такие проблемные аспекты, негативно влияющие на процесс расследования, как:

1) недостаточная подготовка сотрудников правоохранительных органов, осуществляющих расследование хищений в сфере оборота криптовалюты, ввиду отсутствия специальных знаний в области информационных технологий и порядка проведения операций с криптовалютой, а также отсутствие комплексного организационно-методического сопровождения процесса расследования хищений в сфере оборота криптовалюты;

2) отсутствие надлежащего общеустановленного алгоритма конвертации суммы похищенной криптовалюты на белорусские рубли. На сегодняшний день в Беларуси применяются два способа конвертации: либо установление курса криптовалюты по отношению к доллару США через любую общедоступную криптобиржу, обменник или аналитические сайты, отслеживающие курсы криптовалюты на различных биржах и определяющие средневзвешенное значение; либо установление курса криптовалюты по отношению к доллару США через показатели конвертации, предусмотренные встроенным в криптокошелек потерпевшего обменником. Разобщенность подходов приводит к дифференциации счетного показателя, влияющего на общий размер причиненного имущественного вреда;

3) наблюдается разобщенность подходов и в вопросе установления принадлежности криптокошелька потерпевшему, с которого похищена криптовалюта. Проведенное нами исследование дает основание утверждать, что принадлежность криптокошелька потерпевшему устанавливается либо с его слов на основе обладания данными авторизации криптокошелька, либо путем осмотра

устройства потерпевшего и находящейся на нем компьютерной информации, либо путем направления запроса владельцу криптоплатформы (кошелька, биржи, обменника), либо путем осмотра криптокошелька с целью обнаружения привязанных к нему иных данных потерпевшего (абонентского номера, реквизитов банковской карты), либо не устанавливается вовсе;

4) отсутствие законодательно закрепленной процессуальной возможности производства осмотра компьютерной информации в процессе обыска в условиях неотложности. К примеру, в ходе обыска обнаружен ноутбук, на котором запущен браузер и осуществлен вход в онлайн-криптокошелек подозреваемого. Предупреждая возможность перевода криптовалюты на иной кошелек сообщником подозреваемого, лицо, производящее обыск, должно незамедлительно провести осмотр данной компьютерной информации, зафиксировать веб-страницы путем производства скриншотов или фотографирования, наложить арест на криптовалюту. По мнению Л.Л. Мельника, в подобных случаях обыск необходимо приостановить и провести осмотр компьютерной информации [6, с. 149]. С точки зрения тактики целесообразность данного пути сомнений не вызывает, однако уголовно-процессуальная возможность для таких действий на сегодняшний день не предусмотрена.

Часть 13[1] ст. 210 УПК Республики Беларусь предписывает, что при проведении обыска допустимо копирование компьютерной информации в отображаемой форме (в том числе создание образа носителя) при невозможности или нецелесообразности изъятия объекта, ее содержащего[1]. Исходя из этого положения, проводить осмотр криптовалютного кошелька и налагать арест на криптовалюту подозреваемого в ходе обыска, так же как и приостанавливать его для этих целей, незаконно. Кроме того, копирование допустимо тогда, когда изъять устройство невозможно или нецелесообразно, однако в большинстве случаев потребуется не только осмотреть информацию в режиме неотложности, но и изъять после этого само устройство, так как на нем могут быть обнаружены иные имеющие значение для дела данные. Таким образом, имеющие место в правоприменительной практике ситуации, когда в процессе обыска необходимо незамедлительно осмотреть содержимое устройства, аккаунт социальной сети, личный кабинет банкинга, транзакции кошелька, аккаунт криптобиржи и иное в связи с возможностью удаленного доступа к этой информации и ее искажения либо уничтожения третьими лицами, не нашли разрешения в уголовно-процессуальных нормах.

Обсуждение и заключение

Преодоление обозначенных в настоящей статье проблемных вопросов, возникающих в процессе расследования хищений в сфере оборота криптовалюты, возможно следующим образом:

1. По мнению отдельных авторов, традиционные механизмы международного взаимодействия по уголовным делам являются не актуальным в сфере борьбы с киберпреступностью, в связи с этим назрела необходимость установления нового межгосударственного формата оказания правовой помощи по уголовным делам. По мнению Е.М. Якимовой и С.В. Нарутто, международное сотрудничество должно осуществляться путем разработки нормативных актов и выработки общих рекомендаций по противодействию киберугрозам, а также внедрения эффективных моделей организационного взаимодействия между правоохранительными органами различных государств [7, с. 372]. Схожего мнения придерживаются В.Р. Атнашев и С.Н. Яхъеева, которые указывают на необходимость унификации правовых норм всех государств в области киберпреступлений и создания системы координации всех существующих служб противодействия киберпреступности [8, с. 41]. Трудно не согласиться с точкой зрения Я.М. Хаминского, отмечающего, что борьба с преступлениями в сфере оборота криптовалюты силами одного государства невозможна [9, с. 57].

