Переломова Ирина Геннадиевна
канд. экон. наук, доцент
ФГБОУ ВО «Ярославский государственный
университет им. П.Г. Демидова»
г. Ярославль, Ярославская область
Золотин Евгений Максимович
студент
ФГБОУ ВО «Ярославский государственный
университет им. П.Г. Демидова»
г. Ярославль, Ярославская область
Крат Софья Александровна
консультант-стажер
АНО «Ярославское правовое
научно-исследовательское общество»
г. Ярославль, Ярославская область

ТЕХНОЛОГИЧЕСКОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЦИФРОВОЙ ЭКОНОМИКИ НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация*: в статье рассматриваются вопросы организации нормативного и технологического противодействия противоправным проявлениям в области функционирования цифровой экономики в Российской Федерации, авторы исследуют различные методы обеспечения безопасности в сфере оборота различных криптовалют.*

Ключевые слова*: цифровые технологии, цифровая экономика, виртуальная валюта, криптовалюта, незаконный оборот, криптопреступность.*

Современная практика обеспечения безопасности в области цифровой экономики имеет определенные проблемы, без решения которых, к примеру, рынок криминальных услуг с использованием криптовалюты будет постоянно расширяться. Для того, чтобы устранить такие проблемы следует рассмотреть опыт не

только отечественного законодателя в сфере виртуальной валюты, но и обратиться к зарубежным рекомендациям по предупреждению противодействию криптопреступности. Криптовалюта не является единственной виртуальной валютой, но тем не менее она получила большую популярность среди остальных. Технология блокчейн, на основе которой создавалась криптовалюта, является децентрализованной, что позволяет обеспечивать анонимность пользователя криптовалютного рынка. Если свести все задачи расследования цифровых преступлений, то они образуют одну главенствующую – устранение анонимности лица, совершившего криптопреступление. Для решения отмеченных вопросов отечественные ученые предлагают несколько способов, которые базируются как на основании правового подхода, так и технологического [1, с. 88].

«След» цифрового преступления составляет доказательственную базу расследования – он содержит информацию о месте, времени, способах, личности преступника и других субъективных признаках. Рассмотрим пул методов выявления цифровых следов, применяя технологические знания работы системы блокчейн. Вопреки устоявшемуся мнению анонимность, обеспеченная технологией блокчейн, распространяется исключительно на сам адрес криптовалютного кошелька. При этом одна транзакция цифровой валюты оставляет след в виде электронной записи в виртуальной сети. Например, преступником с помощью хакерских операций были похищены денежные средства в виде биткоинов. Далее им же была совершена транзакция на криптовалютном рынке – перевод биткоина в качестве оплаты приобретаемых товаров на адреса интернет – магазинов нескольких продавцов. Информация о транзакциях находится в открытом доступе, поэтому располагая информацией о данной сети можно вычислить, к какому депозитному счету ведут транзакции и определить лицо, совершившее переводы. При этом данный анализ не проводится вручную следственными органами. Алгоритм кластеризации объединяет информацию о конечных кошельках, на которые осуществлялись транзакции, и связывает их с одним пользователем, то есть объединяет в кластер. На сегодняшний день уже существуют инструменты исследования, основанные на алгоритмах кластеризации, например,

система «Crystal Blockchain» показывает хорошие результаты в выявлении подозрительных транзакций, тем самым снимая раскрывая информацию о предполагаемых криптопреступниках.

Пример успешной аналитической работы в поисках цифрового следа зафиксирован в международной правоприменительной практике. Одной из самых известных торговых площадок по сбыту нелегальных товаров, в первую очередь наркотических и психотропных средств, долгое время являлась Silk Road [2, с. 72]. Согласно статистическим данным от деятельности на рынке нелегальных товаров, владелец получал годовой доход равный 17 миллионов долларов вплоть до момента задержания в 2015 году. Владелец компании Р.У. Ульбрихт при идентификации указал адрес личной почты, который в последствии следственный орган связал со всеми нелегальными транзакциями [3, с. 179]. При этом важно помнить, что сама система блокчейн не представляет особой трудности в следственной операции. Настоящей проблемой в поиске цифрового следа является наличие нескольких IP-адресов у криптопреступника, использование им прокси-серверов, в частности браузера TOR или биткоин – миксера. Федеральным законом №149-ФЗ «Об информационных технологиях и о защите информации» уже введен запрет на использование специальных средств, позволяющих получить доступ к ресурсам, запрещенным в Российской Федерации или требующим деанонимизацию ввиду обязательной идентификации личности, как в случае с деятельностью, связанной с цифровой валютой и цифровыми финансовыми активами. Однако, как мы видим, данных мер недостаточно для предупреждения распространения криптовалютной нелегальной деятельности [2, с. 73].

