Красношапка Григорий Витальевич
магистрант
Глухова Арина Витальевна
студентка
ФГБОУ ВО «Ярославский государственный
университет им. П.Г. Демидова»
г. Ярославль, Ярославская область

ИНФОРМАЦИЯ КАК СЛЕД ЦИФРОВОГО ПРЕСТУПЛЕНИЯ: ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И АНАЛИЗ НОРМАТИВНОГО СОДЕРЖАНИЯ

Аннотация*: в статье рассматриваются особенности правоприменительной практики в сфере выявления и пресечения цифровых преступлений. Авторы анализируют содержание специальных признаков, характеризующих особый правовой статус виртуальной информации, содержащей цифровые «следы», исследуют методы фиксации цифровых следов с помощью технологических знаний в процессе работы системы блокчейн, определяют значение информации о месте, времени, способах и других признаках криптопреступления.*

Ключевые слова*: уголовная ответственность, экономическая деятельность, цифровая валюта, криптовалюта, биткоин, цифровое преступление, система блокчейн.*

Проблема с определением криптопреступника обстоит более остро, когда криптовалютная биржа находится за пределами Российской Федерации или транзакция проходит с отечественной площадки на зарубежную. В данном случае правоохранительные органы могут не контролировать данные операции, поскольку это не является обязательным. В ином случае встает вопрос об использовании законодательства – какая страна должна регулировать цифровые отношения, повлекшие совершение преступления. В таких случаях существенное значение имеет анализ информации о виртуальных «следах» такого посягательства. В цифровых преступлениях, в которых криптовалюта выступает не

предметом противоправного деяния, а средством, к уголовной ответственности зачастую привлекаются покупатели, а не продавцы. В частности, это касается сделок по обороту наркотических средств или оружия, которые покупатель приобретает за счет виртуальной валюты. Но для выявления цифровых преступлений любого характера (криптовалюта и предмет, и средство посягательства) необходимо установление цифрового «следа» [1, с. 462].

Виртуальный след по своей правовой природе не будет многим отличаться от традиционного понимания следа совершения преступления. Для его появления также необходимо преступное взаимодействие, только действие будет происходить не в материальном, а в виртуальном мире. Очевидно, что не только действия физических субъектов будут служить для образования следа, но и сами явления совершенного противоправного деяния. Так, цифровой след может появиться в результате какого-либо действия самой электронной системы. В данном случае мы не можем говорить о полном отсутствии воздействия человека, но оно может быть весьма несущественным. В качестве примера возьмем ситуацию, в которой преступник совершает определенное действие с криптовалютой и запускает команду в компьютерной программе, способствующую достижению результата. Само действие может не оставить никакого цифрового следа, но действие виртуальной системы произведет создание нового кода или закрытия цифровой цепочки, что в дальнейшем и позволит обнаружить этот след.

«След» цифрового преступления является базовым доказательством проводимого расследования – он содержит информацию о месте, времени, способах, личности преступника и других субъективных признаках. Рассмотрим группу методов выявления цифровых следов, применяя технологические знания работы системы блокчейн [1, с. 462]. Заметим, что высокая латентность преступлений в сфере оборота цифровых валют образуется в первую очередь по причине отсутствия временного и территориального следа. Прокси сервера, веб – браузер TOR и прочие программы для шифрования не позволяют правоохранительным органам обнаружить цифровой след преступника. Браузер TOR представляет собой сервер, обеспечивающий абсолютную анонимность его пользователям. По

данным исследования от 2020 года IT-оператором данного браузера было обнаружено около 400 сетевых узлов, посредством которых преступники могли незаметно украсть криптовалюту. Определить время и место при описанных обстоятельствах практически не представляется возможным [2, с. 87; 6, с. 152].