В то же время А.О. Миронов приходит к выводу, что «учитывая внешнеполитическую обстановку и нарастающую напряженность между странами, существует угроза если не полного прекращения сотрудничества в правоохранительной сфере, то возможного ослабления данных отношений, что негативным образом скажется на криминогенной обстановке в сфере киберпреступности» [10, с. 190]. Соглашаясь с выводами указанного автора, отметим, что сегодня международное взаимодействие по уголовным делам о хищениях в сфере оборота криптовалюты, равно как и по иным видам трансграничных преступлений, имеет фрагментарный характер ввиду национальных и политических интересов отдельных государств. В связи с этим (не оставляя попыток наладить международное взаимодействие в сфере борьбы с киберпреступлениями) представляется

[1] Уголовно-процессуальный кодекс Республики Беларусь от 16.07.1999 № 295-З (в ред. Закона Респ. Беларусь от 08.01.2024 г. № 349-З). НЦПИ Респ. Беларусь «ЭТАЛОН – ONLINE» (дата обращения: 07.11.2024).

целесообразным изменение внутригосударственного подхода к правовому регулированию оборота криптовалюты на территории Республики Беларусь, который выражается в ограничении реализации правомочий владельцев криптовалюты через операторов криптоплатформ, взаимодействующих с правоохранительными органами в сфере оказания помощи по уголовным делам (в частности, предоставляющих сведения о сторонах криптовалютных операций).

Белорусский законодатель уже предпринял первые шаги в данном направлении. Так, если до середины сентября 2024 г. физические лица были правомочны осуществлять операции с криптовалютой через любых операторов криптоплатформ, в отличие от юридических лиц и индивидуальных предпринимателей, то с момента официального опубликования указа Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)» эти операции физические лица вправе осуществлять только через операторов криптоплатформ и операторов обмена криптовалют, являющихся резидентами Парка высоких технологий. В то же время в целях исключения монополизации белорусских криптоплатформ перед зарубежными представляется целесообразным расширить перечень доступных пользователям белорусского сегмента Сети криптосервисов посредством приглашения к сотрудничеству зарубежных криптоплатформ с белорусскими операторами – резидентами Парка высоких технологий, между которыми обязательным должно стать заключение соглашения о сотрудничестве по оказанию правовой помощи по уголовным делам.

При этом практикоориентированным видится и особый алгоритм взаимодействия правоохранительных органов с операторами – резидентами Парка высоких технологий и их зарубежными партнерами, с которыми заключено указанное выше соглашение по оперативному получению криминалистически значимой информации о криптовалютных транзакциях и сторонах, их осуществивших. Такой алгоритм предусматривает направление запроса об оказании содействия в предоставлении необходимой расследованию информации непосредственно от правоохранительного органа зарубежному криптосервису – партеру резидента Парка высоких технологий через оператора – резидента Парка высоких технологий, заключившего с ним соглашение о сотрудничестве по оказанию правовой помощи по уголовным делам, что позволит сократить время, затрачиваемое на подготовку, отправку и исполнение стандартной международной просьбы от нескольких месяцев до 3-5 дней. Представляется, что предложенные меры позволят обеспечить надежность криптовалютных операций, снизить риск хищений, сформировать новые каналы получения информации, а также сократить количество заведомо нераскрываемых уголовных дел ввиду невозможности получения доказательственной информации из-за рубежа и деанонимизирования личности преступников.

2. Проблема обеспечения правоохранительных органов высококвалифицированными сотрудниками, обладающими необходимым комплексом знаний в сфере IT, находится на данный момент в стадии ликвидации за счет организации обучения по направлению расследования киберпреступлений в форме повышения квалификации для действующих следователей и оперативных сотрудников, а также введения в учреждениях высшего образования, осуществляющих подготовку будущих правоохранителей, узкой специализации, сочетающей освоение обучающимися необходимых для расследования преступлений, совершаемых с использованием информационных технологий, знаний по юридическому и техническому профилю. Вместе с тем не следует забывать, что киберпреступность – явление стремительно развивающееся и повышение квалификации должно носить периодический, а не разовый характер.

