социальной, уголовно-политической, криминологической, уголовно-правовой обусловленности норм, дифференцирующих уголовную ответственность.

Библиографический список

1. Курс уголовного права: в 5 т. Общая часть. Том 1: Учение о преступлении / С. В. Ананич [и др.]; под ред. И.О. Грунтова, А.В. Шидловского. – Минск: Изд. центр БГУ, 2018. – 863 с.

2. Шидловский, А.В. О методологии систематизации уголовного законодательства и её влиянии на ранжирование наказаний // Право в современном белорусском обществе : сб. науч. тр., посвящ. д-ру юрид. наук, проф., засл. юристу Респ. Беларусь С. Г. Дробязко. Выпуск 13 / Нац. центр законодательства и правовых исследований Респ. Беларусь; Ин-т правовых исследований; редкол.: Н. А. Карпович (гл. ред.) [и др.]. – Минск: Колорград, 2018. – С. 767-768.

3. Уголовный кодекс Республики Беларусь [Официальное издание]: принят Палатой представителей 2 июня 1999 г., одобрен Советом Республики Национального собрания Респ. Беларусь 24 июня 1999 г., подписан Президентом Респ. Беларусь 9 июля 1999 г., № 275-З / Национальный центр правовой информации Респ. Беларусь. – Минск, 1999. – 214 с.

4. Уголовный кодекс Республики Беларусь: принят Палатой представителей 2 июня 1999 г.: одобр. Советом Респ. 24 июня 1999 г.: подписан Президентом Республики Беларусь 9 июля 1999 г., № 275-З: в ред. Закона Республики Беларусь от 11.11.2019 г., № 253-З // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. –Минск, 2020.

5. Наумов, А.В. Преступление и наказание в истории России. – В 2 ч. –Ч. II. –М.: Юрлитинформ, 2015. – 656 с.

«SCAM-ПРОЕКТЫ» КАК СРЕДСТВО ХИЩЕНИЯ КРИПТОВАЛЮТ: КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ

Д.И. Шнейдерова
преподаватель кафедры правовых дисциплин
УО «Могилевский институт Министерства внутренних дел Республики Беларусь»

Увеличение количества пользователей ресурсами сети «Интернет» в условиях складывающейся в различных странах социально-политической обстановки способствовало широкому внедрению и развитию мошеннических проектов, направленных на хищениек риптовалют (Scam-проекты). Согласно статистическим данным IT-компании «Kaspersky»за первое полугодие 2020 года в русскоязычном сегменте Интернета было зафиксировано более 23 тысяч подобных ресурсов, что в 3 раза больше, чем за аналогичный период 2019 года [1]. Усложненный механизм таких преступлений, их латентность, отсутствие

свободного доступа к источникам цифровых доказательств, немногочисленный практический опыт расследования подобных уголовных дел представляют актуальную проблему для правоохранительных органов в вопросах методики выявления, раскрытия, пресечения и профилактики хищений в сфере оборота криптовалют. С целью ее разработки представляется необходимым изучение сущности, видовых категорий и механизмов реализации Scam-проектов как одного из часто применяемых средств хищения криптовалют.

Следует отметить, что в целом Scam как разновидность мошенничества в сети «Интернет» можно подразделить на две группы: «Scam-ресурсы» и «Scam-проекты». Ресурсы направлены, в большей степени, на получение от доверчивых пользователей денежных средств для участия в различных рекламных розыгрышах, приобретении криптовалют по стоимости меньше рыночной, получение призов за небольшой взнос в криптовалюте и т.д. В криптоиндустрии наиболее развита сфера Scam-проектов, под которыми следует понимать инвестиционные проекты, направленные на привлечение вкладчиков с целью формирования и циркулярного увеличения цифровых капиталовложений без намерения реализации обещанных условий.Scam-проекты классифицируются по различным основаниям: по форме реализации, по направленности умысла, по сроку действия и по механизму прироста криптовалют. По форме реализации проекты могут быть представлены в виде криптовалютных кошельков, криптобирж или криптоплатформ, включающих и кошельки и биржи одновременно.

