Вестник РУДН. Серия: Юридические науки 2023 Т. 27. № 2. 500—521
RUDN JOURNAL OF LAW. ISSN 2313-2337 (print), ISSN 2408-9001 (online) http://journals.rudn.ru/law

ПРАВО И ЦИФРОВЫЕ ТЕХНОЛОГИИ

LAW AND DIGITAL TECHNOLOGY

https://doi.org/10.22363/2313-2337-2023-27-2-500-521
EDN: GPPYPM

Научная статья / Research Article

Правовое обеспечение развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры

А.Л. Белоусов

Финансовый университет при Правительстве Российской Федерации (Финуниверситет), *г. Москва, Российская Федерация*
✉andreybelousov@mail.ru

Аннотация. Необходимость адаптации регуляторных механизмов к активно развивающимся в настоящее время процессам цифровизации обуславливает актуальность темы исследования. При этом в условиях нарастающих киберугроз и все большей зависимости общественных отношений от информационно-телекоммуникационных технологий определенному переосмыслению в правовом аспекте подлежат направления развития законодательства, обеспечивающее стабильность и безопасность соответствующей инфраструктуры. Предмет исследования — правовое обеспечение развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры. Цель работы — определение ключевых направлений совершенствования правового регулирования в области функционирования и развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры. При проведении исследования использовались методы анализа, синтеза и сравнения, а также буквального и системного толкования норм действующего законодательства в области функционирования и развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры. В заключении сформулированы выводы относительно необходимости развития нормативного регулирования в данной сфере. Предложены конкретные направления изменения правового поля, обеспечивающее устойчивое развитие информационно-телекоммуникационной инфраструктуры в Российской Федерации.

Ключевые слова: информация, безопасность, критическая инфраструктура, регулирование, цифровизация, Интернет, персональные данные

Конфликт интересов: Автор заявляет об отсутствии конфликта интересов.

Информация о финансировании. Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве РФ.

Дата поступления в редакцию: 24 августа 2022 г.
Дата принятия к печати: 15 апреля 2023 г.

Для цитирования:

Белоусов А.Л. Правовое обеспечение развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры // RUDN Journal of Law. 2023. Т. 27. № 2. С. 500—521. https://doi.org/10.22363/2313-2337-2023-27-2-500-521

Legal support for the development of sustainable and secure information and telecommunications infrastructure

Andrey L. Belousov

Financial University under the Government of the Russian Federation (Financial University),
Moscow, Russian Federation
✉andreybelousov@mail.ru

Abstract. The relevance of the work is due to the need to adapt regulatory mechanisms to the actively developing digitalization processes. On the other hand, in the context of growing cyber threats and increasing dependence of public relations on information and telecommunications technologies, the directions for the development of legislation that ensure stability and security of the relevant infrastructure are subject to a certain rethinking in the legal aspect. The subject of the study is the legal support for the development of a sustainable and secure information and telecommunications infrastructure. The purpose of the work is to identify key areas for improving legal regulation in the field of functioning and development of sustainable and secure information and telecommunications infrastructure. The study applies methods of analysis, synthesis and comparison, as well as literal and systematic interpretation of the norms of the current legislation in the field of functioning and developing sustainable and secure information and telecommunications infrastructure. Finally, conclusions are formulated regarding the need for the development of legal regulation in this area. The research outlines the specific directions for changing the legal field, which ensure the sustainable development of information and telecommunications infrastructure in the Russian Federation.

Key words: information, security, critical infrastructure, regulation, digitalization, internet, personal data

Conflict of interest. The author declares no conflict of interest.

Funding information. The article was prepared based on the research financed from budgetary funds under the state assignment of the Financial University under the Government of the Russian Federation.

Article received 24th August 2022
Article accepted 15th April 2023

For citation:

Belousov, A.L. (2023) Legal support for the development of sustainable and secure information and telecommunications infrastructure. *RUDN Journal of Law.* 27 (2), 500—521. (in Russian). https://doi.org/10.22363/2313-2337-2023-27-2-500-521

Введение

Мотивация выбора общественных отношений в области правового обеспечения условий для развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры как объекта исследования заключается в том, что на

сегодняшний день активное развитие современных технологий также, как и обусловленные этим процессы цифровизации, являются значимым фактором повышения качества функционирования государственных институтов. Информационные и телекоммуникационные технологии уже давно представляют собой важнейший и неотъемлемый элемент систем управления как в экономическом секторе, так и в области государственного управления. В том числе это касается и сфер, напрямую завязанных на поддержание правопорядка в обществе и обеспечение обороны и безопасности государства.

Для целей настоящего исследования автор под термином «информационно-телекоммуникационная инфраструктура» рассматривает совокупность объектов информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, а также сетей электросвязи, обеспечивающих функционирование и развитие информационного пространства страны и средств информационного взаимодействия. Опираясь на позицию законодателя, нашедшую отражение в Постановлении Правительства от РФ от 26.06.2012 № 644, отметим, что в качестве составных компонентов информационно-телекоммуникационной инфраструктуры выступают информационные технологии, технические и программные средства, информационно-телекоммуникационные сети, предназначенные как непосредственно для целей реализации полномочий государственных органов, так и для обеспечения функционирования информационных систем[1].

В рамках обозначенной темы исследования в качестве отдельной категории рассмотрена критически важная информационная инфраструктура как ключевая составная часть информационно-телекоммуникационной инфраструктуры. Помимо этого, автором в работе предпринята попытка провести комплексный анализ вопросов обеспечения функционирования устойчивой и безопасной информационно-телекоммуникационной инфраструктуры в частности и информационного пространства в целом. В этой связи в исследовании также затрагивается проблематика регулирования интернет-пространства, вопросы обеспечения защиты персональных данных в информационном пространстве, а также перспективы развития правового поля в области информационной безопасности в целом.

Степень научной разработанности

Говоря о степени научной разработанности заявленной темы важно отметить, что в настоящее время имеется определенная наработанная теоретическая база в данной сфере. Можно выделить ряд ученых, которые в своих трудах затрагивают отдельные аспекты регулирования процессов формирования и развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры. Так, А.К. Жарова в своих работах делает акцент на проблематике правового обеспечения безопасности цифровых отношений (Zharova, 2019; Zharova, 2020). В свою очередь Т.А. Полякова обращается к вопросам становления научно-правовых подходов к развитию системы применения цифровых технологий в нормотворчестве, а также проблемам формирования системы международной информационной безопасности

[1] Постановление Правительства РФ от 26.06.2012 № 644 (ред. от 10.10.2020) «О федеральной государственной информационной системе учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов» // Собрание законодательства Российской Федерации, 2012, № 27, ст. 3753; 2013, № 5, ст. 402; 2013, № 48, ст. 6259).

(Polyakova & Shinkaretskaya, 2020; Polyakova & Troyan, 2022). Интерес также представляют исследования Г.Г. Шинкарецкой и А.Г. Берман, в рамках которых авторы делают акцент на противодействии правовыми инструментами кибератакам (Shinkaretskaya & Berman, 2022). Помимо этого в фокусе внимания авторов находятся и проблемы обеспечения национальной безопасности в условиях цифровизации (Shinkaretskaya & Berman, 2020).

