УДК 343.7(100):347.73

Зарубежный опыт уголовно-правовой охраны сферы функционирования блокчейн и оборота криптовалют*

Мкртчян С.М.
Кандидат юридических наук, доцент кафедры уголовного права Волгоградского государственного университета

Статья посвящена изучению уголовного законодательства зарубежных государств в части регламентации оснований ответственности за совершение преступлений, получивших распространение в сфере функционирования блокчейн и оборота криптовалют. Выделены наиболее удачные технико-юридические и содержательные приёмы формулирования соответствующих уголовно-правовых норм. Внесены предложения по совершенствованию некоторых положений Уголовного кодекса Российской Федерации с учётом положительного зарубежного законодательного опыта.

Ключевые слова: кибепреступления, блокчейн, криптовалюты, мошенничество, преступления против компьютерной информации, зарубежное законодательство, персональные данные.

Согласно позиции Управления ООН по наркотикам и преступности, успех международного сотрудничества в сфере борьбы с преступлениями, совершаемыми с использованием компьютерных технологий, зависит в том числе «от наличия унифицированных национальных законодательств в области борьбы с киберпреступностью, предусматривающих уголовную ответственность за совершение киберпреступлений» [1]. Значимость изучения зарубежного законодательства с целью выявления направлений рецепции наиболее удачных приёмов регламентации уголовно-правовых средств борьбы с киберпреступностью становится ещё более очевидной в рамках сравнительно-правового исследования уголовно-правовых мер борьбы с преступностью в сфере функционирования блокчейн и оборота криптовалют, ведь будучи непосредственно связанными с использованием информационных технологий такие преступления нередко совершаются группами преступников из разных стран в отношении физических и юридических лиц, относящихся к юрисдикции разных государств.

В процессе настоящего сравнительно-правового исследования уголовно-правовых мер борьбы с преступлениями, получившими распространение в названной сфере, необходимо было учесть несколько нюансов. Во-первых, несмотря на позицию многих отечественных и зарубежных исследователей, круг преступлений, совершаемых в сфере функционирования блокчейн, не ограничивается лишь хищениями криптовалют или приобретением с их помощью товаров, оборот которых ограничен, что обусловлено многофункциональностью названной технологии и её применимостью практически во всех значимых сферах жизни общества. Во-вторых, ввиду некой неопределённости позиции отечественного законодателя, данное исследование посвящено максимально широкому кругу вариантов рецепции наиболее удачных новелл зарубежного законодательства с учётом возможности изменения взглядов правотворца и государственных структур Российской Федерации на сущность криптовалют и функционал технологии блокчейн.

I. Уголовно-правовая охрана общественных отношений, возникающих в процессе осуществления профессиональной деятельности по предоставлению услуг в сфере оборота виртуальных валют. Согласно п.п. 9.1, 10 и 10.1 Закона Эстонии о предотвращении отмывания денег и финансирования терроризма от 26.10.2017 г. (в ред. от 23.11.2020 г.) (*Money Laundering and Terrorist Financing Prevention Act. Passed* 26.10.2017 г.; далее – Закон от 26.10.2017 г.),

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00823.

поставщиками услуг в сфере виртуальных валют признаются поставщики услуги виртуальных кошельков (1) и виртуальные биржи (2), то есть, соответственно, поставщики услуг, (1) в рамках которых создаются ключи для клиентов или хранятся зашифрованные ключи клиентов, которые можно использовать с целью хранения и передачи виртуальных валют, и (2) посредством оказания которых лицо обменивает виртуальную валюту на фиатную валюту, или фиатную валюту на виртуальную валюту, или виртуальную валюту на другую виртуальную валюту. Так как, согласно § 4 Закона об учреждениях, осуществляющих платёжные услуги и оборот электронных средств платежа, от 17.12.2009 г. (в ред. от 20.07.2020 г.) (*Payment Institutions and E-money Institutions Act. Passed* 17.12.2009 г.), такие услуги не относятся к платёжным, деятельность по выпуску и обороту виртуальных валют представляет собой разновидность предпринимательской (финансовой) деятельности, а поставщики соответствующих услуг на основании п. 5 § 2 Закона от 26.10.2017 г. приравниваются к финансовым учреждениям. Согласно § 70 Закона от 26.10.2017 г., поставщики услуг в сфере виртуальных валют обязаны получить разрешение на осуществление соответствующей хозяйственной деятельности. Приведённые выше законодательные положения позволяют сделать вывод о применимости § 372 УК Эстонии «Хозяйственная деятельность без лицензии и запрещенная хозяйственная деятельность» (*Penal Code. Passed* 06.06.2001 г.) для привлечения к уголовной ответственности тех лиц, которые осуществляют соответствующую предпринимательскую (финансовую) деятельность по выпуску и обороту виртуальных валют без регистрации и получения соответствующего разрешения. Примечателен тот факт, что осуществление незаконной предпринимательской деятельности, связанной с оказанием финансовых услуг, образует квалифицированный состав названного преступления.

