правонарушитель должен находиться под оперативным контролем со стороны оперуполномоченного в течение одного года. Собственно сам оперативный контроль будет осуществляться также путем проведения ОРМ, т. е. как минимум должен проводиться мониторинг страниц в социальных сетях фигуранта. Ведь будет нелогично оставить данное лицо без контроля со стороны оперативного подразделения, поскольку необходимо убедиться в том, что фигурант отказался от своей преступной деятельности.

Если же фигурант продолжает совершать действия, попадающие под правонарушение экстремистской направленности, то оперуполномоченный опять должен задокументировать правонарушение экстремистской направленности путем проведения ОРМ и только после этого представить результаты ОРД в органы предварительного расследования.

В связи с этим возникает несколько справедливых вопросов. Во-первых, насколько законно проведение ОРМ в целях выявления и документирования административного правонарушения? И, во-вторых, на каком основании будут проводиться ОРМ в отношении фигуранта после привлечения его к административной ответственности?

В поисках ответа на первый вопрос полагаем необходимым обратиться к Федеральному закону Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Закон от ОРД). Так, в соответствии с частью второй ст. 5 Закона об ОРД не допускается осуществление ОРД для достижения целей и решения задач, не предусмотренных Законом об ОРД. В ст. 1 Закона об ОРД определяется, что целью данного вида деятельности является защита прав и свобод человека и гражданина от преступных посягательств. В ст. 2 рассматриваемого закона определяются задачи ОРД, в числе которых называются выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших. Таким образом, законодатель прямо указывает на то, что ОРД предназначена для противодействия преступности и преступникам, а не административным правонарушениям и правонарушителям.

Таким образом, на основании анализа норм Закона об ОРД можно сделать вывод, что выявление и документирование административных правонарушений путем проведения ОРМ является недопустимым.

Однако необходимо также отметить, что выявление административных правонарушений экстремистской направленности без проведения ОРМ является крайне затруднительным.

На основании изложенного можно констатировать, что сегодня все больше происходит сращивание административной деятельности полиции и ОРД. Например, при проведении ОРМ оперуполномоченными активно используются меры административного пресечения (задержание, личный досмотр и т. д.), право на применение которых предоставлено Федеральным законом Российской Федерации от 7 февраля 2011 г. № 3-ФЗ «О полиции», который регламентирует административную деятельность полиции. Таким образом, назрела необходимость совершенствования оперативно-розыскного законодательства.

В ходе анализа оперативно-розыскного законодательства, а именно положений ст. 7 Закона об ОРД, содержащей основания для проведения ОРМ, ответ на второй вопрос, об основаниях проведения ОРМ в отношении фигуранта после привлечения его к административной ответственности нами найден не был.

В заключение необходимо отметить, что обозначенные нами проблемы и предложенные решения требуют более углубленного изучения.

УДК 343.98

Д.И. Шнейдерова

DEFI И СТЕЙБЛКОИНЫ В МЕХАНИЗМЕ ХИЩЕНИЯ КРИПТОВАЛЮТ

Развитие криптовалютной индустрии в совокупности с базовыми принципами ее функционирования (децентрализация, анонимность, трансграничность и т. д.) послужило основой для формирования нового сектора децентрализованных виртуальных финансовых инструментов и сервисов, именуемого Decentralized finance (DeFi). DeFi – понятие собирательное, объединяющие в себе систему сервисов и платформ, действующих на базе публичного блокчейна и не имеющих координационно-управляющего центра. Простота алгоритмов создания, использования и подделки продуктов DeFi не остались незамеченными представителями преступной деятельности, активно применяющими их в своих схемах при хищении криптовалют, реализуемых путем мошенничества, вымогательства или использования компьютерной техники, сопряженного с несанкционированным доступом к компьютерной информации.

С целью формирования криминалистической методики расследования хищений в сфере оборота криптовалют полагаем целесообразным рассмотрение механизмов и способов совершения таких хищений с использованием платформ системы DeFi.

Все сервисы DeFi можно разделить на четыре самостоятельных сектора: децентрализованное кредитование и выдача займов, функционирование децентрализованных бирж, оборот деривативов и криптовалютных активов, а также выпуск и оборот стейблкоинов.

