ОСОБЕННОСТИ РАССЛЕДОВАНИЯ НЕЗАКОННОЙ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ, СОВЕРШАЕМОЙ В СЕТИ ИНТЕРНЕТ

Бачо Ирина Игоревна

преподаватель учебной часть центра профессиональной подготовки УМВД России по Псковской области, РФ, г. Псков

SPECIAL ASPECTS OF INVESTIGATION OF ILLEGAL BANKING ACTIVITIES, COMMITTED WITH THE USE OF THE INTERNET

Irina Bacho

Teacher of the training unit of the vocational training center of the Ministry of Internal Affairs of Russia in the Pskov region, Russia, Pskov

Аннотация. В статье рассматриваются способы и схемы совершения незаконной банковской деятельности, в основе которых лежит использование информационно-телекоммуникационных сетей. Исследуется следообразование при использовании Интернета в данной преступной деятельности, а также особенности расследования обналичивания денежных средств через криптовалюту.

Abstract. The article considers ways and schemes of committing illegal banking activities, which are based on the use of information and telecommunication networks. The article studied investigation of trace formation when using the Internet in this criminal activity, as well as the special aspects of investigation of cashing funds through cryptocurrency.

Ключевые слова: блокчейн, криптовалюта, транзитные операции, обналичивание, Интернет, незаконная банковская деятельность.

Keywords: blockchain, cryptocurrency, transit operations, cashing, the Internet, illegal banking activities.

Обеспечение безопасности экономической системы, в настоящее время является одним из приоритетных направлений государственной политики России. Для сохранения устойчивого развития финансовой системы, 30.05.2018, Президентом Российской Федерации утверждена «Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [5]. Одной из основных целей данной Концепции являются выявление и пресечение незаконных финансовых операций, осуществляемые в рамках незаконной банковской деятельности.

Современный мир находится в довольно сложном временном периоде. Кризис экономического развития, повышение дифференциации уровня жизни населения, внешнеполитические проблемы, нестабильная ситуация в мире - всё это приводит к разрушению экономики страны,

традиционных ценностей, и как следствие, появлению новых видов и способов совершения преступлений, особенно в сфере экономики. На сегодняшний день, одним из основных способов осуществления незаконной банковской деятельности является обналичивание и транзитирование денежных средств. Стоит отметить, что такие преступления имеют сложные схемы совершения, являются многоуровневыми, содержат в себе сопутствующие преступления (ст. ст. 173.1; 174.1, 187, 159 УК РФ [7]) и анализ судебной и следственной практики показывает, что расследование подобных видов преступлений вызывает у правоохранительных органов трудности.

Особую тревогу вызывают преступления, связанные с незаконным обналичиванием и транзитированием денежных средств, совершаемые с использованием информационно-телекоммуникационных сетей. Наряду со «стандартными» способами «обнала», к которым можно отнести заключение договора займа, через фирмы-однодневки путем мнимой сделки, через комиссию по трудовым спорам, снятие наличных денежных средств под отчет либо через корпоративные карты организации и тд., злоумышленники придумывают всё новые, более изощренные способы и схемы обналичивания денежных средств, при этом начиная активно использовать современные технологии и совершать данное преступление на просторах Интернета.

Яркий способ незаконного обналичивания и тразитирования денежных средств, осуществляемый с использованием электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») – это обналичивание через криптовалюту. Стоит отметить, что на сегодняшний день криптовалюта не является средством платежа, но, при совершении преступления, она выступает именно как «платежное средство» и является средством совершения противоправного деяния. Данный способ привлекает всё больше злоумышленников, так, согласно статистическим данным МВД России, за 2024 год количество совершенных преступлений данной категории составляет 60% от общего числа всех преступлений в стране [6]. Происходит это ввиду того, что у криптовалюты отсутствует законодательное регулирование и она совершенно лишена контроля со стороны государства. Также нет единого контролирующего центра, отслеживающего транзакции и ведущего их учет. Регистрация на криптобиржах происходит зачастую анонимно, без указания идентифицирующих данных лица, и к тому же, в большинстве случаях, биржи находятся за пределами РФ, и их деятельность не попадает под российское законодательство. Использование криптовалюты при совершении преступлений, создает у правоохранительных органов трудности в расследовании и в доказывании виновности лиц, причастных к совершению подобных преступлений.