Обеспечение сотрудников правоохранительных органов качественным комплексом методического сопровождения процесса расследования хищений в сфере оборота криптовалют может быть достигнуто посредством обобщения результатов научных исследований, проведенных учеными-теоретиками совместно с практическими работниками правоохранительных органов, в том числе с учетом преемственности положительного зарубежного опыта расследования указанных преступлений. Такой методический комплекс должен содержать терминологический словарь с ключевыми понятиями, характерными хищениям криптовалют (например, хеш, блокчейн-обозреватель, входы и выходы транакции и др.), характеристику способов совершения хищений с практическими примерами (в том числе подкрепленными наглядным материалом в виде схем, рисунков), источники и виды присущих хищениям данной группы цифровых следов, возможности по их обнаружению и анализу с использованием общедоступных веб-сервисов и ботов, тактику и специфику производства следственных действий (обыск, осмотр, допрос, наложение ареста и т.д.), основы планирования расследования,

алгоритмы международного взаимодействия с примерами формулировок запросов.

3. В целях установления единообразного алгоритма определения курса конвертации криптовалюты на национальную валюту представляется целесообразным заключение межведомственного соглашения белорусских правоохранительных органов, в соответствии с которым будет определен единый для всех источник получения сведений о курсах криптовалюты к белорусскому рублю (например, им может выступать один из криптообменников – резидентов Парка высоких технологий).

4. При установлении принадлежности криптокошелька потерпевшему или подозреваемому оптимальным представляется следующий алгоритм процессуальных действий: получение от потерпевшего / подозреваемого сведений о виде и платформе криптокошелька, наличии у него данных авторизации; установление в ходе осмотра компьютерной информации на устройстве владельца кошелька использованных для доступа к нему программ, приложений, браузеров; осмотр кабинета криптокошелька на предмет наличия привязанных к нему данных владельца (абонентский номер, реквизиты банковской карты, электронная почта) и использованного им устройства (вид, IP-, MAC-адрес); направление запроса о предоставлении данных владельца проверяемого кошелька платформе криптокошелька.

5. В случаях когда при производстве обыска по делам о хищениях в сфере оборота криптовалюты возникла необходимость в неотложном проведении осмотра компьютерной информации в целях обнаружения и закрепления цифровых следов, иной имеющей значение информации, а равно в целях наложения ареста на криптовалюту, тактически целесообразно проводить осмотр компьютерной информации непосредственно в ходе обыска, не приостанавливая процесс поисковых действий, что позволит минимизировать вероятность потери или модификации цифровых данных ввиду промедления с производством осмотра, а также обеспечить оперативный доступ к источникам криминалистически значимой информации. Для обеспечения процессуальной возможности одновременного производства обыска и осмотра компьютерной информации рекомендуется внести соответствующее дополнение в нормы уголовно-процессуального законодательства.

Таким образом, комплекс обозначенных в статье проблемных вопросов, возникающих в процессе расследования хищений в сфере оборота криптовалюты, обусловливает актуальность разработки эффективных мер, направленных на противодействие преступлениям, формированию которых способствует интеграция опыта практической деятельности правоохранительных органов (как белорусских, так и зарубежных), научных изысканий в указанном направлении, а также модернизация образовательных программ профильных учреждений высшего образования, нацеленная на подготовку будущих сотрудников правоохранительных органов.

СПИСОК ИСТОЧНИКОВ

1. Евдокимов К.Н., Хобонкова К.В. К проблеме совершенствования международного сотрудничества в сфере противодействия киберпреступности // Сибирский юридический вестник. 2022. № 3 (98). С. 90–95. DOI: 10.26516/2071-8136.2022.3.90

2. Острякова А.Ф., Спешилова Т.С. Международное взаимодействие в сфере борьбы с киберпреступностью // Аграрное и земельное право. 2021. № 8 (200). С. 102–105. DOI: 10.47643/18151329_2021_8_102

3. Пинкевич Т.В. Зарубежный опыт противодействия преступной деятельности с использованием криптовалюты // Научный портал МВД России. 2020. № 3 (51). С. 87–93.

4. Саргсян Ш.М. Международное сотрудничество в борьбе с киберпреступностью: отдельные проблемы и пути их решений. URL: https://odin.mgimo.ru/images/files/2021/06/sargsyan.pdf, свободный (дата обращения: 07.11.2024).

