Правовое обеспечение кибербезопасности оборота цифровых финансовых активов[1]

Алексей Сергеевич ПЕТРОВ,
аспирант кафедры информационного права и цифровых технологий Университета имени О.Е. Кутафина (МГЮА), юрист московского офиса коллегии адвокатов «Регионсервис»
aspetrov234@gmail.com
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Аннотация. *Ключевой особенностью цифровых финансовых активов и иных криптоактивов является то, что их оборот осуществляется в рамках информационной системы, основанной на технологии децентрализованного реестра. В связи с этим для целей стабильности и защиты прав инвесторов большое значение имеет обеспечение кибербезопасности такой системы. Целью настоящей статьи является изучение положений российского законодательства в области кибербезопасности информационных систем, посредством которых осуществляется оборот криптоактивов, и их сравнение с законодательством зарубежных стран, в первую очередь Франции и Мальты. Автор приходит к выводу, что существующее в России правовое регулирование носит общий характер, что препятствует становлению и развитию рынка цифровых финансовых активов в России. При этом неизбежно встает вопрос относительно детализации, в частности, насколько подробно законодательство должно устанавливать требования технологического характера. Представляется, что регулирование должно следовать принципу технологической нейтральности, т.е. устанавливать общие требования и цели, но не предусматривать использование какой-то конкретной технологии.*
Ключевые слова: *криптоактивы, цифровые финансовые активы, токены, биткоины, кибербезопасность, информационные системы, блокчейн, децентрализованный реестр, цифровые технологии, финансовые рынки.*

DOI: 10.17803/2311-5998.2022.92.4.151-157

ALEXEY S. PETROV,
postgraduate student of the Department of information law and digital technologies of the Kutafin Moscow State Law University (MSAL), lawyer of Moscow office of the Regionservice bar Association
aspetrov234@gmail.com
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Legal Regulation of Cybersecurity of the Circulation of Digital Financial Assets

Abstract. *The key feature of digital financial assets and other crypto assets is that their circulation is carried out within the framework of an information system based on decentralized ledger technology. In this regard, for the purposes of stability and protection of the rights of investors, ensuring the*

[1] Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030».

cybersecurity of such a system is of great importance. The purpose of this article is to study the provisions of Russian legislation in the field of cybersecurity of information systems through which the circulation of crypto assets is carried out, and their comparison with the legislation of foreign countries, primarily France and Malta. As a result, the author concludes that the existing legal regulation in Russia is of a general nature, which hinders the formation and development of the market for digital financial assets in Russia.In this case, the question inevitably arises regarding the specification of legal requirements. In particular, how detailed should the legislation establish technological requirements? It seems that regulation should follow the principle of technological neutrality, that is, establish general requirements and goals, but not provide for the use of any specific technology.
Keywords: *cryptoassets, digital financial assets, tokens, bitcoins, cybersecurity, information technologies, blockchain, distributed ledger, digital technologies, capital markets.*

Говоря о правовой природе криптоактивов вообще и цифровых финансовых активов в частности, необходимо отметить, что они в большинстве случаев не представляют собой новый объект гражданских прав. Исключением являются криптовалюты, функционал которых сводится в первую очередь к средству платежа или сбережения. Другие же виды активов (инвестиционные или утилитарные), токены по своей сути, удостоверяют собой уже известные правопорядку имущественные права (корпоративные, вещные, обязательственные).

Так, в соответствии с ч. 2 ст. 1 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[2] (далее — закон о ЦФА) цифровой финансовый актив может удостоверять следующие права:

— денежные требования;
— возможность осуществления прав по эмиссионным ценным бумагам;
— права участия в капитале непубличного акционерного общества;
— право требования передачи эмиссионных ценных бумаг.

Ключевой особенностью криптоактивов (токенов) является то, что их оборот осуществляется исключительно в рамках информационной системы, основанной на технологии блокчейн и децентрализованного реестра. Именно информационная система является тем самым цифровым пространством, в котором обязательственные и иные права трансформируются в цифровые и обращаются как самостоятельный объект, в то время как доступ к информационной системе создает условия для реализации цифровых прав, в том числе распоряжения ими[3].

