УДК 343.985.7 DOI: 10.17277/pravo.2022.02.pp.241-247

Представлена авторская позиция, направленная на исследование некоторых особенностей раскрытия и расследования киберпреступлений в современном мире глобальной цифровизации. Рассмотрены тактические особенности раскрытия и расследования преступлений, совершаемых с помощью криптовалют и майнинга. Определены проблемы, возникающие при раскрытии и расследовании киберпреступлений, а также пути их решения.

Рассмотрены условия и особенности, необходимые для качественного раскрытия и расследования киберпреступлений, которые связанны со спецификой данных преступлений. Представлена технология блокчейна, способствующая раскрытию киберпреступлений. Определены условия, влияющие на успешное расследование указанной категории преступлений. Рассмотрены отличительные качества технологии блокчейна, которые влияют на использование криптовалюты организациями, осуществляющими противоправную деятельность. Представлены выводы по поводу пресечения, предупреждения и раскрытия преступлений указанной категории.

Ключевые слова: информационные технологии; информация; цифровизация; раскрытие и расследование преступлений; киберпреступления; криптовалюта; майнинг; цифровизация.

Денис Валентинович Теткин, *канд. юрид. наук, подполковник полиции, доцент, кафедра уголовного процесса, Рязанский филиал ФГКОУ ФО «Московский университет МВД России имени В. Я. Кикотя», Рязань, Россия; tyotkinden@mail.ru*

Андрей Анатольевич Пудовкин, *канд. юрид. наук, полковник полиции, начальник кафедры уголовного процесса, Рязанский филиал ФГКОУ ФО «Московский университет МВД России имени В. Я. Кикотя», Рязань, Россия; mr.andre.81@mail.ru*

Александр Алексеевич Троицкий, *рядовой полиции, консультант научного общества курсантов и слушателей, кафедра уголовного процесса, Рязанский филиал ФГКОУ ФО «Московский университет МВД России имени В. Я. Кикотя», Рязань, Россия; westgarx@mail.ru*

НЕКОТОРЫЕ ОСОБЕННОСТИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ В СОВРЕМЕННОМ МИРЕ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ

Введение

В современном мире глобальной цифровизации киберпреступность становится новой мировой тенденцией. Средства и методы, используемые хакерами, постоянно улучшаются в стремлении похитить гораздо больше финансовых активов. Возникают закономерные вопросы в современном

мире глобальной цифровизации: каким образом должны противостоять злоумышленникам правоохранительные органы; почему профессиональная квалификация сотрудников никак не повышается?

Результаты и обсуждения

Наше мнение по данному поводу определяет, что критика деятельности сотрудников правоохранительных органов безосновательна, как и заявления о том, что преступления в указанной сфере не раскрываются. История развития правоохранительных органов является длительной и динамично развивающейся [5, с. 14 – 31]. Оснований допускать, что преступления в сфере криптовалют будут оставаться слепым пятном для органов внутренних дел, нет. В связи с тем, что технология блокчейна все еще находится на самой ранней стадии развития, имеется реальная возможность упростить работу сотрудникам полиции. Блокчейн, на который злоумышленники возлагают свои надежды остаться анонимными, может помочь правоохранительным органам в борьбе с киберпреступностью.

Между тем при раскрытии преступлений с использованием криптовалют органам предварительного расследования необходимо обладать сведениями о порядке оборота криптовалюты, об обороте осуществлений транзакций, о самой платежной системе и т.д. То есть успешное расследование данных преступлений возможно лишь при условии наличия квалифицированных специалистов в области IT-технологий (информационно-коммуникационных технологий).

Для качественного раскрытия и расследования киберпреступлений следует установить событие, время и место совершения киберпреступлений, так как фиксация данных обстоятельств также имеет свои особенности, связанные со спецификой этих преступлений. Так, в силу особенностей проведения операций с криптовалютами могут не совпадать местоположение преступника с местоположением аппаратных и программных средств совершения преступления. Между тем мы знаем, что одним из немаловажных условий при расследовании всех преступлений, и преступления, которые совершаются с использованием криптовалют, не являются исключением, – это установление события преступления. Однако, как было отмечено выше, событие киберпреступлений имеет свои особенности, которые связаны со спецификой таких его существенных элементов, подлежащих установлению, как время и место совершения преступления.

При расследовании преступлений, которые совершаются с использованием криптовалют, следует учитывать тот факт, что время совершения преступления имеет свои особенности, так как разнообразные подсистемы компьютера фиксируют время того либо иного события в разных часовых поясах и разной кодировке.