Однако, результат, на которой нацелены злоумышленники, при совершении обналичивания и транзитирования денежных средств – получить денежные средства в наличной форме. И способ с использованием криптовалюты не является исключением. В этом случае, даже при том, что некоторые криптобиржи обеспечивают полную анонимность при их использовании, при совершении транзакций и при переводе виртуальных монет в наличный эквивалент, преступники оставляют определенные следы, по которым их и можно установить.

Самой популярной криптовалютой, используемой в качестве платежного средства при совершении преступления выступает биткоин. Биткоин позволяет делать анонимные платежи, то есть при создании биткоин-кошелька на бирже, не нужно указывать персональные (паспортные) данные при регистрации, в отличие от открытия счета в банке. Однако, система биткоин сохраняет информацию обо всех произведенных транзакциях. Сведения о том, куда, когда и сколько переведено виртуальных монет, записываются в блокчейны. Блокчейн в переводе с английского языка «blockchain» - «цепочка блоков». Именно эти блоки и хранят транзакции, которые происходят в сети. Иными словами, блокчейн – это база данных, содержащая информацию об адресе отправителя (IP-адрес), адрес получателя, сумме транзакции, времени отправки транзакции, количестве подтверждений и хеш-транзакции. Казалось бы, всё просто, правоохранительным органам необходимо узнать номер кошелька, который принадлежит злоумышленнику, обычно это устанавливается при производстве обыска, с изъятием компьютерной, мобильной техники и иных электронных носителей. И уже при производстве компьютерных экспертиз, эксперты могут дать полную информацию о том, какими биржами пользовались злоумышлиники, установить их логины и пароли от ученых записей, и номер криптокошелька. По номеру кошелька в системе биткоин,

на сайте «blockchain.info» можно узнать всю информацию о проведенных транзакциях, а также об IP-адресах получателя и отправителя, так как блокчейн находится в открытом доступе. Зная IP-адреса, сотрудники силовых структур могут установить местонахождение устройства, с которого происходил выход в сеть, ну а дальше не трудно выявить и само лицо, виновное в совершении преступления. К тому же, некоторые преступники используют «холодные» криптокошельки (устройства на подобии флешки), которые также могут быть найдены и изъяты при обыске [2].

Однако, злоумышленники придумывают новые схемы и пути запутывания своих следов, в результате чего расследование подобных видов преступлений становится очень затруднительным.

Рассмотрим некоторые схемы, используемые для запутывания следов обналичивания и транзитирования денежных средств через криптовалюту [4]:

