

Научная статья
УДК/UDC 349
DOI: 10.21779/2224-0241-2024-52-4-157-165

Обеспечение национального суверенитета России в условиях развития наукоемких технологий: противодействие вызовам праву и угрозам информационной безопасности

Т.А. Полякова

Институт государства и права РАН, г. Москва, Российская Федерация, polyakova_ta@mail.ru

Аннотация. В статье рассматриваются вопросы, связанные с реализацией задач обеспечения научно-технологического развития Российской Федерации в условиях цифровой трансформации и правовые проблемы в рассматриваемой сфере. На основе анализа стратегических задач, стоящих перед Российской Федерацией, направленных на обеспечение технологического, цифрового, информационного, культурного суверенитета с позиции информационного права, рассматриваются новые задачи национального развития России до 2030 г. и перспективы до 2036 г., в том числе в рассматриваемой области.

Исследование позволило акцентировать внимание на проблемах правового обеспечения противодействия новым вызовам и угрозам информационной безопасности, ландшафт которых расширяется в связи с процессами цифровизации, реализации политики обеспечения национального суверенитета на основе достижения импортозамещения информационных (цифровых) технологий в условиях санкций недружественных государств, изменения миропорядка. В фокусе внимания противодействие использованию искусственного интеллекта в противоправных целях, в том числе в террористической и экстремистской деятельности. Обосновывается необходимость развития системы документов стратегического планирования для выработки векторов и способов противодействия обозначенным угрозам в информационном пространстве, необходимости модернизации и согласованности актов стратегического планирования в рассматриваемой области.

Ключевые слова: информационное право, суверенитет (технологический, цифровой, информационный, культурный), наукоемкие технологии, вызовы и угрозы, стратегические задачи, искусственный интеллект, террористическая и экстремистская деятельность, противодействие, правовое регулирование, правовые средства

Благодарности: Статья подготовлена в рамках выполнения Государственного задания «Обеспечение цифрового суверенитета и информационной безопасности правовыми средствами».

Для цитирования: Полякова Т.А. Обеспечение национального суверенитета России в условиях развития наукоемких технологий: противодействие вызовам праву и угрозам информационной безопасности // Юридический вестник ДГУ. 2024. Т. 52, № 4 (72). С. 157–165. DOI: 10.21779/2224-0241-2024-52-4-157-165

Original article

Ensuring Russia's National Sovereignty in the Context of the Development of Science-Intensive Technologies: Countering Challenges to Law and Threats to Information Security

Tatyana A. Polyakova

Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation, polyakova_ta@mail.ru

Abstract. The article considers issues related to the implementation of tasks to ensure scientific and technological development of the Russian Federation in the context of digital transformation and legal problems in the area under consideration. Based on the analysis of strategic tasks facing the Russian Federation aimed at ensuring technological, digital, information, cultural sovereignty from the standpoint of information law, new tasks of national development of Russia until 2030 and prospects until 2036, including in the area under consideration, are considered. The study made it possible to focus on the problems of legal support for countering new challenges and threats to information security, the landscape of which is expanding due to digitalization processes, the implementation of policies to ensure national sovereignty based on achieving import substitution of information (digital) technologies in the context of sanctions from unfriendly states, and changes in the world order. The focus is on countering the use of artificial intelligence for illegal purposes, including in terrorist and extremist activities. The need to develop a system of strategic planning documents for the development of vectors and methods for countering the identified threats in the information space, the need for modernization and coordination of strategic planning acts in the area under consideration is substantiated.

Keywords: information law, sovereignty (technological, digital, information, cultural), high technologies, challenges and threats, strategic objectives, artificial intelligence, terrorist and extremist activities, counteraction, legal regulation, legal means

Acknowledgments: The article was prepared as part of the State task "Ensuring digital sovereignty and information security by legal means".

For citation: Polyakova T. A. Ensuring Russia's National Sovereignty in the Context of the Development of Science-Intensive Technologies: Countering Challenges to Law and Threats to Information Security. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2024, vol. 49, no. 1 (69), pp. 157–165. DOI: 10.21779/2224-0241-2024-52-4-157-165. (In Russ.).