А.Н. Савенков проводит исследование сущность киберпреступности в финансово-кредитной сфере и инструменты для ее противодействия в аспекте обеспечения глобальной безопасности (Savenkov, 2017). Также и сам автор настоящего исследования неоднократно обращался к вопросам построения современной цифровой экономики в аспекте решения стратегических задач развития государства в целом, и финансового сектора, в частности (Belousov & Levchuk, 2018). Имеет смысл отметить и зарубежные работы по заявленной проблематике (Sicari, Rizzardi & Grieco, 2015; Adelmeyer & Teuteberg, 2018; Buzdugan & Capatana, 2022; Dehling, Lins, & Sunyaev, 2019; Ghafir & Saleem et al, 2018; Leszczyna, 2019; Linkov & Kott, 2019).

Постановка проблемы

Внедрение новых цифровых решений, как в бизнес-процессы субъектов предпринимательских отношений, так и в работу государственных структур, несет в себе новые специфические риски и угрозы. В частности, речь идет о рисках либо утраты, либо нежелательного распространения конфиденциальной информации. Помимо этого можно говорить и об угрозах несанкционированного вмешательства в работу обеспечивающего оборудования и систем хранения и передачи данных. Так, получение доступа к управлению объектами критически важной информационной инфраструктуры посредством взлома информационных систем способно привести к тяжелейшим техногенным авариям и катастрофам. Нарушение работы государственных органов через вмешательство в их информационные сервисы третьих лиц несут в себе угрозы подрыва суверенитета и основ конституционного строя Российской Федерации. Поэтому в условиях цифровизации существенно возрастает роль и значение бесперебойного, устойчивого функционирования информационно-телекоммуникационной инфраструктуры и ее защита от внешних воздействий.

В этой связи задачей государства на современном этапе является становление и дальнейшее развитие устойчивой и безопасной отечественной информационно-телекоммуникационной инфраструктуры с адаптацией к изменяющимся условиям внешней среды. Для реализации подобной задачи особую роль приобретает отвечающие веяниям времени, полное и четко структурированное правовое поле. Именно в рамках правового регулирования формируется надежный фундамент, опираясь на который возможно создание условий для развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры в Российской Федерации.

Стратегические направления развития информационной безопасности

Реализация на практике новых цифровых решений, особенно в структурах государственного сектора, без формирования необходимой обеспечивающей безопасность инфраструктуры, увязанной на актуальное правовое регулирование, серьезно повышает риски возникновения реальных киберугроз.

В том числе для минимизации подобных угроз и повышения уровня информационной безопасности в конце 2016 года в рамках Указа Президента РФ была утверждена Доктрина информационной безопасности Российской Федерации[2] (далее — Доктрина). В ней, в частности, сформулирован четкий понятийный аппарат — даны определения информационной угрозе, информационной безопасности, национальным интересам в информационной сфере, силам, средствам и системе обеспечения информационной безопасности и т.д. Также в Доктрине на основе оценки текущего состояния информационной защищенности и имеющихся ключевых угроз в данной сфере представлены базовые векторы развития информационной безопасности Российской Федерации.

В мае 2017 г. Указом Президента РФ от 09.05.2017 № 203 правовое оформление получает Стратегия развития информационного общества в Российской Федерации на 2017—2030 гг. (далее — Стратегия). В п. 15 Стратегии содержится тезис о том, что «Повсеместное внедрение иностранных информационных и коммуникационных технологий, в том числе на объектах критической информационной инфраструктуры, усложняет решение задачи по обеспечению защиты интересов граждан и государства в информационной сфере. С использованием сети „Интернет“ все чаще совершаются компьютерные атаки на государственные и частные информационные ресурсы, на объекты критической информационной инфраструктуры»[3].

Также имеет смысл отметить п. 17 Стратегии, в котором обозначена проблема отсутствия работающих на практике международно-правовых механизмов, с помощью которых возможно должным образом обеспечить суверенное право государств как субъектов международного права на регулирование собственного информационного пространства. Это касается также и суверенитета в национальном сегменте сети «Интернет».

В рамках Стратегии формулируется четкий алгоритм действий, с помощью которого возможно обеспечение устойчивого функционирования информационной инфраструктуры Российской Федерации.

Во-первых, отмечается необходимость сформировать на практике единство государственного регулирования. При этом требуется обеспечить централизацию процессов мониторинга и управления работой информационной инфраструктуры. Причем осуществить это следует как на уровне информационных систем, так и в рамках функционирования центров обработки данных и сетей связи.

Во-вторых, предполагается реализовать планомерный переход к использованию инфраструктуры электронного правительства для представителей публичных органом власти.

В-третьих, декларируется идея внедрения в практическую плоскость российских криптоалгоритмов и средств шифрования в рамках электронного взаимодействия властных структур, как между собой, так и в их отношениях с частными субъектами.

В-четвертых, важнейшим положением всей Стратегии можно назвать предложение активизации работы по замене иностранного оборудования и программного

[2] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201612060002 (дата обращения: 20.10.2022).

[3] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201705100002 (дата обращения: 29.10.2022).

обеспечения соответствующими отечественными аналогами. Это же касается и подхода к применению электронной компонентной базы. В итоге это позволит повысить уровень технологической и производственной независимости государства в аспекте общей информационной безопасности.

В-пятых, речь идет в том числе о формировании комплексного подхода к защите всей информационной инфраструктуры государства, включая применение российских систем обнаружения и предотвращения киберугроз.

В-шестых, устанавливается вектор развития в отношении расширения использования инструментов предотвращения угроз, возникающих в связи с внедрением новых цифровых решений, посредством применения непрерывного мониторинга информационных систем.

Также в Стратегии закрепляется тезис о важности обеспечения справедливых условий ведения бизнеса для российских разработчиков программного обеспечения. При этом не раскрывается суть «справедливых» условий и что конкретно под этим следует понимать. Здесь стоит отметить, что для стимулирования ведения успешной и самое главное результативной по отношению к конечному продукту предпринимательской деятельности требуется активная поддержка со стороны государства. Особое значение это приобретает в настоящее время в условиях сложной для таких видов бизнеса, как IT-сфера экономической ситуации. Для предпринимателей, ведущих свою работу в области разработки и внедрения новых информационных технологий и программного обеспечения, важнейшее значение имеют следующие факторы:

1. Наличие подготовленных квалифицированных кадров. Здесь мы видим проблему, связанную с оттоком квалифицированных кадров. Это обуславливается как достаточно низким уровнем оплаты труда в сравнении с зарубежными работодателями, так и возможностью российских IT-специалистов в силу специфики самой деятельности работать удаленно на иностранные компании. Выход здесь может быть только один — повышение уровня оплаты труда для российских специалистов в области информационных технологий, работающих над разработкой отечественных IT-продуктов. Помимо этого, возможны и другие стимулирующие инструменты, способные оставить подобный интеллектуальный капитал в российской юрисдикции. Это могут быть и льготные ипотечные программы, и дополнительные налоговые льготы, и отсрочка от исполнения воинской обязанности и т.д. Также должны быть предложены широкие возможности и получения дополнительного образования, и проведения научных исследований, и повышение квалификации через прохождение стажировок, участия в конференциях и других современных площадках для обмена информацией.

