ВОПРОСЫ РОССИЙСКОЙ ЮСТИЦИИ
ВЫПУСК № 26

УДК 343.7

Буравов Илья Сергеевич
Самарский юридический институт ФСИН России
Факультет внебюджетной подготовки
Россия, Самара
mailto:buravov.law@outlook.com
Ilya Buravov
Samara Law Institute of the Federal Penitentiary Service of Russia
Faculty of extra-budgetary training
Russia, Samara

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ РАЗРАБОТКИ И ПРИМЕНЕНИЯ СМАРТ-КОНТРАКТОВ

Аннотация: в статье рассматриваются возможности использования смарт-контракта в преступных целях. Отмечается, что смарт-контракт может быть, как предметом преступного посягательства, так инструментом для облегчения совершения преступлений, например, он может использоваться для поиска контроля исполнителя преступления со стороны подстрекателя (заказчика). По результатам исследования предлагаются изменения в уголовное законодательство, направленные на охрану общественных отношений, возникающих в сфере разработки и применения смарт-контрактов.

Ключевые слова: смарт-контракт, криптовалюта, хакерские атаки, преступления, блокчейн.

PROBLEMS OF QUALIFICATION OF CRIMES IN THE FIELD OF DEVELOPMENT AND APPLICATION OF SMART CONTRACTS

Annotation: the article examines the use of smart contracts for criminal purposes. It is noted that the smart contract may be both the subject of criminal offence and a tool to

facilitate the commission of crimes, for example, it may be used to seek control of the perpetrator of the crime by the instigator (customer). As a result of the study, amendments to the criminal law are proposed to protect the social relations arising in the development and application of smart contracts.

Key words: smart contract, cryptocurrency, hacking, crimes, blockchain.

Политическое и экономическое давление на Россию заставляет предпринимателей и государство искать новые способы взаиморасчетов с экономическими партнерами из разных стран мира. В связи с этим увеличивается внимание к криптовалютам для совершения различных сделок. Проведение транзакций криптовалюты в рамках сложных договорных конструкций возможно с помощью смарт-контракта. В рамках статьи под ним будет подразумеваться автоматизированные самоисполняющиеся программы, базирующиеся на технологии распределенного реестра (блокчейн).

Смарт-контракт на платформе блокчейна позволяет выполнять различные обязательства (например, выплачивать страховку при наступлении страхового случая или передачи предоставлений по договору купли-продажи при условии, что одной из сторон сделки передается криптовалюта или токен), также большим потенциалом смарт-контракты обладают в банковской и финансовых сферах. Вышеуказанное свидетельствует о необходимости создания эффективных средств защиты прав субъектов правоотношений, в том числе и методами защиты уголовного права, а также проведения теоретических исследований преступлений в этой сфере.

По-нашему мнению, возможно выделить следующие проблемы во внедрении и использовании смарт-контрактов, которые требуют оценки со стороны уголовного права: 1) как квалифицировать деяния, направленные на противоправное завладение криптовалютой и другими токенами 2) уязвимость программного кода смарт-контракта для хакерских атак, возможность создания

лицом, разрабатывающим смарт-контракт, уязвимостей для дальнейшего завладения цифровыми активами; 3) возможность использования смарт-контракта для организации «заказных» преступлений.

Первая проблема заключается в том, что традиционный вещной признак хищения исключает криптовалюту и другие цифровые активы из некоторых составов преступлений Главы 21 УК РФ, в то же время цифровые активы сохраняют за собой юридический и экономический критерии предмета хищения. В связи с этим, если и за противоправное завладение криптовалютой возможно привлечение к уголовной ответственности, то это возможно в рамках преступлений против собственности лишь по некоторым составам преступлений главы 21 УК РФ - ст. 159, 159.6 163,165 УК РФ. В то же время, если противоправное завладение криптовалютой совершаться путем хакерских атак, то преступнику грозит, по-нашему мнению, непропорционально мягкое наказание, в лучшем случае это будет совокупность преступлений ст. 165 или 159.6 УК РФ + преступление в сфере компьютерной информации (Глава 28 УК РФ).