Тем не менее, на наш взгляд, не существует абсолютной анонимности при обороте криптовалюты. Сама информация о транзакции сохраняется в сети и находится в открытом доступе. Биткоин-адрес представляет собой некий номер счета, который может указать на местоположение пользователя (устройства, с помощью которого совершалось преступление). При этом на практике оказывается не все так просто. Теоретически биткоин – адрес возможно связать с IP-адресом криптопреступника, если он не воспользовался специальным сервером (например, TOR) или не создавал несколько IP-адресов. В таком случае поиск места совершения преступления становится практически невозможным [3]. Решение данного вопроса предлагают отдельные практические работники. Назначение перевода устанавливается с помощью допроса или очной ставки с участием отправителя и получателя перевода. Также, возможно привлечение специалиста, который будет исследовать онлайн-кошелек [4, с. 50]. Поскольку все транзакции проходят через криптобиржи, сотрудники правоохранительных органов должны напрямую обращаться к их организаторам.: необходимо ввести обязательное страхование денежных средств участников криптовалютных отношений и обязательную компенсацию в случае их утраты. В таком контексте у самих организаторов криптобирж появится дополнительный стимул в идентификации своих пользователей.

Особенно важным в компьютерной экспертизе будет поиск специального программного обеспечения для хранения виртуальной валюты в электронном кошельке. Самым известным из них на сегодняшний день является Bitcoin Core. Данное обеспечение создает специальный файл на жестком диске компьютера, в котором будет храниться ключ от криптовалютного кошелька. Поэтому при проведении компьютерной экспертизы следует обращать внимание на историю

браузера, загрузок, которые могут содержать информацию о наличии у подозреваемого вышеуказанного кошелька [5, с. 278; 6, с. 151].

Таким образом, при расследовании криптопреступлений органам предварительного расследования необходимо:

а) обладать знаниями в области IT-технологий, знания компьютерных технологий, компьютерной информации, информации, содержащихся на любых электронных носителях, а также электронных систем и иных средств платежей в виртуальной системе, при недостаточности знаний в указанных областях необходимо привлекать специалистов, квалифицирующихся на вышеупомянутых предметах;

б) ввиду специфических особенностей, связанной с основами цифровой экономике, системой работы виртуальной валюты, необходимо углублять знания в механизмах работы децентрализованной системы блокчейн и криптографии в целом;

в) все знания, необходимые для развития криминалистической теории, связанной с цифровыми преступлениями, необходимо доносить до будущих сотрудников правоохранительных органов на уровне вузовского образования, создавая если не специальные кафедры и факультеты, то профильные предметы, дающие фундаментальные знания в области криптовалютных отношений.

Список литературы

1. Ермилов Д. Кластерный анализ биткоин адреса / Д. Ермилов, М. Панов, Ю. Янович // Конференция машинного обучения. – М., 2017. – С. 461–467.

2. Иванцов С.В. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С.В. Иванцов, Э.Л. Сидоренко, Б.А. Спасенников [и др.] // Российский журнал криминологии. – 2019. – Т. 13. №1. – С. 85–93.

3. Надысева Э.Х. Проблемы расследования преступлений в сфере оборота криптовалют / Э.Х. Надысева // Вестник экономической безопасности. – 2019. – №3 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/problemy-rassledovaniya-prestupleniy-v-sfere-

oborota-kriptovalyut (дата обращения: 26.07.2024). – DOI 10.24411/2414-3995-2019-10167. – EDN GCAMWW

4. Волынский А.Ф. Алгоритмы применения специальных знаний для выявления и расследования преступлений в сфере «традиционной» и цифровой экономики / А.Ф. Волынский, В.А. Прорвич // Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: материалы научно-практической конференции с международным участием (5 апреля 2019 г.). – М., 2019. – С. 45–52. – EDN NXORVQ

5. Бударина Д.В. Незаконный оборот цифровых активов в системе уголовно-правовой охраны на современном этапе / Д.В. Бударина, Р.Ю. Смирнов // Право, экономика и управление: актуальные вопросы. – Чебоксары, 2020. С. 277–280.

6. Соловьев О.Г. Цифровые активы как предмет преступления: дискуссионные аспекты законодательной и правоприменительной практики / О.Г. Соловьев, С.Д. Бражник // Наука и знание: актуальные проблемы устойчивого экономического регионов России: правовые, аспекты развития и обеспечения безопасности социально-экономические и гуманитарные: материалы XXIV международной научно-практической конференции / под общ. ред. Л.А. Демидовой, Т.А. Куткович. – Новороссийск, 2022. – С. 150–153. – EDN TSYRHQ