Scam-кошелькипредставляют собой онлайн-сервисы, позволяющие хранить различные виды криптовалют (т.е. можно выделить как одновалютные, так и мультивалютные), осуществлять сделки по купле-продаже одних валют на другие, а также преумножать их количество (к примеру, Dash-Coin.net, Freewallet, StakedWallet, Chartoken и другие).По своему характеру кошельки могут быть активными и пассивными. Активные Scam-кошельки своей целью ставят либо хранение уже существующих криптомонет, либо предназначены для осуществления обменных операций с криптовалютой нового формата, поступающих на счет или приобретаемых на специализированной одноименной криптоплатформе, также являющейся Scam-проектом. В случае работы криптокошелька с уже обращаемыми на рынке видами криптовалют механизм преступного замысла может быть представлен следующим образом: пользователю при посещении различных Интернет-ресурсов (онлайн-игры, розыгрыши, виртуальное казино, ставки и т.д.) предлагается пополнить счет своего аккаунта для возможности участия в некотором виртуальном проекте путем создания криптокошелька в скаме и перечислении на него необходимых криптосрдеств.После того, как пользователь выполнил действия по прописанной мошенниками инструкции криптовалюты действительно попадают на счет нового кошелька, отображаются для пользователя как активный баланс, однако вывести их с кошелька путем обмена на фиатные средства или перевести на другой кошелек уже не представляется возможным,

так как система блокирует подобные действия, поясняя владельцу, что ему необходимо пройти процедуру идентификации по принципу KYC (знай своего клиента). Такая процедура требует от владельца кошелька предоставления анкетных данных, фотографий с изображением личности, а также может запросить дополнительную аутентификацию по номеру мобильного телефона. При отправке необходимой информации сервис уведомляет пользователя, что его данные находятся в обработке и до ее завершения операции с криптосредствами на счете недоступны. Однако к завершению такая проверка так и не приходит, лишая возможности пользователя вернуть свои средства или воспользоваться ими иным образом. В таких случаях система продолжает находиться в состоянии проверки данных и отображает на балансе кошелька наличие криптовалют, однако при самостоятельной проверке пользователем по номеру транзакции на криптоплатформе информации о местонахождении средств последний обнаруживает, что криптомонеты были неоднократно перенаправлены на другие криптокошельки или выведены через криптообменники. В случае использования Scam-кошелька для хранения новых видов криптовалют механизм реализации преступного умысла заключается в убеждении пользователя приобретать криптовалюты нового Scam-проекта, обещая при этом увеличение со временем их капитализации и, соответственно, прибыть от вложения реальных средств в виртуальные. Однако по истечении определенного периода времени такие платформы,получив достаточное количество денежных средств, уничтожают свой сервис и удаляют данные о нем в различных социальных сетях.

Пассивные Scam-кошельки работают по принципу прироста количества криптовалют без совершения каких-либо дополнительных действий за счет привлечения денежных средств новых клиентов. Так пользователям предлагается перечислить на новый Scam-кошелек свои криптосредства или приобрести их на определенной платформе с автоматическим зачислением для последующего хранения, в обмен на ежедневные начисления в размере 1,5 – 2 % к существующей сумме, которые производятся создателями сервиса за счет поступления денежных средств от новых пользователей. При этом привлечение новых клиентов может осуществляться путем рекламы самим сервисом, так и при помощи присоединившихся пользователей, вовлекающих своих знакомых в выгодный финансовый проект. Однако, как и в любом ином случае, попрошествии некоторого промежутка времени создатели выводят средства на свои криптокошельки и уничтожают сервис вместе с всевозможными следами его пребывания в сети «Интернет».

Scam-биржи, как работающие с собственными криптокошельками, так и со сторонними сервисами, реализуют свою преступную деятельность по схеме связанной с невозможностью вывода зачисленных для обменных операций криптосредств, которые в последующем переводятся создателями ресурса на иные кошельки, скрываются посредством использования криптомиксеров, либо реализуются через действующие обменники. Примерами таких бирж являются

Mt.Gox, Cryptsy, BTC-e, WEX, Coincheck, DAO, BitFinex и другие. Сама биржа перестает существовать либо пользователям сообщается о ее взломе хакерами и хищении ими всех активов, которые вернуть не представляется возможным.