2. С учетом венчурного характера большинства видов подобной предпринимательской деятельности значимое место стоит отвести инструментами грантовой поддержки со стороны государства, а также минимизации фискальной нагрузки на подобные сегменты бизнеса. Здесь возможно применение целого спектра фискальных льгот, включая налоговые каникулы, обеспечение доступа к «дешевым» кредитам посредством субсидирования процентных ставок, а также выставления государственных и муниципальных гарантий перед кредитными организациями.

3. Обеспечение государственного заказа на продукцию российских IT-компаний. Именно государство, выделяя значительные объемы финансовых ресурсов и используя прозрачную систему их распределения, должно стимулировать российских предпринимателей выбирать IT- индустрию как перспективный и доходный вид бизнеса.

Обеспечение безопасности критически важной инфраструктуры

Далее, важнейшим шагом на пути становления полноценного правового поля, обеспечивающего устойчивое и безопасное функционирование информационно-телекоммуникационной инфраструктуры, стало принятие в 2017 году Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — Закон о КИИ).

Статья 5 Закона о КИИ посвящена регулированию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. При этом под государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы понимается единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты[4].

Закон о КИИ стал важным шагом на пути формирования необходимого правового поля в области информационной безопасности. Однако спустя уже более пяти лет с момента принятия данного акта имеет смысл отметить отдельные моменты в его регуляторном воздействии, которые требуют устранения и корректировки. В частности, можно согласиться с мнением Э.В. Горян, которая отмечает отсутствие четких критериев отнесения к субъектам критической информационной инфраструктуры, что порождает, по словам автора, «замедление идентификации критических информационных систем и эффективность обеспечения ее безопасности» (Goryan, 2018).

Также в рамках формирования законодательства в области регулирования безопасности критической информационной инфраструктуры Федеральным законом от 26.07.2017 № 194-ФЗ в Уголовный кодекс Российской Федерации (далее — УК РФ) вводится ст. 274.1 УК РФ, предусматривающая уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации[5].

Уже в 2021 году на основании Федерального закона от 26.05.2021 № 141-ФЗ Кодекс Российской Федерации об административных правонарушениях (далее — КоАП РФ) дополняется нормами в рамках ст. 13.12.1. КоАП РФ, устанавливающими административную ответственность за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры[6]. При этом в целом в главе 13 КоАП РФ содержится обширный перечень составов

[4] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201707260023 (дата обращения: 20.10.2022).

[5] Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона „О безопасности критической информационной инфраструктуры Российской Федерации“». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201707260041 (дата обращения: 12.11.2022).

[6] Федеральный закон от 26.05.2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202105260038 (дата обращения: 12.11.2022).

административных правонарушений в области защиты информации и связи. Помимо этого обозначенный Закон внес дополнения, касающиеся информационной безопасности, и в другие главы КоАП РФ.

В развитие положений Закона о КИИ в начале 2018 г. принимаются Постановление Правительства РФ от 08.02.2018 № 127[7] и Постановление Правительства РФ от 17.02.2018 № 162[8], определяющие правила категорирования, перечень критериев значимости объектов критической информационной инфраструктуры, а также правила осуществления государственного контроля в данной области.

Также имеет смысл отметить утвержденные Постановлением от 29 сентября 2018 г. «Основные направления деятельности Правительства Российской Федерации на период до 2024 года» и, в частности, раздел 2 под названием «Цифровизация и научно-технологическое развитие». В данном разделе сформулирован тезис о том, что Правительством РФ будет реализован комплекс мер, направленных на создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры, а также обеспечение условий (в том числе разработка нормативно-правового регулирования) для широкого распространения цифровых технологий[9].

По итогам заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 г. утвержден паспорт национальной программы «Цифровая экономика Российской Федерации». В рамках данного документа одна из целей сформулирована как «создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших данных»[10].

В 2020 г. получает правовое оформления в рамках отдельного федерального закона идея объединения ключевых сведений о населении страны в единый общий регистр[11]. Запуск данного регистра в соответствии с Постановлением Правительства от 12.10.2021 № 1738 намечен на 2023 г.[12]

---

[7] Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 24.12.2021) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений. Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201802130006 (дата обращения: 12.11.2022).

[8] Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201802210006 (дата обращения: 22.11.2022).

[9] «Основные направления деятельности Правительства Российской Федерации на период до 2024 года» (утв. Правительством РФ 29.09.2018 № 8028п-П13).

[10] Паспорт национального проекта «Национальная программа „Цифровая экономика Российской Федерации“» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7).

[11] Федеральный закон от 08.06.2020 № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202006080019 (дата обращения: 12.11.2022).

[12] Постановление Правительства Российской Федерации от 12.10.2021 № 1738 «О сроках перехода субъектов Российской Федерации и муниципальных образований на использование сведений, содержащихся в едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации, в целях, определенных пунктом 3 части 2 статьи 4 Федерального закона «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации», на переходный период». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202110140029 (дата обращения: 11.12.2022).

Новый информационный источник, получивший название единый федеральный информационный регистр (далее — ЕРН), агрегирует в себе огромный массив сведений о населении, которые на сегодняшний день содержаться в множестве различных ведомств. В ЕРН, в частности, войдет информация о фамилии, имени, отчестве, дате и месте рождения физических лиц, их гражданстве, семейном положении, а также номер СНИЛС и ИНН. Полномочия по ведению ЕРН возлагаются на Федеральную налоговую службу (далее — ФНС), которая также обязана обеспечить безопасность и конфиденциальность данной информации. В отношении ЕРН важно отметить значимость защиты содержащейся в нем информации. Для этих целей предполагается тестирование на безопасность ЕРН в уполномоченных органах. Помимо этого на основании Постановления Правительства от 31.12.2020 № 2440 устанавливается применение усиленной квалифицированной электронной подписи при формировании и ведении ЕРН[13].

Обращает на себя внимание и Проект постановления «О государственной информационной системе «Типовое облачное решение системы электронного документооборота» (далее — Проект Постановления). В целом, задачей государственной информационной системы (далее — ГИС) является обеспечение функционирования электронного делопроизводства и электронного документооборота между публичными структурами.

В рамках данного Проекта Постановления четко прописываются полномочия оператора, в том числе и в области обеспечения информационной безопасности. Так, оператор обязан обеспечить соблюдение требований информационной безопасности, включая защиту данных, размещенных в государственной информационной системе.

Для обеспечения защиты информации в ходе создания, эксплуатации и развития государственной информационной системы осуществляются:

- формирование требований к защите информации, содержащейся в государственной информационной системе;
- применение сертифицированных по требованиям безопасности информации средств защиты информации;
- защита информации при ее передаче по информационно-телекоммуникационным сетям.

Также закрепляется положение о том, что ГИС должна опираться как на программно-технические средства, преимущественно российского производства, так и на их размещение на территории государства.

В соответствии с Проектом Постановления пользователи ГИС самостоятельно обеспечивают адаптацию автоматизированных рабочих мест, с которых происходит подключение к ГИС, и информационных систем, в состав которых входят указанные автоматизированные рабочие места, требованиям законодательства.

Распоряжением Правительства Российской Федерации от 20.02.2021 № 431-р с горизонтом планирования до 2025 г. утверждена Концепция цифровой и функциональной трансформации социальной сферы. Профильными субъектами здесь

[13] Постановление Правительства Российской Федерации от 31.12.2020 № 2440 «Об утверждении Правил использования усиленной квалифицированной электронной подписи при формировании и ведении единого федерального информационного регистра, содержащего сведения о населении Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202101090018. (дата обращения: 11.12.2022).

