ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

М. А. БАЖИНА,

д-р юрид. наук, доц. кафедры предпринимательского права УрГЮУ имени В. Ф. Яковлева

Понятие критической информационной инфраструктуры было введено в действие ФЗ № 187-ФЗ от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – ФЗ о КИИ). Под этим термином понимаются объекты критической информационной инфраструктуры, а также электросвязи, используемые для организации взаимодействия таких объектов. В п. 7 ст. 2 ФЗ о КИИ раскрывается то, что понимается под объектами КИИ, а именно: информационные системы, информационно-коммуникационные сети, автоматизированные системы управления субъектов КИИ [1]. В соответствии с п. 3 ст. 2 ФЗ № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» информационными системами выступает совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационные технологии и технические средства. Иными словами, под информационной системой понимается какая-либо цифровая платформа, доступ к которой осуществляется с помощью средств вычислительной техники. Такого рода платформы используются в различных сферах экономической деятельности, что соответствует целям Паспорта национального проекта Национальной программы «Цифровая экономика Российской Федерации», утвержденного Протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию национальным проектам от 4 июня 2019 г. № 7. Так, 3 июня 2019 г. Распоряжением Правительства РФ № 1189-р была утверждена Концепция создания и функционирования национальной системы управления и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019–2021 годы. Такая федеральная государственная информационная система получила наименование «Единая информационная платформа национальной системы управления данными». Такая платформа является ярким примером того, как само государство для предоставления государственных и муниципальных услуг и осуществления своих функций использует платформенные решения. Еще одним примером введения платформенных решений в рамках осуществления государственных функций может служить создание платформы цифрового рубля. Соответствующие изменения, связанные с введением понятия «платформа

цифрового рубля», были внесены в ФЗ № 161-ФЗ от 27 июня 2011 г. «О национальной платежной системе». Так, под платформой цифрового рубля понимается также информационная система, посредством которой взаимодействуют Банк России как оператор данной платформы и ее пользователи в целях совершения операций с цифровыми рублями.

Государственные функции, связанные с контролем и надзором в разных сферах, также реализуются с помощью платформенных решений. Примером может явиться эксперимент по созданию, апробации, внедрению информационной системы «Национальная цифровая транспортно-логистическая платформа» для оформления перевозок грузов, утвержденная Постановлением Правительства от 3 июля 2024 г. № 908. Так, на территории Российской Федерации с 1 августа 2024 г. по 1 июня 2025 г. проводится. Иными словами, речь идет о создании национальной цифровой транспортно-логистической платформы – НЦТЛП. Разработка такой платформы является необходимым этапом не только в рамках реализации целей национального развития, заложенных в Указе Президента от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года», но и необходимости интеграции в международный рынок транспортно-логистических услуг. Аккумулирование информации о транспортных документах, оформляемых в рамках транспортной деятельности, позволит достичь заявленной в Транспортной стратегии РФ до 2030 г. с прогнозом на период до 2035 г., утвержденной Распоряжением Правительства РФ от 27 ноября 2023 г. № 3363-р, целей, а именно: обеспечение прозрачности транспортного документооборота.

При этом, платформы создаются и в коммерческой сфере. Так, в действующем законодательстве, посвященном правовому регулированию инвестиционных отношений с использованием инвестиционных цифровых платформ, а также отношений при выпуске, учете и обращении цифровых финансовых активов, также используются платформенные решения. Так, выпуск и обращение цифровых финансовых активов осуществляется в рамках информационной системы (ст. 2 ФЗ № 259-ФЗ от 31 июля 2020 г. «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ о ЦФА) [2]. В соответствии со ст. 8 ФЗ № 259-ФЗ от 2 августа 2019 г. «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» утилитарные цифровые права приобретаются, отчуждаются, в рамках инвестиционной платформы.

Приведенные выше примеры свидетельствуют об активном использовании платформенных решений во всех сферах жизнедеятельности общества и государства. В связи с этим наиболее актуальным встает вопрос об обеспечении безопасности цифровых платформ как разновидности объектов критической информационной инфраструктуры.

В этой связи 30 марта 2022 г. был издан Указ президента РФ № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». В развитие положений данного нормативного правового акта Постановлением Правительства РФ № 1478 от 22 августа 2022 г. были утверждены требования к программному обеспечению, в т.ч. в составе программно-аппаратных комплексов, используемых органами государственной власти.

Однако, данные меры распространяются именно на те платформы, которые используются для выполнения государственных функций. При этом, как указано выше, платформенные решения могут применяться и в коммерческой сфере. В этой связи могут возникать определенные сложности.

Во-первых, критическая информационная инфраструктура является легко уязвимой. Цифровая платформа, выступая элементом КИИ, может быть подвергнута несанкционированному доступу третьих лиц. Вмешательство третьих лиц в работу цифровых платформ влечет не просто сбой в системе, но возможность утечки информации, в т.ч. персональных данных. В связи с этим возникает вопрос о том, кто несет гражданско-правовую ответственность за неправомерные действия третьих лиц перед пользователями, которым причинен вред таким незаконным распространением информации. Исходя из сути отношений, которые возникают при использовании платформенных решений, пользователи платформ самостоятельно вносят данные. Оператор является лицом, которое осуществляет эксплуатацию информационной системы (цифровой платформы), в т.ч. по обработке информации, содержащейся в ее базах данных (п. 12. ст. 2 ФЗ № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»). Так, в ст. 6 ФЗ о ЦФА указывается в качестве обязанности оператора – обеспечение бесперебойного и непрерывного функционирования информационной системы, целостность и достоверность информации, содержащейся в записях информационной системы. На примере обязанностей оператора информационной системы можно сделать вывод о том, что это лицо обязано обеспечить именно техническую стабильность в работе платформы. При расширительном толковании этих положений можно было бы предположить, что он обязан обеспечить и саму безопасность функционирования платформы. Тем самым, в случае причинения вреда вследствие несанкционированного доступа

к платформе третьих лиц оператор может рассматриваться в качестве ответственного лица.

Во-вторых, функционирование цифровых платформ для коммерческих целей осуществляется по правилам, которые, как правило, устанавливаются самими операторами (за исключением случаев, когда в федеральном законодательстве прямо предусмотрены правила функционирования платформы). В этой части могут возникать определенные проблемы, связанные с «нестыковкой» программного обеспечения. Так, при взаимодействии контрагентов между собой документы могут оформляться в электронном виде. В этой связи формат таких документов не всегда может совпадать. Такие различия могут привести к невозможности оформления отношений с юридической точки зрения и отсутствию соблюдения требований к форме сделки. Исходя из этого, правильным представляется издание общих правил, указывающих требования к формату документа.

Исходя из вышеизложенного, внедрение и развитие критической информационной инфраструктуры становится крайне важным для современных общественных отношений. Однако отсутствие соответствующего правового регулирования является своего рода препятствием для эффективного развития общественных отношений с применением КИИ.

ЛИТЕРАТУРА

1. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: Федеральный Закон Российской Федерации № 187-ФЗ от 26 июля 2017 г. // КонсультантПлюс. – М., 2024.
2. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс]: Федеральный Закон № 259-ФЗ от 31 июля 2020 г. // КонсультантПлюс. – М., 2024.