По большему счету такая информационная система представляет собой базу данных о криптоактивах, их содержании и обладателях. Именно поэтому криптоактив часто отождествляют с записью в информационной системе. Так,

[2] СПС «КонсультантПлюс».

[3] *Одинцов С. В., Миронов Э. Ю.* Цифровизация имущественного оборота: доктринальные трактовки и законодательная практика // Современное право. 2020. № 11.

законодательство Сингапура определяет токен как «криптографически защищенное удостоверение прав владельца токена на получение выгоды или совершение определенных действий в отношении актива или имущества эмитента»[4].

Таким образом, ключевой элемент в обороте цифровых финансовых активов — информационная система. Соответственно, большое значение имеет устройство такой системы с точки зрения надежности и информационной безопасности хранящихся в ней данных. Поскольку цифровые финансовые активы существуют исключительно в виртуальной среде в форме записей, также можно говорить об обеспечении кибербезопасности соответствующих информационных систем.

На первый взгляд лежащие в основе такой информационной системы технологии распределенного реестра и блокчейна сами по себе обеспечивают достаточный уровень безопасности операций с криптоактивами и безопасности данных. Так, данные, хранящиеся в информационной системе, и операции с криптоактивами криптографически зашифрованы, а децентрализованный реестр создает существенные трудности для злоумышленников с точки зрения возможности внесения туда данных и проведения несанкционированных операций. Как отмечается в литературе, именно безопасность цифровых технологий становится ключевым фактором, обеспечивающим доверие к ним[5].

Однако случаи кибератак на информационные системы, связанные с оборотом криптоактивов (например, криптобиржи) встречаются. Так, с 2011 г. было зафиксировано более 30 успешных кибератак на криптовалютные биржи, в результате которых было похищено более 980 000 биткоинов общей стоимостью более 4 млрд долларов[6].

В связи с этим активное внедрение в финансовую систему цифровых финансовых активов должно сопровождаться обеспечением надлежащего уровня кибербезопасности, в том числе установления на законодательных и подзаконных уровнях специальных требований.

Будучи во многом рамочным законом, российский Федеральный закон о ЦФА не содержит конкретно выраженных требований к кибербезопасности. Так, ч. 1 ст. 6 Закона о ЦФА устанавливает следующие обязанности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, относящиеся к кибербезопасности:

1) обеспечение возможности восстановления доступа обладателя цифровых финансовых активов к записям информационной системы по требованию обладателя цифровых финансовых активов, если такой доступ был им утрачен;
2) обеспечение бесперебойности и непрерывности функционирования информационной системы, в том числе наличия и надлежащего функционирования дублирующих (резервных) технологических и операционных средств,

[4] *Basak S., Hui K. J., Tay V.* Initial coin offerings and capital market regulation: Singapore's perspective // I.C.C.L.R. 2019. 30 (10). P. 542.

[5] *Санникова Л. В., Харитонова Ю. С.* Цифровые активы: правовой анализ : монография. М. : 4 Принт, 2020. 304 с.

[6] *Yeo P.* Crypto-assets: regulators' dilemma // J.B.L. 2020. 4. P. 271.

обеспечивающих бесперебойное и непрерывное функционирование информационной системы;

3) обеспечение целостности и достоверности информации о цифровых финансовых активах, содержащейся в записях информационной системы;
4) обеспечение корректности реализации в информационной системе установленных оператором информационной системы алгоритма (алгоритмов) создания, хранения и обновления информации, содержащейся в распределенном реестре, и алгоритма (алгоритмов), обеспечивающих тождественность указанной информации во всех базах данных, составляющих распределенный реестр, а также невозможность внесения изменений в установленные оператором информационной системы алгоритм (алгоритмы) иными лицами — для информационных систем на основе распределенного реестра.

Закон о ЦФА содержит как технические, так и организационные требования к оператору информационной системы.

Предполагается, что конкретизация данных требований будет осуществляться на уровне актов Банка России, которые в настоящий момент не приняты. Такое положение дел, очевидно, не способствует возникновению и развитию отечественного рынка цифровых финансовых активов. Ведь четко сформулированные требования к кибербезопасности позволили бы не только обеспечить защиту прав и законных интересов потенциальных инвесторов, но и выступить в качестве ориентира для операторов соответствующих информационных систем с точки зрения организации их деятельности.