А также в связи с тем, что выпуск криптовалюты возможен лишь в цифровом варианте, теоретически в любое время любой участник Сети может ее «майнить», то есть добывать. При этом Сеть распределяется между ее участниками и органа, который контролировал бы данную Сеть. Следовательно, при таких обстоятельствах трудно как-то установить статус участника данного рынка.

Почему и как технология блокчейна способствует раскрытию преступлений? Не является секретом, что одной из задач, стоящей перед правоохранителями при расследовании киберпреступлений, стоит определение MAC-адреса преступника. Это является достаточно сложно исполнимой задачей в случае, если кто-то использует несколько IP-адресов, TOR, прокси и т.д.

Вспомним об особенности блокчейна – способности отслеживать все транзакции определенного адреса, причем до самой первой транзакции, сделанной с него. Это позволяет отслеживать движения средств так, как это было невозможно никогда ранее. Выходит, что и биткоин не так анонимен, как о нем говорят. Биткоин-адрес – это, в теории, номер счета. Если вы можете связать человека с адресом, то вы сможете узнать все транзакции, которые сделал данный человек.

Камнем преткновения при расследовании киберпреступлений выступают операторы интернет-соединения. Каждый из них имеет свои правила, а если он территориально расположен или документально оформлен за границей, вопрос о предоставлении персональных данных по транзакции может растянуться на годы. В таком случае, есть вероятность, что провайдер удалил данные. Блокчейн, в свою очередь, хранит данные вечно. Процедура их получения – намного легче. Для получения же истории транзакции при работе с блокчейном не требуются документы в силу его открытости [2, с. 52–53].

Здесь следует упомянуть специфику следообразования транзакций криптовалюты. Каждый перевод, каждая операция – это новая запись в блоке данных. Следовательно, в процессе расследования неправомерного использования криптовалюты, время, адрес, количество и другие характеристики будут известны при чтении блока. Более того, некоторая информация о пользователях, совершивших сделку, также сохраняется блокчейном. Соответственно, получить указанную информацию не стоит больших усилий, при этом не нужно обращаться к какому-либо третьему лицу. Фактически, любой пользователь имеет возможность отслеживать транзакции, например, биткоина, загрузив историю его транзакций. К слову, весит она сейчас более 350 гигабайт. Для указанных целей существуют даже специализированные ресурсы в сети Интернет. Всю полученную подобным образом информацию следует занести в протокол осмотра документа и приобщить к делу в целях получения возможности для доказывания фактов преступного использования криптовалют [3, с. 147–148].

Затруднительным моментом является установление систематики совершаемых транзакций. Подробно систему построения доказательств по криптовалютным преступлениям в научных трудах рассмотрели П. В. Галушин и А. Л. Карлов [1]. Дело в том, что для криптовалюты имеет значимость электронный адрес пользователя, при этом адресов может быть множество. На данный момент специалисты устанавливают способы привязки MAC-адресов к информации в блокчейне. Однако нет ничего невозможного. Так, если сетевые транзакции между пользователями неоднократны, то установление двух-трех фактов указанных переводов поможет выявить систематику взаимосвязей и получить новые сведения о преступнике. Существенно облегчают работу в таком случае операции пользователей, например, по отправлению сдачи.

Более сложная задача, стоящая перед правоохранителями, это связывание личности преступника с информацией, полученной в ходе расследования. В теории, информацию о лицах получить вполне возможно, в случае, если удалось получить данные об электронных кошельках, транзакциях и адресах, используемых преступником. Установлению данной информации, в случае, если невозможно выявить транзакцию, способствует проведение допроса. Посредством данной процедуры возможно получить данные о кошельке, транзакциях, круге участников, систематике перевода и, самое главное, пароль от устройства, с которого осуществлялись преступные деяния. Полученные в дальнейшем сведения фиксируются в протоколах осмотра предмета и документов.

Однако в случае, если допрос не дал результатов, не всегда является возможным получение значимой информации. Примером является недавнее заявление прокуратуры Германии[1] о том, что они не смогли получить доступ к изъятым у хакера биткоинам в размере 1 700 штук. Преступник просто не предоставил полиции свой пароль от кошелька. Стоит отметить, что установление пароля не только имеет важное доказательственное значение, но и позволяет успешно совершать уголовно-процессуальные действия, направленные на конфискацию имущества, представленного криптовалютой.

Все вышесказанное не является теорией, не подтвержденной практикой. Например, дело Silk Road[2] продемонстрировало способность правоохранительных органов к использованию блокчейна для противодействия преступности. Так, по указанному криминальному кейсу, среди представленных вещественных доказательств была диаграмма, показывающая, как правоохранительные органы отслеживали средства через блокчейн, несмотря на попытку Карла Форса – обвиняемого – разделить, с целью сокрытия личности, транзакции по многочисленным адресам.