Специфика децентрализованного кредитования заключается в выдаче криптовалютного займа посредством двустороннего контакта между кредитором и заемщиком без участия третьей стороны. Кредитная платформа в данном случае выступает в качестве площадки, содействующей налаживанию связи сторон и предоставляющей смарт-контракты для оформления сделки между ними за минимальную комиссию, но никак не влияет на одобрение самого займа и не является кредитором. В криптокредитных отношениях в качестве кредитора выступает инвестор, который вкладывает свои криптовалюты в пул криптокредитной платформы с целью получения за их использование заемщиком дивиденда в виде некоторого количества криптовалют. Заемщиком выступает любой пользователь, желающий взять в качестве займа определенный вид криптовалюты на некоторый срок (зависит от вида криптокредита). Отличительной чертой децентрализованного кредитования выступает необходимость внесения заемщиком обеспечения криптокредита в виде криптовалют иного порядка и в большем количестве, чем получаемая в кредит криптосумма. Таким образом, смарт-контракт регулирует передачу инвестором криптовалют одного номинала заемщику, а заемщиком – криптовалют другого номинала, но в большем размере (размер обеспечения рассчитывается по курсу криптобиржи, выбираемой в качестве базовой оракулом криптокредитной платформы).

Криптокредиты нередко становятся средством достижения преступного умысла мошенников и хакеров по неправомерному завладению криптовалютами. При этом мошеннические действия могут исходить как от кредиторов, так и от заемщиков, которые, получая залог или займ в криптовалюте, заранее не намереваются их возвращать и выполнять условия сделки, прописанные смарт-контрактом. Кредитная криптовалюта, в частности пул платформы (криптовалюты инвесторов), также может стать предметом хищения посредством компьютерной техники, когда хакерам удается воспользоваться ошибками или уязвимостью смарт-контракта (производят манипуляции с флэш-кредитами путем завышения номинального курса кредитной валюты, что позволяет вернуть залог и получить часть кредитной валюты) и вывести все активы их хранилища.

Децентрализованные биржи, в отличие от стандартных, не имеют центра управления процессами и позволяют пользователям заключать сделки по приобретению криптовалют напрямую без посредника (т. е. их механизм сходен с криптокредитами). При этом протокол биржи не только предоставляет возможность заключения сделки, но и сам автоматически подбирает контрагента по заданным параметрам, ввиду чего биржа выполняет одновременно функции и биржи, и брокера.

Децентрализованные биржи чаще всего подвержены хакерским атакам, вследствие которых с их пулов выводятся временно хранящиеся активы, а также мошенническим действиям по размещению на бирже дубликатов реальных криптовалют и токенов. Создание дублирующих криптовалют стало возможным по причине открытости протоколов децентрализованных платформ, которые позволяют любому пользователю спрограммировать свою криптовалюту или токен (в том числе стейблкоин). Примечательно, что дубликат торгуется на бирже одновременно с реальной криптовалютой и по той же цене, а нередко и не в единственном количестве, т. е. две и более подделки одновременно. Поскольку поддельный токен продается за реальную криптовалюту, то можно говорить о том, что криптовалюта в данном механизме одновременно выступает и как средство реализации преступного умысла, и как предмет хищения.

Стейблкоины – разновидность криптовалют, которые имеют обеспечение либо в фиатных денежных средствах, либо в криптовалюте. Выделяют три вида стейблкоинов: обеспеченные фиатом, обеспеченные криптовалютой и алгоритмические стейблкоины. К числу децентрализованных проектов DeFi относятся только алгоритмические стейблкоины, отличие которых от двух других видов заключается в отсутствии эмиссионного центра и поддержании курса за счет действия смарт-контракта и сверхобеспечения. Так, проект по обороту алгоритмических стейблкоинов направлен на выпуск одной единицы стейблкоина, которая обеспечивается реальной криптовалютой в соотношении 1 : 1,5, т. е. при эмиссии 100 стейблкоинов они должны быть обеспечены 150 единицами какой-либо криптовалюты. Обеспечение блокируется смарт-контрактом и хранится до тех пор, пока пользователь не захочет запустить обменный процесс. Выпуск таких децентрализованных стейблкоинов зависит от курса криптовалют, которыми они обеспечены: чем выше курс криптовалют, тем больше единиц стейблкоина будет эмитировано, и наоборот. Основная функция всех стейблкоинов – служить расчетной единицей при международных переводах, заменив собой фиатные деньги, поскольку они не требуют участия посредника при переводе, не зависят от времени и места осуществления операции, легко конвертируются в обеспечиваемую валюту.

Стейблкоины так же, как и другие токены в DeFi, подвержены дублированию, пулы, хранящие обеспечение, – хакерским атакам и хищению криптовалютных средств, а сами проекты нередко являются заведомо мошенническими (т. е. создается проект по выпуску децентрализованных стейблкоинов, который после сбора криптовалютного обеспечения ликвидируется). Имело место и вымогательство, когда хакер, получив доступ к пулу платформы по эмиссии стейблкоинов, перевел все крип-

товалюты на свой счет и выставил компании-владельцу проекта требование о переводе ему выкупа в особо крупном размере в криптовалютах иного вида, угрожая распродать похищенное обеспечение.