Согласно российскому законодательству (как действующему, так ещё и не вступившему в законную силу), участники цифрового гражданского оборота, осуществляющие выпуск цифровых активов, их обмен и инвестирование с их помощью, подлежат регистрации Центральным банком Российской Федерации. В рамках первого из названных видов деятельности, согласно положениям ст. 5 Федерального закона от 31.07.2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», вступающего в силу 01.01.2021 г. (далее – ФЗ от 31.07.2020 г. № 259-ФЗ), речь идёт о включении Банком России юридических лиц в реестр операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов. В свою очередь, сделки с цифровыми финансовыми активами, включая их обмен друг на друга или иные цифровые права, осуществляются операторами обмена цифровых финансовых активов (кредитные организации, организации торговли, иные юридические лица), которые, согласно ст. 10 ФЗ от 31.07.2020 г. № 259-ФЗ, должны быть включены Банком России в реестр операторов обмена цифровых финансовых активов. Наконец, инвестирование путём цифровых финансовых активов, согласно ст.ст. 10 и 16 Федеральный закон от 02.08.2019 г. № 259-ФЗ (ред. от 20.07.2020 г.) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации», связано с необходимостью включения в реестр операторов инвестиционных платформ. В указанных выше случаях речь идёт о трёх группах крупных игроков виртуального рынка: 1) цифровые площадки для майнинга криптовалюты (в частности, облачного майнинга); 2) провайдеры криптокошельков и виртуальные биржи; 3) площадки *ICO* (первичное размещение монет или токенов) и децентрализованные автономные организации. Указанные субъекты являются посредниками в процессе оборота виртуальных валют и (или) владельцами ресурсов для осуществления такой деятельности.

От указанных выше субъектов необходимо отличать частных майнеров криптовалюты. Согласно ст. 2 ФЗ от 31.05.2020 г. № 259-ФЗ, выпуск цифровых финансовых активов вправе осуществлять физические лица, зарегистрированные в соответствии с Федеральным законом от 8 августа 2001 г. № 129-ФЗ (ред. от 31.07.2020 г.) «О государственной регистрации юридических лиц и индивидуальных предпринимателей» в качестве индивидуальных предпринимателей, а также юридические лица (коммерческие и некоммерческие организации).

В данном случае речь идёт о предпринимательской деятельности, но не связанной с финансовой: такие лица осуществляют за счёт собственных средств (электроэнергия, специальное оборудование, вычислительные мощности) имеющую рисковый характер (риск не добавить блок в цепь раньше других с учётом затрат на электроэнергию и техническую мощность, а также не окупить вложения денежных средств в необходимое оборудование) деятельность, направленную на систематическое извлечение прибыли и заключающуюся в решении сложных математических и криптографических алгоритмов с целью создания товара особого рода – виртуальной валюты [2, с. 132-134].

В 2017 г. Министерство внутренних дел Российской Федерации выпустило пресс-релиз о первом в нашей стране уголовном деле, возбуждённом по факту совершения преступления, предусмотренного ч. 2 ст. 172 УК РФ, в отношении группы злоумышленников, которые организовали виртуальный

сервис по обмену и переводу криптовалюты и путём использования 300 банковских карт через счета и учётные записи в сети «Интернет» незаконно обналичили более 500 млн руб. [3]. Впоследствии была осуществлена переквалификация действий виновных на ст. 171 УК РФ, и виновные были осуждены условно. К сожалению, указанные выше и подобные им правоприменительные решения вплоть до 1 января 2021 г., то есть до вступления в силу цитируемого выше ФЗ от 31.05.2020 г. № 259-ФЗ, вряд ли можно признать соответствующими уголовному закону, так как и в ст. 171, и в ст. 172 УК РФ речь идёт о предпринимательской деятельности без регистрации и (или) лицензии в тех случаях, когда соответствующие обязанности установлены законом, а все виды деятельности в сфере оборота криптовалют (за исключением, пожалуй, услуг провайдера инвестиционной платформы) до настоящего момента не урегулированы. Указанное, однако, не означает отсутствия необходимости совершенствования текстов ст.ст. 171 и 172 УК РФ.