Подобным крупным примером международной организации противодействия киберпреступности в области криптовалют служит операция Operation Shrouded Horizon. Участниками данного дела со стороны правоохранительных органов выступило 20 стран, в числе которых Австралия, Канада, Кипр, США и др. В результате данной операции было подвергнуто аресту около 300 злоумышленников, осуществлявших руководство форумом Darkode в Даркнете, созданном в целях покупки/продажи вредоносного программного обеспечения.

Таким образом, успешное расследование указанной категории преступлений является возможным при условии наличия квалифицированных в области информационно-коммуникационных технологий специалистов, так как, согласно УПК РФ[3], привлекать специалистов в данном случае следует в обязательном порядке, поскольку область работы – компьютерная информация, ее носители, криптография и криптовалюта.

[1] URL: https://bitexpert.io/news/prokuratura-germanii-ne-mozhet-poluchit-dostup-k-1700-bitkoinam/ (дата обращения: 08.02.2022).

[2] URL: https://forklog.com/istoriya-silk-road-kak-bitkoin-vyvel-darknet-ekonomiku-na-novyj-uroven/ (дата обращения: 15.01.2022).

[3] URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 15.01.2022).

К сожалению, следует отметить низкий уровень подготовки специалистов указанного профиля в образовательных учреждениях. В совокупности со всеми мерами, принимаемыми Интерполом, национальными министерствами и органами внутренних дел в частности, шаг по подготовке специалистов к указанным требованиям многократно увеличил бы шанс раскрытия преступлений. Следовательно, высшим образовательным заведениям следует создавать кафедры или факультеты по подготовке специалистов данной области.

Так, выделяя дальнейшие направления развития, нельзя не согласиться с Э. Х. Надысевой в том, что в настоящее время перед органами предварительного расследования стоит достаточно сложная задача, так как отсутствуют:

– правовые нормы, регулирующие функционирование криптовалюты;

– методические рекомендации по организации раскрытия и расследования данных преступлений;

– обобщенные материалы практики не только следственной, но и судебной;

– знания и опыт работы у следователей и работников органов дознания;

– источники доказательственной информации, так как преступления данной категории специфичны, они находятся в виде сайтов и страниц сети Интернет, электронных документов и сообщений [4, с. 226].

Однако все вышеописанное свидетельствует о том, что в скором времени указанные проблемы будут устранены. Несмотря на сложность структуры раскрытия и расследования преступлений указанных категорий, еще пять лет назад система правоохранительных органов смогла быстро отреагировать на возникшую проблему. Теперь, когда темпы нарастания преступности сбиты, стоит обратить внимание на устранение расхождений правового характера, а также на освоение системы блокчейна правоохранительными органами, как России, так и других стран, в целях дальнейшего оказания взаимопомощи по расследованию преступлений в современном мире глобальной цифровизации.

Заключение

Таким образом, подводя итог, стоит отметить, что преступления в сфере криптовалюты являются относительно новым и малоизученным явлением. Несмотря на всю свою популярность среди добропорядочных граждан, статистика все-таки говорит о том, что криптовалюта выступает как средством, так и предметом совершаемых киберпреступлений. Интерес среди преступников к данному финансовому инструменту возник в связи с особенностями технологии, на которой работает криптовалюта – блокчейн. Благодаря отличительным качествам данной технологии, использование криптовалюты делает пользователя практически анонимным, что и породило любовь к активу среди преступных элементов. При этом на базе транзакций инструмента осуществляют свою незаконную деятельность ряд других организаций.

Необходимо обезопасить, сделать «мирной» технологию блокчейн, использовать весь ее потенциал, очистить ее имя от ассоциаций с мошенничеством, Даркнетом и хищениями. Мировая общественность, представители известных организаций, государств и даже президенты упоминают

криптовалюту в различных заявлениях почти каждый день, желая лишь сделать ее более безопасной для инвесторов и пользователей.

Несмотря на то что данная тематика нова для практики правоохранительных органов всего мира, можно смело заявить, что сотрудники всех систем работают оперативно и продуктивно, занимаясь пресечением, предупреждением и раскрытием преступлений указанной категории. Пусть многие вопросы по расследованию отдельных видов преступлений, связанных с данным активом, все еще остаются темным пятном в методической организации следствия, правоохранительными и законодательными органами сделан ряд значимых шагов для достижения указанной цели.

Указанная тематика требует глубокого подхода к ее изучению, формированию новых методов и инструментов расследования, выработке методических рекомендаций для органов внутренних дел, а также разработки новых строк как в законодательстве Российской Федерации, так и современном мире глобальной цифровизации в целом.