Актуальность. В условиях активизации процессов цифровой трансформации, которые сегодня имеют, по сути, транснациональный характер, возрастает значение обеспечения национального суверенитета во всех сферах жизнедеятельности государства общества и каждого гражданина. Настоящее время характеризуется расширением спектра новых вызовов и угроз национальной и международной информационной безопасности. Активизация цифрового оборота персональных данных и недостаточность правового регулирования связанных с этим публично-правовых отношений, требуют пристального внимания при формировании государственной политики на основе научных подходов междисциплинарного характера, развития системы понятийного аппарата и систематизации информационного законодательства. Проблемы развития цифрового права и законодательства не только представляют научный интерес, о чем, например, свидетельствует множество дискуссий относительно необходимости разработки информационного или цифрового кодекса, требуют изучения для развития доктрины информационного права в условиях его модернизации, изменения миропорядка, усиления противодействия противоправному воздействию в информационном пространстве. В.Д. Зорькин, характеризуя происходящие в мире изменения, писал, «что мы входим в беспрецедентный в новейшей истории переломный этап международных отношений: жизнь предъявляет нам новые тенденции и риски» [1]. И, оценивая такую ситуацию, он указывает, «что это требует не только быстрого и одновременно глубокого осмысления. Но и форсированной разработки концепции, методологии и технологий адекватных ответов на эти вызовы. В том числе ответов правовых» [2, с. 5–6]. Эти выводы известного ученого, Председателя Конституционного Суда Российской Федерации В.Д. Зорькина не утратили своего значения, а приобрели ещё большую актуальность сегодня.

Изученность проблемы. В юридической науке проблемы правового обеспечения национального суверенитета, национальной и международной информационной безопасности находятся в фокусе внимания, являются многоаспектными, носят междисциплинарный характер, касаются развития цифрового права, угроз применения и регулирования наукоемких технологий, которые эволюционируют в современных условиях, примером тому является активное развитие и применение технологий искусственного интеллекта. Они находят свое отра-

жение как в международном праве, и это неоднократно отмечали А.Я. Капустин [3, с. 100], Т.А. Полякова, Н.А. Троян [4, с. 47], в монографиях по информационному праву, касающихся трансформации информационного права [5], новых вызовов и угроз информационной безопасности [6], культуры информационной безопасности [7, с. 133], оборота цифровых данных, персональных данных [8], проблем обеспечения принципа достоверности при распространении информации [9].

Целесообразность разработки темы исследования. Обеспечение информационной безопасности во всех ее проявлениях, и необходимости развития системы правового обеспечения информационной безопасности сегодня является одним из приоритетов национальной безопасности России, важных для защиты государственного суверенитета в информационном (цифровом пространстве), поскольку несет новые вызовы и угрозы, а также риски в условиях цифровизации. Одной из ключевых задач становится необходимость разработки новых правовых механизмов защиты прав и свобод человека и гражданина, в том числе в связи с развитием цифрового оборота персональных данных во всех сферах, особенно, как справедливо отмечается С.А. Быстрыковой, в транспортной сфере в целях обеспечения транспортной безопасности и антитеррористической защищенности [10, с. 348].

Новизна работы определяется обоснованием предложений, связанных с модернизацией актов стратегического планирования в области информационной безопасности, направленных на обеспечение национального суверенитета России, совершенствованием информационного законодательства, а также выработку предложений по его совершенствованию и согласованности.

Целью работы является выявление угроз и вызовов информационной безопасности, влияющих на обеспечение национального суверенитета России на связанных с реализацией национальной стратегии научно-технологического развития.

Задачами исследования является развитие знаний в рассматриваемой сфере для формирования доктрины информационного права на основе анализа проблем российского научно-технологического суверенитета, выявление подходов к совершенствованию системы актов стратегического планирования в данной области.

Методология исследования. В исследовании применяются как общенаучные, так и специальные юридические методы.

Теоретическая значимость связана с выработкой ключевых теоретических положений, на основе которых может в дальнейшем развиваться доктрина информационного права и система информационного законодательства, а также осуществляться его систематизация и кодификация.

Практическая значимость обусловлена возможностью развития системы актов стратегического планирования в области информационной безопасности и цифрового оборота персональных данных для обеспечения национального суверенитета в информационной сфере.