1. Подставные криптокошельки. Это самый простой метод избавления от «грязной» крипты. Данный прием обычно используется «новичками» в преступной деятельности, и актуален он лишь на первых этапах совершения преступления. Ведь все транзакции всё равно отражаются в блокчейне, и переводы на подставные криптокошельки не спасают от отслеживания переводов. Однако, это неплохой способ для начала запутывания следов, и дробления крупных сумм на мелкие части, как подготовительный этап для дальнейшего отмывания. А если речь идет о крупных финансовых операциях, которые совершаются организованными преступными формирования, то в таком случае могут использоваться тысячи подставных кошельков. Стоит отметить, что по данным исследования «Big Ideas 2023» в мире на сегодняший день насчитывается около 3,2 млрд. криптокошельков.
2. Децентрализованные криптобиржи. Обычно это мелкие криптобиржи, которые предлагают анонимные транзитные услуги, но в таком случае велик риск, что сама криптобиржа может быть мошеннической, и злоумышленник сам потеряет все деньги, ведь цепочка транзакций в блокчейне обрывается, как только криптовалюта заводится на биржу. С одной стороны, это очень удобно для запутывания следов и дальнейшего обналичивания реальных денежных средств, а с другой злоумышленник уже не контролирует свои виртуальные деньги, а доверяет контроль над ними третьи лицам (бирже). Такие криптобиржи работают как крипто отмывочные, через некоторые биржи может ежегодно проходить миллионы долларов. Но, чем больше оборотов наращивает такая криптобиржа, и чем больше «грязной» криптовалюты через нее проходит, то со времен она привлечет к себе внимание правоохранительных органов, и в таком случае можно будет установить информацию о транзакциях, и о лицах, виновных в совершении преступлений.
3. Финансовые «сервисы-матрешки». Данные сервисы выступают как посредники между криптобиржами и злоумышленниками. Они позволяют торговать на криптобирже без создания аккаунта. То есть, злоумышленник обращается к «сервису-матрешке», с ним связывается агент, который будет курировать сделки с криптовалютой, а злоумышленник только дает указание куда, когда и сколько перевести криптовалюты. В данном случае очень сложно связать транзакции с конкретным лицом, и расследование уголовного дела очень затрудняется. Однако, подобные сервисы имеют низкий рейтинг безопасности и не популярны в использовании у злоумышленников, потому что риск потерять все деньги очень высок.
4. Криптомиксеры. Представляют собой сервисы, которые позволяют скрыть информацию о транзакциях. Злоумышленник, оказывающий услуги по обналичиванию денежных средств, отправляет криптовалюту на сервис-миксер, где она, посредством транзитных операций соединяется со всеми монетами, которые имеются на сервисе, а дальше, спустя некоторое время, «смешанная» криптовалюта поступает на адрес конечного получателя. Связь между отправителем и получателем скрыта. В последующем получатель уже обналичивает криптовалюту и передает наличные денежные средства клиенту. Стоит отметить, что подобные сервисы находятся под пристальным вниманием правоохранительных органов, и в случае, если обнаруживаются обороты «грязной» (нелегальной) криптовалюты, то посредством проведения определённых следственных действий (обыск, выемка, допросы и т.д.) и оперативно-розыскных мероприятий, правоохранительные органы могут получить

информацию о транзакциях и связать их с лицами, причастными к совершению преступлений, связанных с незаконным обналичиванием денежных средств.

5. Даркнет. Не так давно, на просторах «темного интернета» стали появляться сервисы, которые предоставляют услуги по обналичиванию денежных средств через криптовалюту. Для рекламы и поиска клиентов они используют «черный рынок» (даркнет). Конфиденциальность и анонимность – обязательная часть сделки. Сервисы не уточняют каким образом в действительности они будут работать, но результат их услуги – выход в наличный кэш. Однако, даже учитывая, что даркнет использует скрытые сети, неиндексированные ресурсы, нестандартные протоколы и порты, и позиционируют себя как «неуловимые», правоохранительные органы научились выявлять, расследовать, а самое главное доказывать преступную деятельность, осуществляемую на «черном рынке». Яркий пример тому, прекращение в 2022 году деятельности самого известного даркнет-маркета «HYDRA» («Гидра»), и установление виновных лиц, причастных к организации данной преступной деятельности. Стоит отметить, что, предварительное расследование уголовного дела, в отношении российских граждан, преступная деятельность которых связана с «Гидрой», окончено, и в настоящее время уголовное дело находится на рассмотрении во Всеволожском городском суде Ленинградской области [3].
6. Криптообменники. Напомним, что основной результат незаконного обналичивания и транзитирования денежных средств (в том числе и через криптовалюту) – выход в кэш. И первоочередная цель преступников, занимающихся незаконным обналом – как конвертировать криптовалюту в фиатные (наличные) деньги анонимно. После введения законов, контролирующих оборот криптовалюты, все пользователи крупных бирж в обязательном порядке должны подтверждать свои личности, то есть предоставлять паспортные данные. Поэтому получить наличные денежные средства через криптобиржи анонимно невозможно. Для этого злоумышленники пользуются «черными обменниками». Существует два варианта таких обменников. Первый – онлайн. Они представляют собой сайты, которые не требуют регистрации (в редких случаях необходимо указать адрес электронной почты). Схема работы с данными обменниками довольна проста: на сайте оставляется заявка на получение наличных денежных средств, после ее рассмотрения, дается номер кошелька, куда переводятся виртуальные монеты. Наличные денежные средства злоумышленник получает через бесконтактную доставку. Посылку оставляют в постамате, и код для получения отправляют злоумышленнику. Стоит отметить, что такие пользоваться такими онлайн-обменниками очень рискованно, существует большая вероятность, что посылка окажется пустой. Второй вариант – офлайн- обменники. Как правило, они находятся в крупных городах России, таких как Москва и Санкт-Петербург, и представляют собой офисы (помещения), похожие на отделения банковских организаций, где и предоставляются услуги по конвертации криптовалюты. Наличные деньги можно получить прямо после перевода витруальных монет. Однако, таких обменников очень мало, и они находятся под пристальным вниманием правоохранительных органов, оснащены камерами, и в случае возникновения подозрений, что лицо совершает незаконное обналичивание, установить личность довольно просто. Поэтому преступники обычно пользуются услугами закрытых обменников. Сделки проходят как правило в квартирах, редко в офисах, сначала происходит перевод виртуальных монет и только потом готовят наличные денежные средства, и через некоторое время злоумышленник получает свой заказ. Это очень небезопасный способ перевода криптовалюты в наличные для злоумышленников, ведь зачастую, такими «закрытыми обменниками» являются сами правоохранительные органы, которые задерживают преступников непосредственно на месте с поличным, что намного упрощает дальнейшее расследование преступления [1].