5. Клевцов К.К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам // Вестник Санкт-Петербургского университета. Право. 2022. № 3. С. 678–695. DOI: 10.21638/spbu14.2022.306

6. Мельник Л.Л. О некоторых аспектах рабочего этапа обыска при расследовании преступлений, совершенных с использованием токенов и электронных денег // Вестник Акад. МВД Респ. Беларусь. 2022. № 1. С. 147–152.

7. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. № 2. С. 369–378. DOI: 10.17150/1996-7756.2016.10(2)369-378

8. Атнашев В.Р., Яхъеева С.Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // Евразийская интеграция: экономика, право, политика. 2019. № 3. С. 37–42.
9. Хаминский Я.М. Анализ преступлений международного характера, связанных с криптовалютами // Advances in Law Studies. 2022. №. 3. С. 56–60. DOI: 10.29039/2409-5087-2022-10-3-56-60
10. Миронов А.О. Проблемы международного сотрудничества в сфере борьбы с киберпреступлениями // Актуальные проблемы политики противодействия преступности: материалы Всероссийской научно-практической конференции, Иркутск, 27 сентября 2022 г. Иркутск: Байкальский государственный университет, 2023. С. 188–193.

REFERENCES

1. Evdokimov K.N., Hobonkova K.V. K probleme sovershenstvovaniya mezhdunarodnogo sotrudnichestva v sfere protivodejstviya kiberprestupnosti // Sibirskij yuridicheskij vestnik. 2022. №3 (98). S. 90–95. DOI: 10.26516/2071-8136.2022.3.90
2. Ostryakova A.F., Speshilova T.S. Mezhdunarodnoe vzaimodejstvie v sfere bor'by s kiberprestupnost'yu // Agrarnoe i zemel'noe pravo. 2021. № 8 (200). S. 102–105. DOI: 10.47643/18151329_2021_8_102
3. Pinkevich T.V. Zarubezhnyj opyt protivodejstviya prestupnoj deyatel'nosti s ispol'zovaniem kriptovalyuty // Nauchnyj portal MVD Rossii. 2020. № 3 (51). S. 87–93.
4. Sargsyan Sh.M. Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupnost'yu: otdel'nye problemy i puti ih reshenij. URL: https://odin.mgimo.ru/images/files/2021/06/sargsyan.pdf, svobodnyj (data obrashcheniya: 07.11.2024).
5. Klevcov K.K. Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupnost'yu v kontekste protivodejstviya novym vyzovam i ugrozam // Vestnik Sankt-Peterburgskogo universiteta. Pravo. 2022. № 3. S. 678–695. DOI: 10.21638/spbu14.2022.306
6. Mel'nik L.L. O nekotoryh aspektah rabochego etapa obyska pri rassledovanii prestuplenij, sovershennyh s ispol'zovaniem tokenov i elektronnyh deneg // Vestnik Akad. MVD Resp. Belarus'. 2022. № 1. S. 147–152.
7. Yakimova E.M., Narutto S.V. Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupnost'yu // Vserossijskij kriminologicheskij zhurnal. 2016. № 2. S. 369–378. DOI: 10.17150/1996-7756.2016.10(2)369-378
8. Atnashev V.R., Yah"eeva S.N. Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupnost'yu i kiberterrorizmom // Evrazijskaya integraciya: ekonomika, pravo, politika. 2019. № 3. S. 37–42.
9. Haminskij Ya.M. Analiz prestuplenij mezhdunarodnogo haraktera, svyazannyh s kriptovalyutami // Advances in Law Studies. 2022. №. 3. S. 56–60. DOI: 10.29039/2409-5087-2022-10-3-56-60
10. Mironov A.O. Problemy mezhdunarodnogo sotrudnichestva v sfere bor'by s kiberprestupleniyami // Aktual'nye problemy politiki protivodejstviya prestupnosti: materialy Vserossijskoj nauchno-prakticheskoj konferencii, Irkutsk, 27 sentyabrya 2022 g. Irkutsk: Bajkal'skij gosudarstvennyj universitet, 2023. S. 188–193.

Информация об авторе:
Шнейдерова Дарья Игоревна, старший преподаватель кафедры уголовного права, уголовного процесса и криминалистики Могилевского института МВД Республики Беларусь, shneidmimvd@mail.ru
Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Shneiderova Daria I., Senior Lecturer of the Department of Criminal Law, Criminal Procedure and Criminalistics, Mogilev Institute of the Ministry of Internal Affairs of the Republic of Belarus, shneidmimvd@mail.ru
The author has read and approved the final version of the manuscript.

Статья получена: 09.11.2024.
Статья принята к публикации: 24.12.2024.
Статья опубликована онлайн: 24.12.2024.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.