Дедковский А. А.

КРИПТОПРЕСТУПЛЕНИЕ: ПОНЯТИЕ, ВИДЫ, ХАРАКТЕРИСТИКА ОТДЕЛЬНЫХ КОМПОНЕНТОВ

УО ФПБ «Международный университет «МИТСО»,
ул. Казинца, д. 21, к. 3, 220099, г. Минск, Беларусь,
a.dziadkouski@gmail.com

Представлено авторское определение категории «криптопреступление», выявлены и описаны типичные сведения, образующие криминалистическую характеристику криптопреступлений: личность криптопреступника, способ совершения преступления, способ легализации преступных доходов (через криптосервисы), предмет преступного посягательства, следования картина, обстановка совершения преступления. Определены основные направления развития криптопреступности.

Ключевые слова: криминалистическая характеристика; криптопреступление; виртуальные следы; электронно-цифровая информация; криптовалюта; токен; блокчейн.

Анализ правоприменительной практики Республики Беларусь свидетельствует о том, что состояние преступности характеризуется не просто ростом киберпреступлений, а фактическим стиранием границ, разделявших их с иными традиционными для нашего общества преступлениями. Появление в Республике Беларусь новых способов совершения криминальных деяний, связанных с использованием криптовалют, в настоящее время характерно не только для преступлений против собственности (хищение имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса Республики Беларусь (далее – УК), вымогательство (ст. 208 УК), мошенничество (ст. 209 УК) и компьютерной безопасности (несанкционированный доступ к компьютерной информации (ст. 349 УК), уничтожение, блокирование или модификация компьютерной информации (ст. 350 УК), неправомерное завладение компьютерной информацией (ст. 352 УК), разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (ст. 354 УК), но и таких предикатных к легализации (отмыванию) средств, полученных преступным путем преступлений, как незаконный оборот наркотических средств (ст. 328 УК), изготовление и распространение порнографических материалов (в том числе с изображением несовершеннолетнего) (ст.ст 343 УК, 343-1 УК), организация незаконной миграции (ст. 371-1 УК), и др. С учетом высокой латентности таких

преступлений и отсутствия целенаправленного учета, в 2023 году возбуждено более 1000 уголовных дел, по которым фигурирует криптовалюта если ни как предмет преступного посягательства, то как средство достижения преступного результата [1].

Отсутствие единого универсального подхода к определению криптовалюты, а равно бессистемное участие банковской системы в криптовалютных транзакциях стимулирует преступников на создание и развитие сервисов по конвертации криптовалюты в фиатную валюту. В итоге именно эти сервисы и становятся основными звеньями в системе легализации преступных доходов. Так, по оценкам специалистов, более 20% всех поступающих на конвертацию криптовалют приходили непосредственно из незаконных источников. С помощью криптовалют сегодня легализуются практически все виды нелегального дохода. Преступники используют анонимность блокчейна, чтобы скрыть источники незаконных средств и конвертировать их в наличные, которые затем могут быть заведены в легальный оборот через банковскую систему. Согласно «Отчету о криптопреступности за 2024 год» от Chainalysis, за 2023 год суммарно через криптовалюту было легализовано более 22 млрд долларов [2].

В научном сообществе на такой феномен, как криптовалюта имеются разные, иногда противоположные взгляды. Одни ученые полагают, что биткоины могут быть использованы исключительно для перевода на другой биткоин-адрес [5, с. 45], другие олицетворяют криптовалюту с электронными деньгами [3, с. 201], что не совсем верно, как в техническом, так и финансово-экономическом аспектах, а по мнению третьих, развитие криптовалют может значительно снизить контроль и эффективность существующих механизмов регулирования на национальном уровне и создать реальную угрозу экономической безопасности любого государства [4, с. 86].

Качественным отличием традиционных преступных посягательств от деяний, механизм которых предусматривает использование IT-технологий является возможность совершения последних удаленно, без физических контактов соучастников. Вследствие чего следовая картина таких преступлений обретает определенную специфичность и традиционных криминалистических средств и методов для собирания полноценной доказательственной базы уже недостаточно. Не являются в этом исключением и преступления, по которым в качестве предмета, средства совершения или сокрытия выступают криптоактивы, (далее – «криптопреступление»), в т. ч. криптовалюта, крипто-облигации.

Под криптопреступлением в контексте настоящего исследования предлагается понимать совокупность общественно опасных деяний, в ходе совершения которых в качестве предмета преступного посягательства, средства совершения или сокрытия преступления выступают криптоактивы

(криптовалюта, крипто-облигации иные формы цифровых финансовых активов).