В связи с этим можно отметить, что в условиях реформирования экономических отношений существующая доктрина и система преступлений против собственности не отражают комплексной модели уголовно-правовой охраны имущественных отношений. В связи с этим мы поддерживаем позицию о необходимости разделения составов преступлений главы 21 УК РФ. Для этого необходимо пересмотреть главу 21 УК РФ, разделив составы преступлений на преступления против материальных и нематериальных благ. Таким образом, будет необходимость в переименовании главы 21 УК РФ, например, «Преступления против собственности и цифровых прав» или «Преступления против собственности и объектов оборота гражданских прав».

Далее нам бы хотелось отметить, что смарт-контракт, представляя собой компьютерный код, может обладать недоработками (уязвимостями), которыми

может воспользоваться злоумышленник для неправомерного завладения криптовалютой или иными токенами.

Так Е. Е. Богданова приводит пример, показывающий уязвимость смарт-контрактов от действий хакеров, которые могут выявить уязвимость в компьютерном коде, чтобы неправомерно завладеть криптовалютой, так в 2016 году злоумышленники в результате атаки на смарт-контракт DAO, в котором были выявлены ошибки, удалось вывести более 53 млн долл. США. Это событие привело к падению стоимости DAO-токенов на торгующих ими биржах и последующему прекращению существования организации [1, с. 113]. В 2014 году хакеры завладели 950 т. биткоинами, в результате хакерских атак на биржу mr.gox. Вышеуказанное свидетельствует о рисках использования смарт-контрактов в крупных коммерческих проектах [2].

Возможно выделить несколько уязвимостей, которые позволяют нарушить информационную безопасность смарт-контракта:

- уязвимости, связанные с ошибками реализации (программирования) смарт-контракта;

- уязвимости, связанные с ошибками при построении архитектуры системы на основе распределенных реестров;

- уязвимости, связанные с логикой смарт-контракта;

- уязвимости, связанные с реализацией алгоритма консенсуса.

Для нас интересны прежде всего уязвимости первого типа, которые в основном допускаются в результате недосмотра, ошибок на этапе разработки смарт-контракта. По нашему мнению, программист может намерено создать уязвимость в коде смарт-контракта, чтобы противоправно завладеть криптовалютой или другим активом. В случае, если он самолично создает и пользуется такой уязвимостью для совершения преступления, то он должен привлекаться к уголовной ответственности в качестве исполнителя преступления. В то же время, если лицо узнает об уязвимости спустя некоторое

время, но сам не вмешивается в работу смарт-контракта, информационной системы, а предоставляет информацию об уязвимости другим лицам, то его можно привлекать к уголовной ответственности в качестве пособника при условии, что он осознает, что сообщает информацию лицам, которые намерены совершить преступление.

Также интересным представляется момент, что смарт-контракт может использоваться злоумышленниками для контроля совершения «заказных» преступлений и автоматического перечисления вознаграждений исполнителю. Это объясняется тем, что смарт-контракт способен обеспечить анонимность сторон, например, транзакции в биткоине не несут никакой информации о контексте платежа, который бы позволил идентифицировать перечисление криптовалюты, как связанное с преступной деятельностью [3, с. 212].

На данный момент смарт-контракты используются в работе площадки darkleaks через которую продается информация, представляющая коммерческую, банковскую или государственную тайну. Платформа позволяет потенциальным покупателям перед совершением транзакции ознакомиться со случайно выбранной частью документа или файла. После того как собирается достаточная запрошенная продавцом информации сумма остальная часть расшифровывается и отправляется покупателям или публикуется в открытом доступе [4].

Также смарт-контракт позволяет перечислить вознаграждение исполнителю за совершенное преступление, также в случае, если исполнитель не смог довести преступление до конца по каким-либо причинам, то смарт-контракт не перечисляет вознаграждение и криптовалюта остается у заказчика преступления.