Выделение уголовно-правовых средств защиты именно банковской деятельности в тексте самостоятельной нормы УК РФ объяснимо, так как, во-первых, эта деятельность связана с получением сверхприбыли, и во-вторых, речь идёт о возможности причинения весьма значительного ущерба гражданам и организациям в результате неквалифицированного предоставления соответствующих услуг предпринимателем, компетенция и профессионализм которого не были удостоверены получением соответствующей лицензии и прохождением процедуры регистрации. Впрочем, точно такие же риски связаны с осуществлением инвестиционной и иных видов финансовой деятельности, однако о них в ст. 172 УК РФ не упоминается. В условиях функционирования блокчейн и оборота виртуальных валют уровень общественной опасности осуществления названных выше разновидностей предпринимательской деятельности без регистрации значительно увеличивается в связи: 1) с предъявлением особых требований к участникам цифрового оборота (обязанность представлять дополнительную информацию относительно аутентификации пользователей, отслеживания недобросовестного поведения, дополнительная ответственность за утечку информации, возникновение технических сбоев), 2) с применением в процессе такой деятельности специальных знаний и навыков в области шифрования данных, программирования, 3) с чрезвычайно рисковым характером деятельности, вытекающим из беспрецедентной волатильности стоимости соответствующих цифровых активов, 4) с возможностью причинения ущерба или извлечения дохода в размере, в десятки раз превышающем определяемые с учётом примечания к ст. 170.2 УК РФ объёмы крупного и особо крупного ущерба или размеров дохода.

Кроме того, следует также задуматься о соответствии положений ст. 171 УК РФ современному уровню и темпу развития социально-экономических отношений и информационных технологий. Так, в результате уточнения процедуры технического осмотра транспортных средств в ст. 171 УК РФ были внесены изменения (Федеральный закон от 26.07.2019 г. № 207-ФЗ), однако развитие робототехники, Интернета вещей, индустрии компьютерных игр, внедрение технологий искусственного интеллекта, нейронных сетей и т.п. позволяют сделать вывод о том, что в скором времени законодательство Российской Федерации вновь может быть дополнено требованиями в области регистрации и лицензирования. Следовательно, текст ст. 171 УК РФ должен содержать абстрактные, приспособляемые к изменениям социально-экономических отношений термины.

II. Положения зарубежного законодательства в части регламентации уголовной ответственности за преступления, получившие распространение в сфере функционирования блокчейн с учётом многофункциональности названной технологии. Законодатели тех государств, которые предпринимают попытки регулирования сферы оборота криптовалют, обращают особое внимание на следующие аспекты данных финансовых активов: 1) они являются выражением стоимости, экономической ценности; 2) представлены исключительно в цифровой форме; 3) не являются законным платёжным средством; 4) могут признаваться платёжными средствами, но только в рамках соответствующих соглашений (договоров) между физическими или юридическими лицами (см., например: § 1 Закона ФРГ о банковской деятельности (*Gesetz über das Kreditwesen (Kreditwesengesetz – KWG*). *Ausfertigungsdatum:* 10.07.1961; *zuletzt geändert durch Art.* 4 *Abs.* 7 *G v.* 10.7.2020 I 1633; п. 1 и 4 § 2 Закона Финляндии о провайдерах виртуальной валюты от 26.04.2019 № 572 (26.4.2019/572 *Laki virtuaalivaluutan tarjoajista*)). Исходя из приведённых выше суждений и результатов исследования статей УК зарубежных государств об ответственности за имущественные и компьютерные преступления, можно сделать несколько выводов: 1) зарубежные законодатели признают возможность применения положений собственных уголовных законов для уголовно-правовой охраны имущественных интересов владельцев криптовалют, так как признают последние неким видом имущества, не имеющего материального выражения (не существует чёткого разграничения между предметами хищений и других преступлений в сфере экономики); 2) сущность предмета компьютерных преступлений тоже не конкретизирована, так как используются более абстрактные формулировки типа «системы обработки данных», «информационная система»,