На основании изложенного классифицировать криптопреступления можно на две основные группы:

Общественно опасные деяния, в ходе совершения которых в качестве предмета преступного посягательства выступают криптоактивы. К таким преступлениям можно отнести хищения, наиболее распространёнными формами которых применительно к криптопреступлениям являются хищение имущества путем модификации компьютерной информации (ст. 212 УК), вымогательство (ст. 208 УК), мошенничество (ст. 209 УК); взяточничество (ст.ст. 430-432 УК); незаконное вознаграждение (ст. 433 УК), когда криптоактивы передаются в качестве предмета взятки.

Общественно опасные деяния, в ходе совершения которых средства совершения или сокрытия преступления выступают криптоактивы: легализация («отмывание») средств, полученных преступным путем (ст. 235 УК); изготовление, хранение либо сбыт поддельных денег или ценных бумаг (ст. 221 УК), незаконный оборот наркотических средств (ст. 224 УК), взяточничество (ст.ст. 430-432 УК), изготовление и распространение порнографических материалов или предметов порнографического характера (ст. 343 УК) и др., при совершении которых криптоактивы как средство оплаты используются для сокрытия преступления; мошенничество (ст. 209 УК), когда привлекаются фиатные деньги потерпевших для приобретения криптоактивов.

Качество и полнота расследования данной категории уголовных дел во многом зависят от понимания следователем наряду с классическими элементами криминалистической характеристики преступлений (личность преступника, способ совершения преступления, предмет преступного посягательства, механизм следообразования, обстановку совершения преступления) основополагающих принципов блокчейн-технологий, криповалютной экосистемы, технической и правовой природы криптовалют, точек соприкосновения криптоиндустрии с привычным нам фиатным финансовым миром.

Анализ правоприменительной практики позволяет смоделировать типичный портрет криптопреступника:

– лицо мужского пола в возрасте от 20 до 40 лет;

– к уголовной ответственности ранее не привлекался;

– обладает высоким интеллектом, способен принимать быстрые решения;

– материально обеспечен (с достатком на уровне среднего или выше среднего);

– не состоит в браке, не имеет детей;

– имеет достаточный опыт работы в сфере информационных технологий;

– работник, добросовестно исполняющий свои обязанности, имеющий устойчивый статус в глазах окружающих людей, любящий работать в уединенной атмосфере, для решения рабочих вопросов до конца часто задерживающийся и редко использующий отпуск.

Немаловажной особенностью такой личности выступает информационно – технические навыки преступной деятельности в удаленном от места происшествия месте, корыстный мотив при решении задач, склонность к творческим открытиям при разработке преступных схем, а также в некоторых случаях, способность вызывать доверие у людей.

При совершении «криптопреступления» применяются следующие наиболее типичные способы:

– использование фейковых (поддельных) электронных кошельков. Потерпевшие, покупая товар или услуги на популярных сервисах, перечисляют деньги на фишинговые кошельки, имеющие другие адреса, посредством использования преступниками вирусных программ;

– создание фишинговых сайтов (или сайтов-копий) популярных ресурсов. Так, популярным способом хищения криптовалюты на данный момента является технология фишинга (phishing), не предусматривающая контакта злоумышленника и жертвы, в основе которой находится рассылка писем на электронную почту владельцев криптовалюты о том, что они якобы стали победителями какой-либо акции. Если владелец переходит на свой кошелек по ссылке, отраженной в этом письме, его данные отсылаются злоумышленникам. Далее единицы криптовалюты потерпевшего без его ведома перемещаются на электронные кошельки, подконтрольные виновным, причем нередко производится коррекция страниц с историей доступного баланса с целью скрыть хищение [6, с. 173];

– краудинвестинговые проекты. Развитие новой модели коллективного инвестирования (ICO, IPO и др.) привело к появлению мошеннических компаний, собирающих с потерпевших средства в криптовалюте, заведомо не имея цели заниматься предпринимательской деятельностью;

– создание инвестиционных фондов, работающих с использованием криптовалюты.