Основная часть

Новые вызовы и угрозы информационной безопасности

В соответствии со Стратегией национальной безопасности Российской Федерации (2021)¹ обеспечение информационной безопасности определено на 4 месте среди 9 приоритетов обеспечения национальной безопасности. Эти вопросы нашли отражение и в ст. 71. Конституции Российской Федерации². В современных условиях, как показывает анализ, меняющегося спектра угроз информационной безопасности, к ним относятся не только масштабные информационные операции, развязывание информационной войны со стороны недружественных государств, основанные на вмешательстве во внутренние дела государств, так и попытки прямого нарушения суверенитета государств, путем оказания многовекторного давления на экономику, в том числе на объекты критической информационной инфраструктуры (далее – КИИ). Кроме того, это угрозы деструктивного и информационно-психологического воздействия, на что неоднократно нами обращалось внимание [11, с. 40–45].

Среди таких угроз выделяется сегодня усиливающиеся попытки оказания воздействия на молодежную среду, включая различные способы отрицания и разрушения традиционных духовно-нравственных и культурных ценностей, национальной идентичности, и искажения исторической правды, по сути культурного суверенитета. С помощью компьютерных атак на государственную информационную инфраструктуру, цифровую среду осуществляется также пропаганда экстремистских идей, вербуются новые участники, соверша-

ются преступные действия, диверсионно-террористические акты. Это особенно обострилось со стороны недружественных государств в условиях проведения СВО. Среди угроз информационной безопасности, цифровому, технологическому, сетевому, культурному и иным составляющим национального суверенитета, выделяется стремление ряда государств оказывать технологическое доминирование, влекущее за собой зависимость, сдерживание цифрового развития других государств. В связи с этим в свою очередь возрастает значение обеспечения суверенитета в технологической сфере, который в соответствии со Стратегией научно-технологического развития Российской Федерации³ определяется «как способность государства создавать и применять наукоемкие технологии, критически важные для обеспечения независимости и конкурентоспособности, и иметь возможность на их основе организовать производство товаров (выполнение работ и оказание услуг) в стратегических значимых сферах деятельности общества и государства»⁴.

Нельзя обойти вниманием угрозы роста недостоверной, так называемой фейковой информации и противоправных деяний в киберпространстве (отмечается увеличение более чем в 2 раза за последние 5 лет)⁵. Активное использование технологий искусственного интеллекта (далее – ИИ), например, ChatGPT⁶. Поэтому как справедливо отмечается «динамика и беспрецедентная глубина происходящих преобразований определяют необходимость научных исследований характера угроз собственности, жизни и здоровью человека, функционированию государственных и общественных институтов» [12, с. 84–92].

Очевидно, что угрозы информационной безопасности возрастают под влиянием роста науко-

¹ Указ Президента Российской Федерации от 02.07.2021. № 400 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>. 03.07.2021.

² Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г., с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>, 04.07.2020. Поправки, внесенные Законом РФ о поправке к Конституции РФ от 14.03.2020 № 1-ФКЗ, вступили в силу 4 июля 2020 года (Указ Президента РФ от 03.07.2020 № 445).

³ Указ Президента Российской Федерации от 28.02.2024 №145 «О Стратегии научно-технологического развития Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>. 28.02.2024.

⁴ Указ Президента Российской Федерации от 28.02.2024 №145 «О Стратегии научно-технологического развития Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>. 28.02.2024.

⁵ За пять лет число киберпреступлений увеличилось более чем в два раза // Российская газета. URL: <https://rg.ru/2024/09/25/policiia-v-seti.html?ysclid=m3lhg60fmh730564783> (дата обращения: 17.ноября 2024 г.).

⁶ Так, ChatGPT, сегодня широко уже используются для дезинформации, разжигания вражды, распространения деструктивного контента, написания вредоносного кода и фишинговых электронных писем и т.д. Угрозы представляет применение технологий ИИ, имеющих информационно-техническое измерение и относящиеся к наукоемким технологиям. Например, возможности ChatGPT и иных подобных нейросетей используются даже для написания вредоносного кода и фишинговых электронных писем.

емких технологий, поскольку увеличение объема цифровых данных, а тем самым обострение рисков, связывают с использованием наукоемких (в том числе, сквозных и критических) технологий.

Риски в цифровой сфере связывают с необходимостью формирования пространства доверия (идентификацией объектов и субъектов в цифровой среде принятия мер по усилению защиты каналов связи, обеспечению конфиденциальности информации [13, с. 90–100.], а также повышению уровня достоверности информации [14, с. 46–50] и знаний в цифровых коммуникациях.