В связи с этим представляется полезным обратиться к зарубежному опыту. В настоящий момент наиболее подробное регулирование оборота криптоактивов установлено во Франции и на Мальте. На Мальте в 2018 г. был принят Закон о виртуальных финансовых активах (Virtual financial act).

Во Франции же правовое регулирование цифровых финансовых активов устанавливается в так называемом Плане действий по развитию бизнеса и трансформации (Action Plan for Business Growth and Transformation), внесшем поправки в валютно-финансовый кодекс[7]. Кроме того, контролирующие и уполномоченные органы приняли руководства в области обеспечения кибербезопасности — MSFA Guidance Noteson Cybersecurity и AMF Digital Assets Service Providers. Cybersecurity System of Requirements. Background Regulation, соответственно. Рассмотрим данные руководства подробнее.

В первую очередь и французское, и мальтийское руководство предъявляет определенные требования к организационной структуре оператора. В частности, каждый оператор информационной системы должен иметь директора по информационной безопасности, обладающего необходимой квалификацией и играющего ключевую роль в обеспечении информационной безопасности. По мальтийскому руководству в обязанности такого директора входят:

— общая интеграция системы кибербезопаности в деятельность организации;
— консультирование и оказание помощи руководству в разработке и реализации политики кибербезопасности;

[7] *Buttigieg C. P., Cuyle S.* A comparative analysis of EU homegrown crypto-asset regulatory frameworks // E. L. Rev. 2020. 45 (5). P. 645.

— разработка, реализация комплексной программы управления киберрисками;
— анализ и выявление рисков и угроз кибербезопасности, а также определение необходимых средств для обеспечения кибербезопасности;
— координация и взаимодействие с государственными органами и третьими лицами по вопросам киберзащиты;
— разработка методологии оценки состояния киберзащиты, подготовка соответствующих отчетов;
— разработка системы реагирования на киберинциденты;
— проведение учений по обеспечению кибербезопасности;
— руководство системой кибербезопасности;
— проведение оценки системы кибербезопасности.

Российский закон о ЦФА также устанавливает необходимость наличия у операторов службы внутреннего контроля и службы управления рисками, но не предусматривает отдельной службы или руководителя в области кибербезопасности.

Все операторы также должны иметь локальный нормативный правовой акт, закрепляющий основы политики организации в области кибербезопасности. Во многом аналогичное требование закреплено и в российском законе о ЦФА: оператор обязан утвердить правила информационной системы, содержащие требования к защите информации и операционной надежности. Помимо этого, мальтийское законодательство также требует от операторов утверждения таких документов, как план обеспечения непрерывности деятельности бизнеса (Business Continuity Plan) на случай кибератак и иных угроз и планы аварийного восстановления после инцидента (Disaster Recovery Plans).

Большое внимание также уделено превентивным мерам, направленным на выявление потенциальных угроз кибербезопасности, и постоянному мониторингу состояния информационной системы. В частности, любой инцидент, связанный с кибербезопасностью, подлежит детальному расследованию, отчет о котором направляется в контролирующие органы.

Что касается технических требований к информационным системам, то здесь мальтийский и французский контролирующие органы стремятся к политике так называемой технологической нейтральности. Это означает, что, закрепляя лишь общие определенные требования к информационной системе, законодатель оставляет за самими операторами выбор тех или иных технических решений и технологий[8]. Представляется, что такое решение, с одной стороны, обеспечивает гибкость в регулировании и не препятствует внедрению инноваций, а с другой стороны, предоставляет определенные гарантии участникам оборота цифровых финансовых активов. Как верно отмечается в литературе, современная правовая система не способна быстро реагировать на изменение цифровых технологий, поскольку они совершенствуются значительно быстрее[9].

При этом французское законодательство требует обязательной сертификации технологии распределенного реестра, если она разработана самим оператором

[8] *Houdrouge T.* Distributed ledgers: from the shadow to the light — the Swiss example // I.B.L.J. 2021. 2. P. 240

[9] *Минбалеев А. В.* Трансформация регулирования цифровых отношений // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 12. С. 32.

или же по его заказу. Такие технологии часто также называются проприетарным блокчейном[10].