Обращает на себя внимание широкий спектр способов легализации преступных доходов через криптосервисы. Как правило, отмывание денег осуществляется:

1) посредством использования одноранговых транзакций «человек - человек»;

2) применения биткойн-автоматов (крипто-матов, криптотерминалов); отсутствие системы идентификации клиента делает эти устройства

чрезвычайно популярными среди преступников даже несмотря на высокую комиссию транзакций (10-15%);

3) использования смесителей (микшеров), позволяющих запутывать цепочки транзакций;

4) через нелегальные обменные сервисы (В последнее время их популярность стремительно растет. По данным международных экспертов, больше всего «грязных» денег было отмыто через конвертацию валют в странах Европы. В страновом срезе можно заметить интересную закономерность: больше всего «грязных» денег проходит через офшорные юрисдикции, на втором месте - Европа, на третьем - Азия. Список замыкает Африка: на этом континенте сервисы по конвертации практически не развиты. Показательно и то, что до введения в Китае запрета на оборот криптовалюты именно Азия занимала лидирующее положение в рейтинге по отмыванию преступных доходов с использованием криптовалюты. Положительное изменение динамики этих преступлений в Китае является свидетельством того, что криминальный рынок криптовалют чувствителен к нормативному регулированию);

5) популярность приобретает легализация преступных доходов через азартные онлайн игры; по мнению экспертов, именно через смесители и онлайн игры в год отмывается более 78% грязных виртуальных денег [7].

Предмет преступного посягательства характеризуется рядом признаков – экономический (стоимость), физический (материальность), юридический (принадлежность другому лицу). Экономический признак криптовалюты заключается в наличии определенного курса токена к официальным валютам. Токены являются и средством платежа за обычные товары или услуги. Так, Legal Prime GS Consulting, Subway, Amazon, Ebay и ряд других организаций принимают к оплате биткоины. Юридический признак состоит в принадлежности криптокошельков конкретному лицу и проявляется через специфическую форму криптовалюты – цифровой код. Более сложный вопрос с физическим признаком, поскольку предмет материально должен быть очерчен в пространстве (т.е. должен находиться в твердом, жидком или газообразном состоянии, быть одушевленным или неодушевленным). Вместе с тем, в современной уголовно-правовой литературе все чаще стал обсуждаться вопрос о том, что объекты права собственности в условиях современного информационного общества не обязательно должны иметь материальную природу, потому как отношениям собственности в юридическом и экономическом смысле подвержены и нематериальные блага.

Следовая картина криптопреступления непосредственно коррелирует с спецификой средств совершается рассматриваемого преступления – следы представляют собой совокупность материально-фиксированных и виртуальных следов, первые – это отпечатки пальцев на устройствах

периферии, элементах системного блока, вторые – на жестких дисках компьютеров, в истории браузеров, в истории точек восстановления системы, «кэше», cookie-файлы. Виртуальные следы представляют собой зафиксированное в виде цифрового образа формальной модели изменение состояния информации в памяти абонентских электронных устройств (терминалов, биллинговых систем и т.п.), вызванное алгоритмом установленного программного обеспечения и связанное с событием преступления.

Представляется, что следы при расследовании преступлений в данной сфере имеют решающее значение, так как в большинстве случаев являются единственным источником информации и играют немаловажную роль при диагностике, позволяющей восстановить механизм совершения преступления.

В этой связи следователю необходимо:

– знать и понимать основополагающие принципы блокчейн-технологий, криповалютной экосистемы, технической и правовой природы криптовалют;

– уметь осуществлять поисково-следственную работу в DarkWeb (сервисы – https://www.producthunt.com/posts/this-person-does-not-exist или https://thispersondoesnotexist.com/; https://www.mightycall.com/virtual-phone-number/; https://www.virtualphone.com/);

– использовать возможности открытых ресурсов, например, биткойн-платформы: Blockchain.com, Blockchain.org;

– ориентироваться в листинге торговых онлайн площадок в DarkWeb – https://www.thedarkweblinks.com/ и Dark.fail (для анализа криптотранзакций целесообразно использовать бесплатный софт walletexplorer.com, который позволяет установить принадлежность кошелька к бирже, сервису или пулу; для анализа транзакций при наличии информации о биткойн-адресе преступника, мест нахождения криптовалютных банкоматов (Coinatmradar.com);

– уметь определять IP-адресов (ripe.net);

– взаимодействовать с IT-компаниями, финансовыми регуляторами (НацБанк, МинФин) по разработке механизмов обнаружения финансовых следов вывода криптовалют в фиат.

Специфична и обстановка совершения «криптопреступления» – виртуальное кибернетическое пространство. Особенностью его является то, что в результате использования информационных сетей (проводных и беспроводных технологий) в одном преступлении одновременно могут быть задействованы множество компьютеров. Соответственно находиться эти компьютеры могут в пространственно удаленных друг от друга местах и даже в разных государствах. Место «криптопреступления» характеризуется двумя составляющими: местоположением в реальном

пространстве (роль индивидуализирующей информации играет адрес местонахождения физического лица, организации, используемых ими аппаратно-программных средств) и местоположением, которое постоянно отождествляется в локальной и глобальной сети с уникальным номером – IP-адресом.