По направленности умысла создателей Scam-проекты подразделяются на «хайпы» (HYIP) и «real-проекты». «Хайпы» представляют собой криптоинвестиционные проекты, которые создавались с целью осуществления мошеннической деятельности. Такие проекты отличаются краткосрочным характером деятельности, распространяются и привлекают клиентов за счет многочисленной рекламы на форумах, в социальных сетях и Интернет-магазинах, в качестве ключевых, обращающих на себя внимание, факторов являются обещания о быстром заработке и развитии проекта, а также об увеличении процента начислений и прироста средств в случае вложения большего количества денег или криптовалюты в проект.Сам ресурс выглядит довольно примитивно, не содержит или содержит в малом количестве информацию об основателях проекта, схемах его работы, источниках стартовых капиталовложений, либо использует данные, не соответствующие действительности, в том числе графического характера (например, фотографии сторонних лиц, полученные из социальных сетей). В отличие от «хайпов» реальные проекты первоначально создавались с целью осуществления инвестиционной деятельности на криптовалютном рынке, однако в результате неблагоприятных факторов не смогли реализоваться и преобразовались в Scam-проекты, осуществляющие преступную деятельность. В качестве факторов, способствующих преобразованию характера деятельности инвестиционных ICOпроектов в Scam, можно выделить следующие: снижение притока внешних инвестиций в проект, конфликтные ситуации между учредителями относительно распределения активов, характера и механизма деятельности проекта, вывод активов привлеченными инвесторами, невостребованность проекта на инвестиционном рынке криптовалют, недостаточность средств для старта проекта.

При этом следует отметить, что, несмотря на разницу целей создания «хайпов» и «реальных» проектов, в качестве причин прекращения деятельности и потери средств инвесторов как первые, так и вторые прибегают к одним и тем же схемам ликвидации стартапа. Так можно выделить два способа прекращения проекта: полное уничтожение ресурса либо его «заморозка» по причинам внешнего воздействия, повлиявшего на потерю ресурсов инвесторов, т.е. банкротство. В первом случае, после вывода активов создатели проектов удаляют веб-страницы из сети «Интернет» и любую иную информацию о проекте со сторонних ресурсов, тем самым уничтожая цифровые следы своей деятельности. Во втором случае создатели объясняют потерю средств взломамисервиса путем хакерских атак, ошибками или противоправными действиями сотрудников проекта, техническими проблемами, переходом на новые методы работы, обманом со стороны партнеров и т.д., т.е. действиями со стороны, свидетельствующими об отсутствии вины самих создателей в

банкротстве проекта, который в последующем может быть восстановлен и возобновлен по той же схеме.

По сроку действия Scam-проекты подразделяются на краткосрочные (от нескольких дней до 1-2 недель), среднесрочные (от 1 до 3 месяцев) и долгосрочные (свыше 3 месяцев). При этом срок деятельности проекта находится в прямой зависимости от активности притока новых инвесторов. Как только проект перестает привлекать новых пользователей, а также теряет уже существующих, тогда преступниками принимается решение о его ликвидации и выводе накопленных средств. Для среднесрочных и долгосрочных проектов характерно создание видимости деятельности, когда инвесторам начисляются проценты или преумножается размер их криптовалютных средств на счетах.

Среди механизмов прироста криптовалют в рамках Scam-проектов можно выделить прамайнинг (увеличение инвестиций зависит от количества привлеченных пользователем новых инвесторов в проект), использование скрытого алгоритма торговли (проприетарные проекты), поиск и осуществление выгодных криптовалютных операций роботом (базируется на росте и падении курсов криптовалют), а также генерацию дохода по схеме «Понци» (создание финансовой пирамиды, где первые инвесторы получают доход за счет вложений последующих).

Таким образом, анализ сущности, видов и механизмов реализации корыстного преступного умысла создателей криптовалютных Scam-проектов является основой для разработки криминалистами и сотрудниками правоохранительных органов эффективной методики расследования и раскрытия хищений в сфере оборота криптовалют.

Библиографический список

1. Сапрыкина, А. Скам шагает по стране[Электронный ресурс] / А. Сапрыкина // Новостной портал «ComNews». – Режим доступа: https://www.comnews.ru/content/208121/2020-07-16/2020-w29/skam-shagaet-strane. – Дата доступа: 12.11.2020.

РАЗВИТИЕ УГОЛОВНОГО СУДОПРОИЗВОДСТВА НА ТЕРРИТОРИИ БССР С ПРИНЯТИЕМ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО КОДЕКСА РСФСР 1922 ГОДА

Н.В. Шпаковский
инспектор Управления Следственного комитета Республики Беларусь по г. Минску

В 1922 году в Советской России была проведена судебная реформа, созданы прокуратура и адвокатура, проведена кодификация уголовно-процессуального законодательства. Постановлением III сессии ВЦИК 25 мая 1922 года был утвержден первый на территории РСФСР Уголовно-Процессуальный Кодекс.