«компьютерные программы или данные» вне зависимости от наличия статуса «охраняемой законом информации» (обычно указывается лишь то, что такая информация для виновного не предназначалась). Представляется, что указанные технико-юридические особенности позволяют не вносить постоянно изменения в статьи, содержащие признаки таких преступлений.

В уголовных законах некоторых государств содержатся нормы, подобные ст. 272 УК РФ, содержащие признаки составов компьютерных преступлений, сконструированных по типу материальных (например, § 303a УК ФРГ «Изменение данных» или § 126a УК Австрии «Повреждение данных»). Подобные преступления могут быть признаны оконченными только с момента наступления негативных последствий несанкционированного доступа в виде уничтожения, блокирования, модификации либо копирования компьютерной информации или причинения иного вреда. Между тем в особенности применительно к сфере оборота криптовалют и функционирования блокчейн следует помнить о значительной степени общественной опасности действий, которые непосредственно не связаны с удалением, блокированием, искажением или копированием информации, например, скрытый криптомайнинг [4, с. 30], фоновое отслеживание личной и финансовой информации потерпевшего и т.п. Установить признаки состава преступления, предусмотренного ст. 272 УК РФ, в подобных случаях не представляется возможным, что может способствовать уклонению от ответственности виновных лиц. Решение указанной проблемы видится в заимствовании идеи зарубежных законодателей конструировать составы преступлений в сфере компьютерной информации, связанных с несанкционированным доступом к данным, по типу формальных и даже усечённых. Так, § 118a УК Австрии «Незаконный доступ к компьютерной системе» (Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB)) предусмотрена уголовная ответственность за получение доступа к компьютерной системе либо к её части в результате преодоления определенных мер безопасности с намерением получить конфиденциальные сведения о личных данных для себя или другого неуполномоченного лица, а равно причинить вред другому человеку в результате использования данных, хранящихся в системе и не предназначенных для него. В свою очередь, согласно § 202a УК ФРГ (*Strafgesetzbuch* (*StGB*). *Ausfertigungsdatum:* 15.05.1871; *zuletzt geändert durch Art.* 1 *G v.* 9.10.2020 I 2075), признанное виновным в выведывании данных лицо подлежит уголовной ответственности за получение для себя или другого лица несанкционированного доступа к данным, которые специально защищены от такого доступа, путём преодоления систем защиты.

В ноябре 2019 г. в адрес президента Национального совета Швейцарии и его депутатов руководителем федерального министерства финансов У. Маурером и федеральным канцлером У. Турнхерром было направлено официальное письмо с предложениями по изменению федерального законодательства в связи с развитием технологии распределённого реестра (*Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom* 27. *November* 2019). Несмотря на то что Национальный банк Китайской Народной Республики последовательно проводил политику ограничения оборота виртуальных валют на территории Китая и даже обращал внимание, что «законная виртуальная валюта ещё не выпущена», другие виртуальные валюты «не могут и не должны использоваться в качестве валют в процессе обращения на рынке» и весьма часто используются в спекулятивных целях и в незаконной деятельности типа финансовых пирамид и мошенничества (金融知识普及补充材料 (2019) 专题一：人民币知识), задолго до пробного введения собственной виртуальной валюты в ключевых экономических регионах страны особое внимание названный финансовый регулятор уделял исследованиям в области блокчейн и даже становился участником нескольких проектов, основанных на указанной технологии (*BOCwallet, IBM HyperLedger Fabric* и другие). Подобное внимание государственных органов зарубежных стран к технологии блокчейн вполне объяснимо, так как она предоставляет широкие возможности для децентрализованного хранения данных и их защиты от постороннего вмешательства в различных сферах (банковское дело и финансовые операции, здравоохранение, логистика, хранение личных данных на государственных порталах и т.п.). В этой связи особый интерес представляют положения уголовно-правовых актов зарубежных государств, предусматривающие ответственность за разнообразные злоупотребления в сфере нарушения режима охраны информации.