Изложенное позволяет сделать следующие выводы:

Под криптопреступлением предлагается понимать совокупность общественно опасных деяний, в ходе совершения которых в качестве предмета преступного посягательства, средства совершения или сокрытия преступления выступают криптоактивы (криптовалюта, крипто-облигации иные формы цифровых финансовых активов).

Классифицировать криптопреступления можно на две основные группы:

– Общественно опасные деяния, в ходе совершения которых в качестве предмета преступного посягательства выступают криптоактивы. К таким преступлениям можно отнести хищения, наиболее распространёнными формами которых применительно к криптопреступлениям являются хищение имущества путем модификации компьютерной информации (ст. 212 УК), вымогательство (ст. 208 УК), мошенничество (ст. 209 УК); взяточничество (ст.ст. 430-432 УК); незаконное вознаграждение (ст. 433 УК), когда криптоактивы передаются в качестве предмета взятки.

– Общественно опасные деяния, в ходе совершения которых средства совершения или сокрытия преступления выступают криптоактивы: легализация («отмывание») средств, полученных преступным путем (ст. 235 УК); изготовление, хранение либо сбыт поддельных денег или ценных бумаг (ст. 221 УК), незаконный оборот наркотических средств (ст. 224 УК), взяточничество (ст.ст. 430-432 УК), изготовление и распространение порнографических материалов или предметов порнографического характера (ст. 343 УК) и др., при совершении которых криптоактивы как средство оплаты используются для сокрытия преступления; мошенничество (ст. 209 УК), когда привлекаются фиатные деньги потерпевших для приобретения криптоактивов.

Систему характерных криминалистических признаков, образующих криминалистическую характеристику «криптопреступлений», составляют описанные выше личность криптопреступника, способ совершения преступления, способ легализации преступных доходов (через криптосервисы), предмет преступного посягательства, следования картина, обстановка совершения преступления.

Следовая картина преступлений, по которым в качестве предмета или средства выступают криптоактивы, в т. ч. криптовалюта, крипто-облигации, является весьма специфичной и традиционных криминалистических средств и методов для собирания полноценной доказательственной базы

уже недостаточно. Модернизированные схемы достижения преступниками преступного результата свидетельствуют о необходимости постоянного системного совершенствования криминалистических средств и методов выявления, фиксации и сохранения следов преступления, формирования доказательственной базы в новых, виртуальных условиях. Неотъемлемой частью организации следственной работы по расследованию преступлений в отношении криптовалюты либо с ее использованием является мониторинг развития криптоиндустрии, появляющихся на рынке IT-продуктов в области криптоанализа, ситуационного анализа активности в DarkWeb и их применения при разработке уголовно-процессуальных и криминалистических средств противодействия использованию криптовалют в преступных целях.

Библиографический список

1. Статистика МВД Республики Беларусь [электронный ресурс]. – Режим доступа: http:// www.mvd.gov.by/ru/page/statistika. – Дата доступа: 04.08.2024.

2. Как криминальный мир использует криптовалюту [электронный ресурс]. – Режим доступа: http://knife.media/cryptocriminal.– Дата доступа: 07.08.2024.

3. Ёлохова, И. В. Подходы к определению правового статуса криптовалют в ведущих странах мира / И. В. Ёлохова, М. И. Ахметова и др. / Вестн. ПНИПУ. Социально-экономические науки. – №1 (5). – 2019. – С. 201–209.

4. Сильченков, И. А. Криптовалюта как современный вызов экономической системе безопасности государства / И. А. Сильченков // Научный вестник ЮИМ. – №3. – 2019. – С. 83–87.

5. Урбан, П. Д. Криптовалюта как новое явление в преступном мире / П. Д. Урбан, А. Г. Корчагин // Теология. Философия. Право. – №1 (5). – 2018. – С. 43–51.

6. Рубцова, А. С. Криптовалюты : предмет и средство совершения преступления / А. С. Рубцова // Вестник Университета имени О.Е. Кутафина. – № 12 (52). – 2018. – С. 172–181.

7. Криптопреступность как новое криминологическое явление [электронный ресурс]. – Режим доступа: http:// https://cyberleninka.ru/article.– Дата доступа: 14.08.2024.