являются Министерство труда и социальной защиты Российской Федерации, Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации и федеральные учреждения медико-социальной экспертизы. В отношении них предполагается формирование соответствующей информационно-технической инфраструктуры с обязательным учетом необходимости максимизации использования российских импортозамещенных решений и постоянного повышения уровня информационной защищенности и обеспечения кибербезопасности[14]. Основой информационной инфраструктуры данных субъектов является единая цифровая платформа, для которой и должен быть разработан комплекс эффективных мер, направленных на защиту информации и повышение устойчивости работы всей системы.

Важное место в системе поддержания устойчивой и безопасной информационно-телекоммуникационной инфраструктуры в Российской Федерации занимает деятельность Федеральной службы по техническому и экспортному контролю (далее — ФСТЭК России). Одна из ключевых ее задач заключается в обеспечении безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, которые оказывают или могут оказать существенное влияние на безопасность государства в информационной среде.

ФСТЭК России в рамках своих полномочий выпускает различного рода документацию, направленную на регулирование функционирования ключевых систем информационной инфраструктуры. Так, ФСТЭК России 24 марта 2022 г. выпустило Информационное сообщение № 240/22/1549 «О мерах по повышению защищенности информационной инфраструктуры». В нем, в частности, содержится тезис о том, что в настоящее время в отношении объектов критической информационной инфраструктуры Российской Федерации зарубежными хакерскими группировками осуществляются масштабные компьютерные атаки.

В качестве примера можно привести статистику по количеству заведенных уголовных дел, напрямую связанных с кибератаками и воздействием на критически важную инфраструктуру. Так, в 2020 году таких дел было 22, в то время как в 2021 уже 70.

Особенности регулирования интернет-пространства

Достаточно резонансным стал принятый в середине 2021 г. Федеральный закон от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации». Под его новые требования попали иностранные IT-компании, работающие в российском сегменте сети «Интернет» и обладающие аудиторией более 500 тыс. человек в сутки. В соответствии с положениями данного закона такие организации с 2022 г. для возможности продолжения работы обязаны создавать свои филиалы, открывать представительство либо учреждать российские юридические лица, а также им необходимо зарегистрировать личный кабинет на сайте Роскомнадзора для взаимодействия с органами власти и установить на информационном ресурсе

[14] Распоряжение Правительства Российской Федерации от 20.02.2021 № 431-р. Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202103010045 (дата обращения: 11.12.2022).

рекомендованный счетчик посещаемости[15]. Как представляется, ключевой целью подобного шага со стороны законодателя является побуждение крупнейших зарубежных представителей IT-сферы к сотрудничеству с государством и соблюдению российских нормативных актов.

При этом важнейшим базовым актом в области использования информационных технологий и обеспечения защиты информации на сегодняшний день продолжает оставаться Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации).

Помимо названного выше Закона об информации стоит отметить и Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (далее — Закон о связи), также затрагивающей регулирование отношений в рассматриваемой сфере. Именно в эти два нормативных акта были внесены значимые и достаточно резонансные изменения Федеральным законом от 01.05.2019 № 90-ФЗ.

Данный закон на практике получил неофициальное название «Закон о суверенном Рунете». Его основной целью было формирование условий для стабильной работы российского сегмента сети Интернет в случае отказа в доступе к зарубежным корневым серверам и соответствующей маршрутной информации. В частности, с целью обеспечения условий для устойчивой работы сети Интернет в Российской Федерации и предотвращения угроз его «отключения» со стороны зарубежных государств или корпораций, на операторов возлагается обязанность передавать в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) определенные виды предусмотренной законом технической информации.

Также данным нормативным актом дополняется Закон о связи, в рамках которого начинает действовать гл. 7.1 «Обеспечение устойчивого, безопасного и целостного функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет».

В частности, был установлен порядок проведения учений в целях приобретения практических навыков по обеспечению устойчивого, безопасного и целостного функционирования Интернета на территории РФ.

Особо стоит отметить утверждение 29 декабря 2021 г. Правительством Российской Федерации Правил ведения перечня отечественных социально значимых информационных ресурсов (далее — Правила). Данными Правилами вводится четкий порядок ведения перечня отечественных социально значимых информационных ресурсов, при доступе к которым услуги связи по передаче данных и по предоставлению доступа к сети «Интернет» оказываются гражданам Российской Федерации без взимания платы. Помимо этого в Правилах закрепляются критерии отбора сайтов в сети «Интернет», информационных систем и программного обеспечения для их включения в данный перечень. Это имеет особую актуальность и значимость в условиях наличия реальных угроз внешнего воздействия на российскую информационную инфраструктуру.

[15] Федеральный закон от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202107010014 (дата обращения: 11.12.2022).

Защита персональных данных в информационном пространстве

Стоит сказать также о такой проблеме, как утечка персональных данных граждан. Опасность этого заключается в том, что доступ к таким персональным данным получают недобросовестные субъекты. В частности, в последние годы значительно выросло число преступлений, связанным с так называемым «телефонным» мошенничеством. Как правило, преступники опираются в том числе на купленные базы персональных данных. Сегодня нарушение правового поля в области персональных данных регулируется статьей 13.11 КоАП РФ. В рамках решения данного вопроса в мае 2022 г. в окончательном варианте был представлен Законопроект о внесении изменений в КоАП РФ в части усиления ответственности за утечки персональных данных граждан (далее — Законопроект). Так, в соответствии с Законопроектом для представителей бизнеса предусматривается штраф в размере 1 % от годового оборота за утечку персональных данных клиентов. А в случае, если имело место сокрытие распространения данных, предполагается увеличение размера штрафа до 3 % от оборота субъекта хозяйствования. Также на предпринимателей предполагается возложить обязанность в течение суток с момента утечки конфиденциальной информации уведомлять о ней Роскомнадзор. Помимо этого в течение 72 часов необходимо предоставить результаты расследования инцидента с указанием виновника.

6 июня 2022 г. законопроект был принят Госдумой в третьем чтении. Однако, как представляется, подобное ужесточение ответственности представителей бизнеса в условиях внешнего санкционного давления и объективных экономических проблем может негативным образом повлиять на финансовую устойчивость предпринимателей. В этой связи имеет смысл пересмотреть сформулированные в законопроекте положения. В частности, возможно предусмотреть наказание только за второй случай утечки информации — в виде фиксированного штрафа. А за третью и последующие — уже оборотный штраф. Еще одним инструментом борьбы с утечкой и неправомерным использованием персональных данных может стать институт аккредитации представителей бизнеса на предмет обеспечения информационной безопасности. В рамках данного механизма будет подтверждаться на соответствие принятые в организации меры по защите персональных данных.

Развитие правового поля в области информационной безопасности

В 2021 г. была обновлена Стратегия национальной безопасности России. В соответствии с Указом Президента Российской Федерации от 02.07.2021 г. № 400 утверждается Стратегия национальной безопасности Российской Федерации (далее — Стратегия), одной из отличительных черт которой является усиление акцентов именно на обеспечение информационной безопасности. В рамках Стратегии закрепляется важнейший на сегодняшний день тезис о том, что «информационное пространство выступает новой сферой ведения военных действий». В Стратегии указано, что «Российская Федерация также стремится к повышению эффективности многостороннего сотрудничества на важных для мирового сообщества направлениях, в числе которых международная информационная безопасность»[16].