Таким образом, подводя итог, можно сделать вывод, что операции с криптовалютой вовсе не так анонимны, как их позиционируют. Осуществить транзитные операции, а уж тем более конвертировать виртуальные монеты в наличные денежные средства и при этом не оставить никаких следов просто невозможно. Несомненно, расследование подобных преступлений представляет сложность и требует большого количества времени. В первую очередь это связано с плохой технической оснащенностью правоохранительных органов, ведь преступления, совершаемые с использованием информационно-телекоммуникационных сетей, совершаются в большей степени в Интернете, и для установления следообразования

преступной деятельности, требуются новые и эффективные технические средства, позволяющие быстро обнаружить данные следы, а самое главное процессуально их оформить, чтобы в соответствии с законом, выявленные сведения смогли стать доказательствами по уголовному делу. Как итог, стоит отметить, что необходимо выработать единую тактику и методику расследования подобных категорий преступлений, ведь незаконное обналичивание и транзитирование денежных средств, особенно совершаемые с использование информационно-телекоммуникационных сетей представляют угрозу экономической безопасности не только России, но и всего мира.

Список литературы:

1. Анонимные денежные переводы и подводные камни криптовалютных операций [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/587940/ (дата обращения 07.01.2025).

2. Зиновьева Н.С. Возможности блокчейн-технологии в раскрытии и расследовании преступлений в интернет-пространстве // Вестник Восточно-Сибирского института МВД России. – 2018. – № 3(86). –

С. 184–189.

3. Исследование крупнейшего теневого рынка Hydra [Электронный ресурс]. –Режим доступа: https://www.securitylab.ru/news/543799.php (дата обращения: 06.01.2025).

4. Как отмывают криптовалюту: самые популярные способы / Блог Касперского [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/crypto-laundering-and-ransomware/35298/ (дата обращения 06.01.2025).

5. Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (утв. Президентом РФ 30.05.2018) [Электронный ресурс]. –Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_299375/ (дата обращения: 05.01.2025).

6. Статистические данные МВД России за 2024 год [Электронный ресурс]. –Режим доступа: https://мвд.рф/reports/item/42989123/ (дата обращения 05.01.2025).

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024) (с изм. и доп., вступ. в силу с 08.01.2025) // «Собрание законодательства Российской Федерации» № 25 от 17.06.1996 ст. 2954 [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_10699/, (дата обращения 11.01.2025).