Таким образом, сервисы DeFi, ставя своей целью создание открытой, бесплатной и трансграничной системы реализации финансовых услуг, вместе с преимуществами несут и определенные риски, связанные с беспорядочностью системы (т. е. сервисов достаточно много и порой невозможно определить, нацелен ли тот или иной на оказание реальных услуг либо заранее преследует преступные цели), волатильностью курса криптовалют и подверженностью платформ мошенническим действиям и хакерским атакам. Отсутствие контрольного звена негативно сказывается не только на обеспечении безопасности сделок, проводимых в системе DeFi, но и на процессе расследования и раскрытия хищений криптовалют ввиду невозможности изъятия криминалистически значимой информации о пользователях и проводимых ими сделках, необходимой для установления личности преступников и отыскания похищенных криптосредств по цифровым следам, что является актуальным вопросом для дальнейшего криминалистического исследования в данной области.

УДК 343.985

О.Н. Шуляковский

ЗАРУБЕЖНЫЙ ОПЫТ ОБЕСПЕЧЕНИЯ ГОСУДАРСТВЕННОЙ ЗАЩИТЫ ЛИЦ, СОТРУДНИЧАЮЩИХ С ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ

(на примере государств – членов Европейского союза)

Анализ практики противодействия преступным проявлениям показывает, что невозможно обеспечить раскрытие преступлений и неотвратимость уголовной ответственности совершивших их лиц без противопоставления криминальной деятельности целенаправленного комплекса оперативно-розыскных мероприятий и следственных действий, без использования в качестве доказательств материалов оперативно-розыскной деятельности, без привлечения граждан к борьбе с преступностью, в том числе на конфиденциальной основе.

В большинстве случаев как ученые в области оперативно-розыскной деятельности, так и практические сотрудники оперативных аппаратов убеждены, что получить, закрепить и надлежащим образом реализовать оперативную информацию часто невозможно без такой важной составляющей, как разведывательная деятельность конфидентов. Нередко в связи с сотрудничеством с правоохранительными органами лица, оказывающие содействие органам внутренних дел на конфиденциальной основе, а также их близкие рискуют стать объектами давления или мести со стороны лиц, в отношении которых осуществляется уголовное преследование. Таким образом, конфиденты действуют в условиях риска, подвергая себя, а также в ряде случаев своих родственников, в том числе иных лиц, которых они обоснованно считают близкими, существенной опасности.

В ряде зарубежных государств имеются правовые нормы, всесторонне регулирующие вопросы обеспечения безопасности свидетелей, в том числе свидетелей из числа конфидентов или, как их по-другому называют, информаторов (осведомителей). Данные нормы также определяют компетенцию органов, в ведении которых находится применение мер по обеспечению безопасности данных лиц. Интересным, по нашему мнению, является изучение опыта правового регулирования мер по обеспечению безопасности, существующих в Италии и Германии.

Система государственной защиты свидетелей в Италии формировалась на базе ряда законодательных актов, которые в конце 80-х – начале 90-х гг. предусматривали определенные привилегии и льготы для лиц, совершивших преступления, сотрудничающих со следствием. В 2001 г. законодателем внесены существенные изменения, разграничившие порядок защиты преступников, помогающих правосудию, и свидетелей.

Для реализации указанных изменений в структуре Центральной службы защиты созданы два специализированных департамента. Нынешняя структура органов, включенных в систему обеспечения государственной защиты, и непосредственно сам механизм включения лиц, подлежащих государственной защите, в программу выглядят следующим образом. Органом, применяющим меры по обеспечению безопасности, является Центральная служба защиты, учрежденная в 1991 г. в составе Департамента общественной безопасности. В ее структуру входят четыре дивизиона (управления), на каждый из которых возложены специфические функции: 1) охраны свидетелей; 2) охраны осведомителей; 3) управления и бухгалтерии; 4) общих дел. Последний занимается обеспечением деятельности всех вышеуказанных дивизионов, а также осуществляет научно-исследовательскую работу, поддерживает взаимодействие с Интерполом и полицейскими ведомствами иностранных государств, обеспечивает юридическое, медицинское, кадровое и документационное обеспечение. Дивизионы состоят из секций, отвечающих за отдельные направления работы. Центральная служба защиты отвечает за реализацию программы защиты свидетелей и осведомителей, которая разрабатывается Центральной комиссией, ею же принимается решение об применении конкретной меры защиты.