[16] Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202107030001 (дата обращения: 11.12.2022)

Важным событием, связанным с программой импортозамещения в аспекте обеспечения информационной безопасности государства, можно назвать принятие в августе 2021 г. Постановления Правительства Российской Федерации от 28.08.2021 № 1432. В нем закрепляется запрет на проведение государственных закупок в отношении планшетов, ноутбуков, портативных компьютеров, серверов и интегральных микросхем, относящихся к категории импортных[17].

Правительством Российской Федерации 9 сентября 2021 г. была утверждена новая «дорожная карта» по развитию IT-отрасли. План мероприятий под названием «Создание дополнительных условий для развития отрасли информационных технологий» предусматривает среди прочего ввод в эксплуатацию трех сегментов киберполигона, предназначенного для обучения и тренировки широкого спектра различных субъектов, задействованных в противодействии киберугрозам[18]. Идея создания киберполигона была заложена в федеральном проекте «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»[19]. Сам по себе киберполигон представляет собой виртуальную копию инфраструктуры субъектов различных сфер. Наибольшая его востребованность имеет место для отраслей электроэнергетики, транспорта, связи и оборонно-промышленного комплекса. Использование киберполигона дает возможность в условиях, максимально приближенных к практике, отработать навыки по оперативному выявлению угроз и противодействию кибератакам.

Также имеет смысл отметить Распоряжение Правительства Российской Федерации от 22.10.2021 № 2998-р, утвердившем новую Концепцию цифровой трансформации государственного управления (далее — Концепция), в рамках которой четкий вектор развития придается идее цифровой перестройки государственного управления. Одной из задач подобной трансформации, согласно утвержденной Концепции, декларируется рост уровня надежности и безопасности информационных систем, а также обеспечение технологической независимости информационно-технологической инфраструктуры от зарубежного программного обеспечения и оборудования[20]. Помимо этого в Концепции формулируются ключевые стратегические риски, связанные с информационной безопасностью. Речь, в частности, идет об отсутствии должного правового регулирования, способного обеспечить автоматизированный сбор социально-экономических показателей, необходимых для принятия взвешенных и просчитанных управленческих решений. Также поднят вопрос о нехватке цифровых компетенций у большей части работников государственного аппарата и проблемах, связанных с переходом взаимодействия внутри государственных структур на электронный документооборот.

---

[17] Постановление Правительства Российской Федерации от 28.08.2021 № 1432 «О внесении изменений в некоторые акты Правительства Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202108310011 (дата обращения: 11.12.2022).

[18] План мероприятий («дорожная карта») «Создание дополнительных условий для развития отрасли информационных технологий» (утв. Правительством РФ 9 сентября 2021 г.). Режим доступа: http://www.garant.ru/hotlaw/federal/1484752/#review (дата обращения: 11.12.2022).

[19] Паспорт национального проекта "Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7).

[20] Распоряжение Правительства Российской Федерации от 22.10.2021 № 2998-р. Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202110260034 (дата обращения: 11.12.2022).

В конце 2021 года выходят в свет сразу несколько Распоряжений Правительства Российской Федерации, утвердившие Стратегические направления в области цифровой трансформации в сфере образования[21], здравоохранения[22], экологии и природопользования[23], в отраслях агропромышленного и рыбохозяйственного комплекса[24], обрабатывающих отраслях промышленности[25], а также транспортной[26] и строительной[27] отраслях. В каждом из этих актов, в большей или меньшей степени, прямо или косвенно, затрагиваются вопросы необходимости выстраивания работы по обеспечению информационной безопасности.

В начале 2022 года в соответствии с Указом Президента Российской Федерации от 17.01.2022 № 15 наряду с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации (далее — Минцифры РФ) полномочия в области определения политики в сфере информационной безопасности получает и Министерство обороны Российской Федерации (далее — Минобороны РФ)[28].

В марте 2022 года Постановлением Правительства РФ от 02.03.2022 № 279 создается государственная информационная система «Платформа «Центр хранения электронных документов» (далее — платформа). Оператором платформы выступает Минцифры РФ. Одной из ключевых функций платформы является защита информации от несанкционированного доступа, искажения, удаления или блокирования[29].

Также с марта 2022 г. на основании Постановления Правительства Российской Федерации от 28.12.2021 г. № 2518 вводится запрет для иностранных юридических лиц осуществлять отдельные виды деятельности в области информационной безопасности, если они отнесены к компетенции Федеральной службы безопасности России и Федеральной службы по техническому и экспортному контролю России[30].

---

[21] Распоряжение Правительства Российской Федерации от 02.12.2021 № 3427-р. Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202112070025 (дата обращения: 11.12.2022).

[22] Распоряжение Правительства Российской Федерации от 29.12.2021 № 3980-р (31.12.2021). Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202112310112 (дата обращения: 11.12.2022).

[23] Распоряжение Правительства Российской Федерации от 08.12.2021 № 3496-р. Режим доступа:http://publication.pravo.gov.ru/Document/View/0001202112140019 (дата обращения: 11.12.2022).

[24] Распоряжение Правительства Российской Федерации от 29.12.2021 № 3971-р (31.12.2021). Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202112310100 (дата обращения: 11.12.2022).

[25] Распоряжение Правительства Российской Федерации от 06.11.2021 № 3142-р. Режим доступа:http://publication.pravo.gov.ru/Document/View/0001202111090018 (дата обращения: 11.12.2022).

[26] Распоряжение Правительства Российской Федерации от 21.12.2021 № 3744-р. Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202112270030 (дата обращения: 11.12.2022).

[27] Распоряжение Правительства Российской Федерации от 27.12.2021 № 3883-р. Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202112290003 (дата обращения: 11.12.2022).

[28] Указ Президента Российской Федерации от 17.01.2022 № 15 «О внесении изменений в Положение о Министерстве обороны Российской Федерации, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1082, и Положение о Генеральном штабе Вооруженных Сил Российской Федерации, утвержденное Указом Президента Российской Федерации от 23 июля 2013 г. № 631. Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202201170005 (дата обращения: 11.12.2022).

[29] Постановление Правительства РФ от 02.03.2022 N 279 "О государственной информационной системе «Платформа «Центр хранения электронных документов». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202203030024 (дата обращения: 11.12.2022).

[30] Постановление Правительства Российской Федерации от 28.12.2021 № 2518 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам лицензирования отдельных видов деятельности и признании утратившим силу отдельного положения акта Правительства Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202112300215 (дата обращения: 20.12.2022).

В апреле 2022 г., в ответ на недружественные действия со стороны отдельных стран и групп государств, в целях обеспечения технологического суверенитета Российской Федерации в области устойчивости и развития КИИ, Указом Президента РФ от 14 апреля 2022 г. № 203 создается Межведомственная комиссия Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации. На комиссию, в частности, возложена функция по прогнозированию, выявлению и оценке внутренних и внешних угроз национальной безопасности в ряде сфер, связанных с развитием информационных технологий[31].

Таким образом, в рамках данного правового акта закрепляются принципы и алгоритмы принятия решений по вопросам создания безопасной и автономной отечественной информационной инфраструктуры как ответ на недружественные действия со стороны ряда зарубежных партнеров. В условиях реальных угроз обострения киберпротивостояния это становится действительно важным вопросом.