Список литературы

1. **Галушин П. В., Карлов А. Л.** Сведения об операциях с криптовалютами (на примере биткойна) как доказательство по уголовному делу // Ученые записки Казанского юридического института МВД России. 2017. Т. 2, № 4. С. 90 – 100.
2. **Коржова И. В., Хан Н. А.** Расследование совершаемых в сфере оборота цифровых финансовых активов уголовных преступлений // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2019. № 4. С. 52–53.
3. **Маркарян Э. С.** Специфика проведения следственного осмотра при расследовании преступлений, совершенных с использованием криптовалют // Актуальные проблемы российского права. 2018. № 6 (91). С. 147–148.
4. **Надысева Э. Х.** Проблемы расследования преступлений в сфере оборота криптовалют // Вестник экономической безопасности. 2019. № 3. С. 223 – 227.
5. **Соборнов П. Е.** История Органов внутренних дел. М.: Директ-Медиа, 2020. 305 с.

References

1. **Galushin P.V., Karlov A.L.** [Information about transactions with cryptocurrencies (on the example of bitcoin) as evidence in a criminal case], *Uchenyye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii* [Uchenye zapiski Kazanskogo juridical institute of the Ministry of Internal Affairs of Russia], 2017, v. 2, no. 4, pp. 90-100. (In Russ.)
2. **Korzhova I.V., Khan N.A.** [Investigation of criminal offenses committed in the sphere of circulation of digital financial assets], *Vestnik Baltiyskogo federal'nogo universiteta im. I. Kanta. Seriya: Fiziko-matematicheskiye i tekhnicheskiye nauki* [Bulletin of the Baltic Federal University. I. Kant. Series: Physical, mathematical and technical sciences], 2019, no. 4, pp. 52-53. (In Russ.)
3. **Markaryan E.S.** [Specificity of conducting an investigative examination in the investigation of crimes committed with the use of cryptocurrencies], *Aktual'nyye problemy rossiyskogo prava* [Actual problems of Russian law], 2018, no. 6 (91), pp. 147-148. (In Russ.)
4. **Nadyseva E.Kh.** [Problems of investigating crimes in the sphere of cryptocurrency turnover], *Vestnik ekonomicheskoy bezopasnosti* [Bulletin of economic security], 2019, no. 3, pp. 223-227. (In Russ.)
5. **Sobornov P.Ye.** *Istoriya Organov vnutrennikh del* [History of Internal Affairs], Moscow: Direkt-Media, 2020, 305 p. (In Russ.)

Some Features of Disclosure and Investigation of Cybercrimes in the Modern World of Global Digitalization

D. V. Tetkin, *Cand. Sci. (Law), Police Lieutenant Colonel, Associate Professor, Department of Criminal Procedure, Ryazan Branch of Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Ryazan, Russia; tyotkinden@mail.ru*

A. A. Pudovkin, *Cand. Sci. (Law), Police Colonel, Head of Department of Criminal Procedure, Ryazan branch of Moscow University Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Ryazan, Russia; mr.andre.81@mail.ru*

A. A. Troitsky, *Police Officer, Consultant, Scientific Society of Cadets and Students, Department of Criminal Procedure Ryazan Branch of Moscow University Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Ryazan, Russia; westgarx@mail.ru*

The paper presents the authors' position aimed at studying some features of the disclosure and investigation of cybercrime in the modern world of global digitalization. The article discusses the tactical features of the disclosure and investigation of crimes committed with the help of cryptocurrencies and mining. The problems that arise during the disclosure and investigation of cybercrimes, as well as ways to solve them, are identified.

The conditions and features necessary for the qualitative disclosure and investigation of cybercrimes, which are associated with the specifics of these crimes, are considered. Blockchain technology is presented, which contributes to the disclosure of cybercrime. The conditions affecting the successful investigation of this category of crimes are determined. The distinctive qualities of blockchain technology that affect the use of cryptocurrency by organizations engaged in illegal activities are considered. Conclusions are presented regarding the suppression, prevention and disclosure of crimes of this category.

Keywords: information technology; information; digitalization; detection and investigation of crimes; cybercrime; cryptocurrency; mining; digitalization.

Статья поступила в редакцию 13.02.2022

При цитировании использовать:

Теткин Д. В., Пудовкин А. А., Троицкий А. А. Некоторые особенности раскрытия и расследования киберпреступлений в современном мире глобальной цифровизации // Право: история и современность. 2022. Т. 6, № 2. С. 241 – 247. doi: 10.17277/pravo.2022.02.pp.241-247