Решение данного вопроса может выглядеть следующим образом. Назначение перевода устанавливается с помощью допроса или очной ставки с участием отправителя и получателя перевода. Также, возможно привлечение специалиста, который будет исследовать онлайн-кошелек. Поскольку все транзакции проходят через криптобиржи, сотрудники правоохранительных органов должны напрямую обращаться к их организаторам. Первыми в области верификации участников криптовалютных рынков и взаимодействии с полицией при

расследовании цифровых преступлений стал Евросоюз. Криптобиржа обязана проводить идентификацию своих пользователей согласно Федеральному закону №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Однако, по нашему мнению, даже при успешном взаимодействии с организаторами цифровых площадок, данных мер бывает порой недостаточно для снижения процента криптопреступности. В связи с чем мы предлагаем превентивные меры по противодействию цифровой преступности. Необходимо ввести обязательное страхование денежных средств участников криптовалютных отношений и обязательную компенсацию в случае их утраты [3, с. 179]. В таком контексте у самих организаторов криптобирж появится дополнительный стимул в идентификации своих пользователей. Некоторые обстоятельства, подлежащие доказыванию, могут быть установлены в ходе компьютерной экспертизы. Предметом данной экспертизы является исследование содержащейся на компьютере информации. К сожалению, на практике подобная экспертиза используется крайне редко для установления факта использования криптовалют. При этом современные возможности позволяют определить цифровые следы.

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. При обнаружении на электронном носителе криптовалютного кошелька, который может находиться как на компьютере, так и на телефоне с высокотехнологичной операционной системой, важно понимать, что подозреваемый также заинтересован в том, чтобы махинации следственных органов над ним не привели к утере криптоключа, поскольку без него произойдет окончательная утрата

виртуальной валюты. Электронные носители в ходе осмотра должны быть изъяты и отправлены на компьютерную экспертизу [4, с. 173].

Приведенные примеры расследования цифровых преступлений помогают точечно бороться с последствиями пробела правового регулирования цифрового финансового актива и цифровой валюты. Мы должны понимать, что правоприменительные проблемы необходимо решать на уровне выше, то есть первостепенной задачей мы должны поставить выработку авторской концепции уголовно-правовой политики в контексте предупреждения криптопреступлений. Разработанный механизм регулирования оборота цифровых финансовых активов и цифровых валют будет реализован посредством: 1) совершенствования существующих нормативно-правовых актов, регулирующих цифровые отношения; 2) создания новых норм, способствующих предупреждению криптопреступлений. В Федеральном законе №259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» говорится о правилах работы криптообменников и условиях, на которых организация может заниматься подобной деятельностью. При этом закон не содержит четкого указания, на какие именно криптобиржи распространяются данные условия: на российские или международные? Другими словами, не совсем понятно, как регулировать транзакции, связанные с иностранными криптобиржами. Исходя из смысла доктринальных взглядов, становится понятно, что российский законодатель предъявляет одинаковые требования к лицензированию криптовалютных бирж, как для российский организаций, так и для иностранных организаций, проводящих свою деятельность на территории РФ. При этом выдача лицензии будет напрямую контролироваться Банком России. Остается открытым вопрос касающийся иностранных организаций, напрямую не входящим на российский рынок криптовалюты, но который каким-либо образом стал фигурировать в цифровом преступлении. Напрашивается внести пояснение в существующий Закон о цифровых активах, что с целью правомерного функционирования рынка криптовалюты необходимо получение лицензии участниками оборота цифровых валют, дающую право на реализацию деятельности в цифровой экономике и позволяющую взаимодействовать только с такими

провайдерами, которые имеют аналогичную лицензию. Другими словами, необходимо уточнить, что любая иностранная или отечественная организация должна лицензироваться для того, чтобы осуществлять операции на криптовалютном рынке.

Список литературы

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

2. Полонных А.В. Проблемные аспекты выявления и расследования преступлений, связанных с оборотом криптовалюты / А.В. Полонных // Развитие таможенных органов и современное образовательное пространство в условиях цифровизации: научная конференция. – Улан-Удэ, 2020. – С. 71–73. – EDN XIYPPS

3. 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. – С. 277–280.

4. Рубцова А.С. Криптовалюты: предмет и средство совершения преступления / А.С. Рубцова // Вестник Университета им. О.Е. Кутафина. – 2018. – №12. – С. 172–182. – DOI 10.17803/2311-5998.2018.52.12.172-181. – EDN YXPJUT