Также в апреле 2022 г. публикуется указ Президента Российской Федерации №166, посвященный вопросам приобретения и применения отечественных средств радиоэлектроники и программного обеспечения некоторыми структурами, отнесенными к субъектам КИИ[32].

Для поддержки и стимулирования развития российской IT-индустрии Постановлением Правительства Российской Федерации от 06.04.2022 г. № 598 увеличены размеры грантов, предоставляемых на поддержку проектов по разработке и внедрению отечественных решений в IT-сфере. В частности, закреплены минимальный (20 млн руб.) и максимальный (500 млн руб.) размеры гранта. Исключение здесь будут составлять особо значимые проекты, для которых максимальный размер гранта может составлять до 6 млрд руб. В том числе и для этих целей законодателем сформулировано понятие особо значимого проекта. Под ним следует понимать ключевые проекты, разработка которых направлена на устранение рисков и последствий ограничительных мер и обеспечение ускоренного развития отрасли информационных технологий.

Так же как одну из льгот можно рассматривать возможность увеличения сроков реализации проекта при предоставлении необходимых обоснований. Однако здесь действует ограничение на продление сроком не более чем на 6 месяцев. Помимо этого важной новацией можно считать снижение требований по софинансированию проекта за счет средств получателя гранта с 50 до 20 процентов[33].

Стоит отметить также и потенциальные изменения действующего правового регулирования становления устойчивой информационной инфраструктуры,

[31] Указ Президента РФ от 14 апреля 2022 г. № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202204140035 (дата обращения: 11.12.2022).

[32] Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202203300001 (дата обращения: 11.12.2022).

[33] Постановление Правительства Российской Федерации от 06.04.2022 г. № 598 «О внесении изменений в Правила предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий». Режим доступа: http://government.ru/docs/all/140306/ (дата обращения: 11.12.2022).

в результате которых предложения по реформированию, находящиеся в данный момент в статусе проектов, в ближайшей перспективе могут принять силу полноценных правовых актов. Так, ФСТЭК России опубликовала проект о внесении изменений в статью 16 Закона об информации. Основная суть изменений заключается в установление требований о защите информации, обладателями которой являются государственные органы, вне зависимости от места ее хранения или обработки[34].

Эти изменения направлены на решение проблемного вопроса, связанного с тем, что в настоящее время государственные органы поручают обработку информации, обладателями которой они являются, подведомственным организациям, коммерческим организациям, информационные системы которых не относятся к государственным. Вследствие этого имеет место снижение уровня защищенности информации, относящейся к государственным информационным ресурсам.

Кроме того, важно назвать еще один проект изменений Закона об информации, связанный с введением в правовое поле определения государственной единой облачной платформы (далее — «ГосОблако»)[35]. Легальное закрепление понятия «ГосОблако», как представляется, придаст импульс позитивным изменениям в регулировании защиты и доступности данных. Целью проекта «ГосОблако» является предоставление органам власти защищенной единой облачной платформы. В целом история создания проекта «ГосОблако» тянется еще с 2015 г., когда была представлена первая концепция единой облачной платформы для органов власти. При этом в 2019 г. эта концепция подверглась значительной доработке и переосмыслению.

Отметим Указ Президента Российской Федерации от 01.05.2022 г. № 250, которым устанавливается обязанность формирования в каждом ведомстве, учреждении и системообразующих организациях специального подразделения. Они призваны курировать вопросы оперативного обнаружения, предупреждения и ликвидации угроз информационной безопасности[36]. Как представляется, данный нормативный акт является одним из регуляторных инструментов достижения базовой цели в вопросе обеспечения технологического суверенитета государства. Далее в рамках исполнения этого Указа Президента исполнительные органы власти федерального уровня формируют конкретные требования к управленцам высшего звена, ответственным за кибербезопасность в государственных органах и корпорациях.

Распоряжением Правительства РФ от 22.06.2022 № 1661-р утвержден список организаций, которым обязаны провести аудит защищенности на предмет обеспечения должной информационной безопасности[37]. Субъектам, перечисленным в указанном распоряжении, необходимо реализовать комплекс мероприятий по оценке уровня защищенности своих информационных систем с привлечением организаций,

[34] Проект о внесении изменений в статью 16 Федерального закона об информации, информационных технологиях и о защите информации: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=120094

[35] Проект Федерального закона «О внесении изменений в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Режим доступа: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=122604 (дата обращения: 11.12.2022).

[36] Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Режим доступа: http://www.kremlin.ru/acts/bank/47796 (дата обращения: 11.12.2022).

[37] Распоряжение Правительства РФ от 22.06.2022 № 1661-р «Об утверждении перечня ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202206240033 (дата обращения: 11.12.2022).

имеющих лицензии ФСБ России и ФСТЭК России. Предполагается, что результаты аудита будут влиять на принятие решений при дальнейшей разработке мер по обеспечению безопасности информационных ресурсов государства.

Отдельно стоит сказать и о необходимости развития нормативной базы в области отношений, связанных с созданием и использованием распределенного реестра, который также может рассматриваться как элемент критически важной информационной инфраструктуры. С одной стороны, бизнес очень восприимчив к подобного рода технологиям, и в первую очередь предприниматели являются драйвером для развития более широкого использования блокчейна (Belousov & Shustrov, 2022). Вместе с тем важна четко сформулированная позиция государства по вопросу подхода к криптовалютам, а также детальное регулирование отношений в области блокчейн-технологий. Здесь имеет смысл ориентироваться уже на накопленный зарубежный опыт (Tvaronavičienė, Plėta, Casa & Latvys, 2020). Так, во многих государствах на протяжении длительного периода идут дискуссии относительно перспектив рассмотрения биткоина в качестве стандартной валюты (Ciaian, Rajcaniova & d'Artis, 2018). В большинстве теоретических исследований европейских и американских ученых прослеживается четкий тезис относительно приравнивания криптовалюты к категории «другое имущество» и рассматривать ее как полноценный актив (Vandezande, 2017).

Заключение

В области обеспечения условий для развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры уже сформировано обширное правовое поле, которое продолжает дополняться необходимыми регуляторными инструментами.

Вместе с тем в условиях жесткого санкционного давления, которое также сопровождается хакерскими атаками и попытками нарушения целостности критически важной информационной инфраструктуры, имеет место уязвимость отечественной информационно-телекоммуникационной цифровой системы. На это накладывается сохраняющаяся зависимость отечественной информационной инфраструктуры от иностранного программного обеспечения (далее — ПО), которое в значительной степени принадлежит правообладателям, зарегистрированным в юрисдикциях недружественных государств.

Помимо этого имеет место объективный дефицит кадров и слабый уровень подготовки российских IT-специалистов. Усугубляет данную проблему тенденция оттока квалифицированных работников в этой сфере заграницу.

Важно также отметить, что наибольшую уязвимость в плане обеспечения безопасности данных и обеспечения устойчивой работы на сегодняшний день имеют информационные системы государственных и муниципальных органов. Это обуславливается в том числе значительным несовершенством закупочных процедур, которые не имеют адаптации под специфику IT-отрасли. Отсутствие гибкости и строгий формализм не позволяют оперативно реагировать на появляющиеся угрозы как в плане приобретения средств защиты, так и в плане привлечения необходимых компетентных в подобных вопросах специалистов.