Уголовная ответственность, в соответствии с § 119a УК Австрии, например, предусмотрена за получение доступа для себя или другого к непредназначенным для посторонних данным, передаваемым посредством компьютерной системы, или за опубликование в целях извлечения материальной выгоды для себя или другого лица. Согласно ст. 179*novies* УК Швейцарии, уголовной ответственности подлежит любое лицо, которое без разрешения получает в результате сбора данных личные данные или профили личности, которые являются особо конфиденциальными и не находятся в открытом доступе. Обращает на себя внимание тот факт, что, в отличие от ст. 137 УК РФ, подобные ей статьи зарубежных уголовных законов не связывают уголовно-правовую оценку соответствующих противо-

правных деяний с наличием фактов собирания или распространения сведений, с характером этих сведений (ст. 137 УК РФ: «сведения о частной жизни, составляющие личную или семейную тайну») и со сферой их распространения (ст. 137 УК РФ: «в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации»). С учётом чрезмерно конкретизированного текста ст. 137 УК РФ общественные отношения, обеспечивающие охрану не связанных с личной или семейной тайной персональных данных, в частности, при условии, если они были распространены в виртуальном пространстве (что, кстати, обусловливает повышение уровня общественной опасности соответствующих деяний), фактически лишены уголовно-правовой защиты.

С учётом приведённых выше рассуждений представляется возможным сформулировать следующие предложения по совершенствованию положений УК Российской Федерации (представлены редакции и тексты диспозиций соответствующих статей):

1) изложить название и текст ч. 1 ст. 172 УК РФ в следующей редакции: «Незаконная банковская, инвестиционная и иная финансовая деятельность. 1. Осуществление банковской, инвестиционной и иной финансовой деятельности (банковских, инвестиционных и иных финансовых операций) без регистрации или без специального разрешения (лицензии) в случаях, когда такое разрешение (лицензия) обязательно, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере»;

2) изложить ч. 1 ст. 171 УК РФ в следующей редакции: «Осуществление предпринимательской деятельности без регистрации или без лицензии либо без иного специального разрешения в случаях, когда такие лицензия или иной специальное разрешение обязательны, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере, за исключением случаев, предусмотренных статьей 171.3 настоящего Кодекса»;

3) сформулировать ст. 137.1 УК РФ «Нарушение неприкосновенности персональных данных» в следующей редакции:

«1. Незаконное получение доступа для себя или других лиц, собирание, распространение любым способом, сбыт, приобретение персональных данных другого человека;

2. Те же деяния, совершённые путём вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей;

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершённые лицом с использованием своего служебного положения;

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, повлекшие тяжкие последствия».

Литература:

1. Серия университетских модулей «Киберпреступность». Модуль 7: Международное сотрудничество в борьбе с киберпреступностью. Официальные механизмы международного сотрудничества // Управление ООН по наркотикам и преступности: официальный сайт. – URL: https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html (дата обращения: 20.11.2020).
2. Егорова М.А., Белицкая А.В. Майнинг криптовалюты в России и в мире: понятие и правовое регулирование // Вестник университета имени О.Е. Кутафина (МГЮА). – 2020. – № 4. – С. 129-136.
3. Костромские полицейские направили в суд уголовное дело в отношении злоумышленников, которые нелегально зарабатывали на обналичивании и продаже криптовалюты. – URL: https://xn--b1aew.xn--p1ai/news/item/11019155/ (дата обращения: 23.11.2020).
4. Печегин Д.А. К вопросу о правовом регулировании криптовалют в Германии // Журнал зарубежного законодательства и сравнительного правоведения. – 2019. – № 6. – С. 21-33.

Foreign Experience of Criminal Protection of the Sphere of Blockchain Functioning and Cryptocurrency Turnover

Mkrtchian S.M.
Volgograd State University

The article deals with the research of the foreign legislation regarding regulations of criminal liability for offences committed in the sphere of blockchain functioning and cryptocurrency turnover. The most successful techniques for formulation of respective criminal norms were determined. The amendments to the Criminal Code of the Russian Federation were suggested according to the positive foreign legislative experience.

Key words: cybercrimes, blockchain, cryptocurrencies, fraud, offences against computer information, foreign legislation, personal data.