Исходя из анализа мальтийских и французских руководств, можно выделить следующие требования технического характера:

— шифрование с помощью криптографии коммуникационных потоков, связанных с администрированием системы. При этом рекомендуется использовать уже хорошо себя зарекомендовавшие протоколы и алгоритмы шифрования;
— компоненты технической и сетевой инфраструктуры, обеспечивающие работу информационной системы должны быть идентифицированы, сертифицированы и надежны с точки зрения существующих и потенциальных рисков;
— наличие двухфакторной аутентификации для входа пользователей в информационную систему;
— резервирование данных, хранящихся в информационной системе;
— установление различных уровней допуска для сотрудников оператора к тем или иным элементам информационной системы;
— наличие технических систем, в режиме реального времени отслеживающих состояние информационной системы и выявляющих сбои в работе. Такие системы должны на постоянной основе тестироваться и обновляться.

Примечательно, что рассматриваемые нами руководства содержат отсылки к тем или иным документам, которые не являются нормативными правовыми актами, принятыми уполномоченными государственными органами. Так, во Франции при разработке информационных систем и политики кибербезопасности операторы обязаны принимать во внимание следующие руководства по кибербезопасности, принимаемые онлайн сообществом OWASP (Open Web Application Security Project):

— 10 генеральных рекомендаций OWASP по кибербезопасности (OWASPR);
— 10 текущих самых распространенных уязвимостей для веб-приложений и сайтов (OWASPW);
— 10 самых распространенных уязвимостей для мобильных приложений (OWASPM).

Предполагается, что контроль за безопасностью информационной системы операторы информационных систем в первую очередь будут осуществлять самостоятельно. Между тем интересное решение в области контроля за технической надежностью и безопасностью информационной системы предложено на Мальте. Там предусмотрен обязательный ежегодный технический аудит информационной системы, который проводится лицензированным и независимым аудитором.

Еще один пробел российского законодательства в сфере правового обеспечения информационной безопасности вытекает из того факта, что закон о ЦФА крайне узко определяет круг субъектов — участников отношений в сфере оборота цифровых финансовых активов.

Законом о ЦФА определен правовой статус только эмитентов, а также операторов информационных систем, в которых осуществляется выпуск и обмен цифровых финансовых активов. Между тем современный финансовый рынок

[10] *Lucchesi M.* Blockchain and financial law: which legal responses to a technological evolution that could transform the sector? // I.B.L.J. 2021. 2. P. 173.

характеризуется большим количеством посредников между инвестором и эмитентом. Не стали исключением и криптоактивы. В качестве таких посредников можно привести номинальных держателей, управляющих кошельками пользователей. Часто такие лица создают веб- или мобильные приложения, через которые осуществляется взаимодействие с клиентами. Поэтому мальтийское и французское законодательство также определяет правовой статус лиц, оказывающих услуги в данной сфере. Соответственно, и на них распространяются требования, связанные с кибербезопасностью.

БИБЛИОГРАФИЯ

1. *Минбалеев А. В.* Трансформация регулирования цифровых отношений // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — № 12. — С. 31—36.
2. *Одинцов С. В., Миронов Э. Ю.* Цифровизация имущественного оборота: доктринальные трактовки и законодательная практика // Современное право. — 2020. — № 11.
3. *Санникова Л. В., Харитонова Ю. С.* Цифровые активы: правовой анализ : монография. — М. : 4 Принт, 2020. — 304 с.
4. *Basak S., Hui K. J., Tay V.* Initial coin offerings and capital market regulation: Singapore's perspective // I.C.C.L.R. — 2019. — 30 (10). — P. 530—549.
5. *Buttigieg C. P., Cuyle S.* A Comparative analysis of EU homegrown crypto-asset regulatory frameworks // E. L. Rev. — 2020. — 45 (5). — P. 639—659.
6. *Houdrouge T.* Distributed ledgers: from the shadow to the light — the Swiss example // I.B.L.J. — 2021. — 2. — P. 227—239.
7. *Lucchesi M.* Blockchain and financial law: which legal responses to a technological evolution that could transform the sector? // I.B.L.J. — 2021. — 2. — P. 167—178.
8. *Yeo P.* Crypto-assets: regulators' dilemma // J.B.L. — 2020. — 4. — P. 265—286.