В настоящее время для решения обозначенных проблем и качественного роста уровня устойчивости и безопасности информационно-телекоммуникационной

инфраструктуры требуется переосмысление существующих подходов к информационной безопасности государства, сопровождаемых изменениями в законодательстве, которые должны быть направленны на адаптацию правового поля в данной сфере под новые условия внешней среды.

Представляется оправданным и необходимым обеспечить качественное развитие российской информационной инфраструктуры, подпадающей под критерии критически важной. Для этого необходимы точечные изменения законодательства уже сейчас с выработкой в ближайшем будущем новой единой концепции, которая станет прообразом и основой для формирования нового, цельного правового института безопасной информационно-телекоммуникационной инфраструктуры. При этом реформирование правового регулирования в данной области отношений должно основываться на сценариях развития информационных технологий на среднесрочную и долгосрочную перспективы с выделением наиболее вероятных ситуационных моделей, в рамках которых специалисты способны определить уязвимые элементы системы, требующие особой защиты и внимания.

Проведя комплексную аналитическую работу по оценке состояния правового регулирования создания условий для развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры в Российской Федерации, можно прийти к определенным промежуточным *выводам*.

Во-первых, на сегодняшний день имеет место значительное число рекомендательных актов от отдельных уполномоченных органов. С одной стороны, рекомендательный характер подобных актов позволяет подвластным субъектам иметь большую гибкость в принятии решений по вопросам обеспечения устойчивости и безопасности функционирования информационно-телекоммуникационной инфраструктуры, в том числе и относящейся к категории КИИ. Также у исполняющих субъектов появляется возможность выбора направлений развития информационно-телекоммуникационной инфраструктуры с учетом специфики той или иной отрасли. Однако, с другой стороны, для обеспечения комплексного характера защиты российской информационно-телекоммуникационной инфраструктуры необходима унификация требований и стандартов. И здесь имеет смысл говорить о том, что наиболее целесообразным как раз видится подход к установлению однородных требований к используемому оборудованию и программному обеспечению для поддержания стабильности и устойчивости функционирования отечественной информационно-телекоммуникационной инфраструктуры.

Во-вторых, фрагментарное регулирование вопросов развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры не способствует выстраиванию оптимальной правоприменительной практики, которая позволит в полной мере достичь желаемых целей. Имеет определенный смысл объединить имеющееся правовое обеспечение под эгидой отдельного единого нормативно-правового акта. Он может стать основой правового института регулирования информационно-телекоммуникационной инфраструктуры и будет являться хорошей базой для обеспечения развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры в Российской Федерации.

На основе проведенного аудита состояния регуляторного воздействия на условия, необходимые для развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры, а также сформулированных на базе этого выводов, можно вынести обоснованные *предложения по изменению правового регулирования*

создания условий для развития устойчивой и безопасной информационно-телекоммуникационной инфраструктуры:

1. Обеспечение благоприятных условий для доступа к инструментам грантовой и кредитной поддержки в отношении ИТ-компаний, которые занимаются разработкой российского ПО.

- Закрепить в рамках нормативно-правового акта понятие «Значимый российский ИТ-проект» и его критерии. Ключевым критерием должно выступать отсутствие российского аналога.
- Нормативно определить ключевые направления грантового финансирования, взяв за основу критерий отсутствия российских аналогов.
- Упрощение процедуры подачи заявок на гранты для ИТ-компаний, которые занимаются разработкой российского ПО и подпадают под критерий значимого российского ИТ-проекта. В частности, в отношении пользовательских продуктов и платформ возможно проводить предварительный отбор заявок через механизм публичного питчинга (публичной защиты проекта).
- Закрепление для значимого российского ИТ-проекта модели субсидирования, при которой от 75 до 90 % расходов будет брать на себя государство.
- Законодательно закрепить возможность для ИТ-компаний, которые занимаются разработкой российского ПО и подпадают под критерий значимого российского ИТ-проекта, предоставлять в качестве обеспечения под привлекаемое заемное финансирование нематериальный залог.

2. Изменение подходов к бюджетному финансированию в целях формирования запроса на проведение фундаментальных прикладных и поисковых научных исследований в области криптографии и защиты информационных ресурсов.

3. Повышение уровня защищенности государственных информационных систем и ресурсов. Ключевое направление изменений правового поля — законодательное закрепление критерия в виде показателя: «минимальная доля в стоимости закупаемого и (или) арендуемого органами власти различных уровней российского программного обеспечения».

4. Внесение изменений в регулирование подходов к выстраиванию образовательной деятельности и формированию образовательных стандартов в сфере среднего специального и высшего образования, направленных на решение проблемы, связанной с низким уровнем кадрового обеспечения функционирования устойчивой и безопасной информационно-телекоммуникационной инфраструктуры.

В частности, предлагаются следующее направление по изменению правового регулирования в рамках данной проблематики: формирование перечня средних специальных и высших заведений, охватывающих в совокупности не менее 60 % субъектов Российской Федерации. Внедрение в данных учебных заведениях программ целевого набора по предметным областям «Математика», «Информатика», «Информационная безопасность», «Криптография» и «Технология» на следующих условиях:

- оплата обучения за счет средств федерального бюджета;
- на пятилетний срок по окончании обучения гарантированное предоставление рабочего места с заработной платой не ниже, чем 1,2 средней заработной платы по субъекту Федерации для лиц, получивших среднее специальное образование, и не ниже, чем 1,6 средней заработной платы по субъекту Федерации для лиц, получивших высшее образование.

- на пятилетний срок по окончании обучения, в случае трудоустройства по полученной специальности в российские организации, предоставление отсрочки от прохождения обязательной воинской службы.

Помимо этого представляется оправданным решение следующих вопросов:

- обеспечение объективной оценки стратегических рисков в области информационной безопасности;
- анализ информационной инфраструктуры на предмет уязвимости и нарушения штатного режима работы;
- оценка эффективности используемых средств защиты информации и программных продуктов;
- подготовка программы пошаговой модернизации информационной инфраструктуры в аспекте минимизации рисков нарушения устойчивости и безопасности функционирования информационно-телекоммуникационной инфраструктуры.

5. Усиление ответственности за нарушение норм, регламентирующих вопросы обеспечения функционирования информационно-телекоммуникационной инфраструктуры. В частности, как представляется, назрела объективная необходимость пересмотра отдельных положений гл. 28 УК РФ. Так, по мнению автора, имеет смысл ужесточить наказание за деяния, предусмотренные ч. 1 и ч. 2 ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Также стоит обращать внимание на сохранение и развитие инфраструктуры традиционных услуг связи. К ним можно отнести классическую почтовую связь и электросвязь, которые в случае нарушения целостности и устойчивости работы российского цифрового информационного пространства могут стать временной надежной альтернативой для бесперебойной работы государственного аппарата, нормального, полноценного функционирования хозяйствующих субъектов и систем обеспечения обороноспособности и безопасности. Особую актуальность эти вопросы приобретают в настоящее время в условиях беспрецедентного санкционного давления, оказывающего влияние в том числе и на устойчивость функционирования элементов критически важной информационной инфраструктуры.

References / Список литературы

Adelmeyer, M., & Teuteberg, F. (2018) Cloud computing adoption in critical infrastructures — status quo and elements of a research agenda. In: *MKWI 2018 Proceedings*. Germany, Lüneburg. pp. 1345—1356.