Рассмотрим, как может использоваться смарт-контракт в противоправных целях на примере хакерской атаки на веб-ресурс. Так вначале должен быть разработан программный код смарт-контракта, который содержит алгоритм

отслеживания изменений на сайте и механизмы проверки наличия денежных средств у заказчика и перечисления денежных средств исполнителю. Потом заказчик и исполнитель достигают соглашения о том, на какой сайт должна быть совершена атака и размер вознаграждения в случае успеха. После чего злоумышленник совершает хакерскую атаку.

Далее смарт-контракт или программа, которая передает в него данные может зафиксировать прекращение работы веб-ресурса или появления на нем информационной провокации, которая размещена по заказу заинтересованного лица (для этого в программном коде контракта размещается ссылка на сайт и текст, который необходимо на нем разместить или код ошибки). Смарт-контракт фиксирует появление нужно текста на сайте и автоматически перечисляет вознаграждение на кошелек исполнителя.

Смарт-контракт может отслеживать исполнение «обязательств» по взлому учетных записей, например, злоумышленник заказывает у «хакера» получение данных учетной записи жертвы в социальной сети или мессенджере. В таком случае смарт-контракт проверяет достоверность передаваемой «хакером» данных ученных записи жертвы после чего предоставляет возможность получить вознаграждение исполнителю [5, с. 4].

Также можно автоматизировать отслеживание процесса совершения убийства медийной личности, политиков, общественных деятелей. Для этого в коде смарт-контракта возможно включить ключевые слова «ФИО», «погиб», «убит» и ссылки на популярные интернет-издания, которые сложно заподозрить в публикации недостоверной информации. В случае появления ключевых слов в статьях на данных ресурсах исполнителю автоматически будет отправлено вознаграждение.

Аналогично смарт-контракты можно разработать для заказа совершения других преступлений - поджоги, теракты и другие преступления, которые будут отражены СМИ. Для этого также можно использовать отслеживание появления

ключевых слов сразу в нескольких источниках, а в качестве ключевых слов могут быть место, время, способ, орудия и средства совершения преступления.

В завершении можно отметить следующие. По нашему мнению, смарт-контракты будут постепенно находить все более широкое применение вместе с цифровыми активами, что неизбежно будет увеличивать и без того большой интерес со стороны злоумышленников, как для противоправного завладения различными активами, так и упрощения поиска исполнителей для совершения преступлений. Таким образом, смарт-контракт в зависимости от ситуации может быть как предметом преступления, так и одним из средств достижения цели преступления.

В связи с вышесказанным и учитывая, что сейчас отсутствует единая позиция по вопросу квалификации преступлений, совершаемых в отношении цифровых активов и они активно используются в преступной деятельности для оплаты различный услуг, товаров, предлагается разделить составы преступлений главы 21 УК РФ на преступления против материальных и нематериальных благ, а также разработать квалифицированные составы для преступлений в сфере компьютерной информации.

Список литературы:

1. Богданова Е. Е. Проблемы применения смарт-контрактов в сделках с виртуальным имуществом // Lex russica (Русский закон), 2019, № 7 (152), С. 108-118.

2. Биткоин-биржу обанкротили хакеры / Коммерсантъ [Электронный ресурс] // URL: https://www.kommersant.ru/doc/2426539 (Дата обращения: 13.03.2023).

3. Буравов И. С. Проблемы квалификации преступлений в сфере разработки и применения смарт-контрактов // XLVIII Самарская областная

студенческая научная конференция: тезисы докладов, Самара – 11–22 апреля 2022 года, С. 211-212.

4. Juels, Ari, Ahmed Kosba, and Elaine Shi. «The ring of gyges: using smart contracts for crime», 2015 [Электронный ресурс] // URL: https://eprint.iacr. org/2016/358.pdf.

5. Ndiaye M., Konate P. K. Cryptocurrency crime: Behaviors of malicious smart contracts in blockchain // International Symposium on Networks, Computers and Communications (ISNCC), IEEE, 2021, С. 1-8.