Belousov, A.L. & Levchuk, E.Yu. (2018) Digitalization of the banking sector. *Finance and credit*. 24(2), 455—464. https://doi.org/10.24891/fc.24.2.455 (in Russian).
Белоусов А.Л., Левчук Е.Ю. Диджитализация банковского сектора // Финансы и кредит. 2018. Т. 24. № 2. С. 455—464. https://doi.org/10.24891/fc.24.2.455

Belousov, A.L. & Shustrov, A.A. (2022) Opportunities of using the blockchain technology in the insurance industry. *Digest Finance*. 27(1), 89—107. https://doi.org/10.24891/fc.25.1.196 (in Russian).
Белоусов А.Л., *Шустров А.А.* Возможности применения технологии блокчейн в сфере страхования // Дайджест-финансы. 2022. Т. 27. № 1. С. 89—107. https://doi.org/10.24891/fc.25.1.196

Buzdugan, A. & Capatana, G. (2022) Cyber security maturity model for critical infrastructures. In: Ciurea, C., Boja, C., Pocatilu, P. & Doinea, M. (eds.) *Education, Research and Business*

Technologies. Smart Innovation, Systems and Technologies. Vol. 276. Springer, Singapore. pp. 225—236. https://doi.org/10.1007/978-981-16-8866-9_19.

Ciaian, P., Rajcaniova, M. & d'Artis, K. (2018) Virtual relationships: Short- and long-run evidence from BitCoin and altcoin markets. *Journal of International Finansicial Markets, Institutions & Money*. (52), 173—195.

Dehling, T., Lins, S. & Sunyaev, A. (2019) Security of critical information infrastructures. In: Reuter, C. (ed.) *Information Technology for Peace and Security*. Springer Vieweg, Wiesbaden. pp. 319—339. https://doi.org/10.1007/978-3-658-25652-4_15

Goryan, E.V. (2018) Institutional mechanisms for ensuring the security of the critical information infrastructure of the Russian Federation and Singapore: a comparative legal aspect. *Administrative and municipal law*. (9), 49—60. https://doi.org/10.7256/2454-0595.2018.9.27762 (in Russian).

Горян Э.В. Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект // Административное и муниципальное право. 2018. № 9. С. 49—60. https://doi.org/10.7256/2454-0595.2018.9.27762

Ghafir, I., & Saleem, J. et al. (2018) Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*. (74), 4986—5002. https://doi.org/10.1007/s11227-018-2337-2

Leszczyna, R (2019) Cybersecurity controls. In: *Cybersecurity in the electricity sector*. Springer, Cham. pp. 181—209. https://doi.org/10.1007/978-3-030-19538-0_7

Linkov, I. & Kott, A. (eds.). (2019) Fundamental concepts of cyber resilience: introduction and overview. In: *Cyber resilience of systems and networks. Risk, systems and decisions*. Springer, Cham. pp. 1—25.https://doi.org/10.1007/978-3-319-77492-3_1.

Polyakova, T.A. & Shinkaretskaya, G.G. (2020) Issues of formation of the international information security system in the context of transformation of law and new challenges and threats. *Law and State: Theory and Practice*. 10(190), 138—142. https://doi.org/10.47643/1815-1337_2020_10_138 (in Russian).

Полякова Т.А., Шинкарецкая Г.Г. Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз // Право и государство: теория и практика. 2020. № 10(190). С. 138—142. https://doi.org/10.47643/1815-1337_2020_10_138

Polyakova, T.A. & Troyan, N.A. (2022) Formation of scientific and legal approaches to the development of a system for the use of digital technologies in rule-making. *Legal policy and legal life*. (1), 43—58. https://doi.org/10.24412/1608-8794-2022-1-43-58 (in Russian).

Полякова Т.А., Троян Н.А. Формирование научно-правовых подходов к развитию системы применения цифровых технологий в нормотворчестве // Правовая политика и правовая жизнь. 2022. № 1. С. 43—58. https://doi.org/10.24412/1608-8794-2022-1-43-58

Savenkov, A.N. (2017) Counteracting cybercrime in the financial and credit sphere as a vector for ensuring global security. *State and Law*. (10), 5—8. (in Russian).

Савенков А.Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 5—8.

Shinkaretskaya, G.G. & Berman, A.M. (2020) Digitalization and the problem of ensuring national security. *Education and Law*. (5), 254—260. https://doi.org/10.24411/2076-1503-2020-10544 (in Russian).

Шинкарецкая Г.Г., Берман А.М. Цифровизация и проблема обеспечения национальной безопасности // Образование и право. 2020. № 5. С. 254—260. https://doi.org/10.24411/2076-1503-2020-10544

Shinkaretskaya, G.G. & Berman, A.M. (2022) Cyberattacks — the illegal use of digital technologies. International Law. (1), 40—50. https://doi.org/10.25136/2644-5514.2022.1.37271 (in Russian).

Шинкарецкая Г.Г., Берман А.М. Кибератаки — противоправное использование цифровых технологий // Международное право. 2022. № 1. С. 40—50. https://doi.org/10.25136/2644-5514.2022.1.37271

Sicari, S., Rizzardi, A. & Grieco, L.A. (2015) Coen — Porisini A. Security, privacy and trust in Internet of things: the road ahead. *Computer Networks.* (76), 146—164.

Tvaronavičienė, M., Plėta, T., Casa, S.D. & Latvys, J. (2020) Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development.* 2(4), 802—813. https://doi.org/10.9770/IRD.2020.2.4(6)

Vandezande, N. (2017) Virtual currencies under EU anti — money laundering law. *Computer law & Security review*. (33), 341—353.

Zharova, A.K. (2019) Legal support of information security in "smart cities". *Lawyer*. (12), 69—76. https://doi.org/10.18572/1812-3929-2019-12-69-76 (in Russian).
Жарова А.К. Правовое обеспечение информационной безопасности в «умных городах» // Юрист. 2019. № 12. С. 69—76. https://doi.org/10.18572/1812-3929-2019-12-69-76

Zharova, A.K. (2020) Issues of ensuring the security of a person's digital profile. *Lawyer*. (3), 55—61. https://doi.org/10.18572/1812-3929-2020-3-55-61 (in Russian).
Жарова А.К. Вопросы обеспечения безопасности цифрового профиля человека // Юрист. 2020. № 3. С. 55—61. https://doi.org/10.18572/1812-3929-2020-3-55-61

Сведения об авторе:

Белоусов Андрей Леонидович — кандидат экономических наук, доцент департамента правового регулирования экономической деятельности, Финансовый университет при Правительстве Российской Федерации; Российская Федерация, 125167, г. Москва, Ленинградский пр-т, д. 49

ORCID ID: 0000-0002-9069-8830; ResearcherID: L-2766-2018; SPIN-код: 3633-3515

e-mail: andreybelousov@mail.ru
albelousov@fa.ru

About the author:

Andrey L. Belousov — Candidate of Economic Sciences, Associate Professor of the Department of Legal Regulation of Economic Activities, Financial University under the Government of the Russian Federation; 49 Leningradsky prospect, Moscow, 125167, Russia Federation

ORCID ID: 0000-0002-9069-8830; ResearcherID: L-2766-2018; SPIN-code: 3633-3515

e-mail: andreybelousov@mail.ru
albelousov@fa.ru