Для устойчивого развития России и реализации перспектив ее будущего, достижения технологического лидерства развитие науки имеет одно из приоритетных значений. На это обращается Президентом РФ внимание практически во всех актах стратегического планирования, начиная со Стратегии национальной безопасности¹, Стратегии научно-технологического развития², Доктрине информационной безопасности³, а также иных документах стратегического планирования Российской Федерации, в соответствии с которой именно российская наука является основой суверенного развития государства [15].

Это вытекает и из майских указов Президента РФ 2024 г., новых стратегических приоритетов национального развития до 2030 года и перспектив до 2036 г., задач укрепления цифрового суверенитета в российском информационном пространстве, и очевидности возрастающего значения правовых научных исследований в области информационной безопасности, включая правовые проблемы обеспечения цифрового оборота персональных данных в системе транспортной безопасности РФ. В рамках данной статьи акцент на последнее делается, учитывая, что сегодня транспортная сфера связана со всеми сферами и отраслями нашей жизни, на осно-

ве решения задач, направленных на достижение «цифровой зрелости» [16, с.107–116].

Развитие системы международной информационной безопасности

В современных условиях противодействия продвижения российских инициатив на площадке ООН, как справедливо отмечается и в Концепции внешней политики России, а также и в научных исследованиях сектора информационного права и международной информационной безопасности ИГП РАН, необходима активизация деятельности региональных объединений (ШОС, ОДКБ, СНГ и др.). Особенно, на наш взгляд, требует внимания эта тема в повестке БРИКС, в год председательства России в этом региональном объединении. Указанная тема широко обсуждалась на Международном Юридическом Форуме БРИКС, проходившем в сентябре 2024 г. в МГИМО. Также расширение сотрудничества стран БРИКС на основе общих интересов и ключевых приоритетов, приверженности духу БРИКС, в том числе суверенного равенства, открытости и иных, связанных с этим вопросов, отражены в Казанской декларации по итогам саммита БРИКС 23 октября 2024⁴ г. (что особенно важно в год председательства России в БРИКС) для укрепления противодействия информационным вызовам, необходимости усиления интеграции мировых правовых усилий и международного сотрудничества в области международной информационной безопасности (далее – МИБ) [17, с. 139–149].

Представляется, что нельзя, учитывая транснациональный характер многих информационных угроз, отрицать роль норм и общепризнанных принципов международного права при обеспечении безопасности в ИКТ-среде. Нужна консолидация действий государств для эффективного решения данной проблемы в информационном пространстве и справедливым является утверждение, что, «ключевую роль в механизме обеспечения международной информационной безопасности играет правовое регулирование» [18, с. 9–18].

Следует обратить внимание, что такая позиция, касающаяся обеспечения МИБ, последовательно продвигается Россией на площадке ООН с 1998 года (в рамках деятельности различных групп, открытого состава по данным вопросам и т.д.) [19, с. 53–60]. В 2023 г. Россией в ООН был внесен проект Конвенции об обеспечении МИБ и важно отметить, что в нем сделан акцент на принципе суверенного равенства государств и невмешательства во внутренние дела, в том числе для наращивания сил ИБ. Также нужно отметить значение одобрения в августе 2024 г. (специальным комитетом ООН) проекта международной конвенции о противодействии использованию ИКТ в преступных целях, который направлен

¹ Указ Президента РФ от 2 мая 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (часть II), ст. 5351.

² Указ Президента РФ от 28 февраля 2024 г. № 145 «О Стратегии научно-технологического развития Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 28.02.2024.

³ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. №50, ст.7074; Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20, ст. 2901; Указ Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СЗ РФ. 2021. № 16 (ч. I), ст.2746; Указ Президента РФ от 29 мая 2020 № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Официальный интернет-портал. URL: <http://www.pravo.gov.ru>, 29.05.2020.

⁴ Президент России : официальный сайт. URL: <http://www.kremlin.ru/search?query=Казанской+декларации+по+итогам+саммита+БРИКС+23+октября+2024/> (дата обращения: 17.ноября 2024).

на укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и обмен доказательствами в электронной форме. Это исключительно важные вопросы сотрудничества в области ИБ и, по сути, первый проект универсальной конвенции по такому вопросу. Учитывая, что последняя в ООН универсальная конвенция была принята уже более 20 лет назад, этот проект можно расценивать, как определенный прорыв и первый проект такого уровня в области борьбы с информационной преступностью¹. Кроме того, его оценивают как акт нового поколения, поскольку в него включены вопросы защиты персональных данных и сбора цифровых доказательств, который отличается, по своей, сути, и содержанию, еще и тем, что в нем предлагается закрепить принцип государственного суверенитета². Хотя следует признать, что этому проекту нужно преодолеть тернии на пути его принятия, еще и потому, что в нем предпринята весьма сложная попытка детально регламентировать порядок международного сотрудничества (включая киберпреступления, а также вопросы оказания взаимной правовой помощи по уголовным делам).

В условиях развивающихся в мире дискуссий относительно утраты в настоящее время (в период тектонических сдвигов) позиций международного права³, его отрицания, отмечается рост международного сотрудничества в региональных и двусторонних форматах России в области МИБ, что происходит на фоне укрепления потенциала многосторонних региональных объединений и интеграционных структур (БРИКС, ШОС, СНГ, ЕАЭС, ОДКБ), где в течение 20 лет принят целый ряд международных правовых актов в области МИБ⁴.

¹ Как известно, Будапештскую, европейскую конвенцию о киберпреступности 2001 г. Россия не подписала как нарушающую права суверенных государств и противоречащую интересам суверенных государств (п.32b).

² Закрепление в данном проекте принципа государственного суверенитета существенно отличает его от вышеназванной Будапештской конвенции (2001 г.).

³ Вместе с тем, сегодня следует отметить, в российском паспорте научных специальностей по праву включено в международное публичное право (5.1.5) такое направление, как международное информационное право.

⁴ Среди них следует выделить: Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г., Соглашение о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности от 20 ноября 2013 г., Соглашение о сотрудничестве государств - членов ОДКБ в области обеспечения информационной безопасности от 30 ноября 2017 г., Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г.

Сегодня наращивание усилий по развитию международно-правовой базы сотрудничества в области МИБ в форматах региональных международных организаций и объединений – перспективная тенденция. Важно дальнейшее развитие двустороннего сотрудничества России в рассматриваемой сфере с конструктивно настроенными дружественными государствами⁵. В условиях гибридной войны коллективного Запада против России возрастает значение сотрудничества России с Республикой Беларусь – в области МИБ, с нашим стратегическим союзником⁶.

Противодействие угрозам нового цифрового мира и правовое измерение национального суверенитета России

Политика России, направленная на противодействие угрозам нового цифрового мира, безусловно, связана с развитием системы правового регулирования в сфере ИБ, которая как уже отмечалось, выделена в качестве национального приоритета. 21 век, неслучайно называют информационным, в России был утвержден ряд актов стратегического планирования и сформирована обширная организационно-правовая основа обеспечения ИБ⁷. Создана и функционирует государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, развивается ведомственное правовое регулирование (ФСБ и ФСТЭК России) в сфере обеспечения безопасности КИИ. Совершенствуется законодательство в области защиты информации ограниченного доступа, включая федеральные законы «О государственной тайне», «О коммерческой тайне», «О персональных данных» и другие. В декабре 2022 г. принят Федеральный закон, регулирующий отношения, возникающие при осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных с использованием специализированной государственной информаци-

⁵ В настоящее время Россией заключено более 30 межправительственных двусторонних соглашений (с Бразилией, Вьетнамом, Индией, Китаем, Кубой, Туркменистаном и др.).

⁶ В 2021 году в рамках заседания Совета министров Союзного государства были утверждены 28 союзных программ (дорожных карт), направленных на реализацию масштабных задач по укреплению российско-белорусской интеграции, в которых уделено внимание и вопросам информационной безопасности. В частности, одна из программ нацелена на гармонизацию требований в области обеспечения ИБ в финансовой сфере. Важным шагом на пути сотрудничества наших государств в этой области стало утверждение в 2023 г. Концепции информационной безопасности Союзного государства Республики Беларусь и России.

⁷ Базовыми в информационной сфере являются федеральные законы «Об информации, информационных технологиях и о защите информации» «О защите детей от информации, причиняющей вред их здоровью и развитию», «О безопасности критической информационной инфраструктуры Российской Федерации».

онной системы. С 1 января 2025 г. вступает в силу Федеральный закон № 168-ФЗ (принят в 2020 г.) о едином федеральном регистре сведений о населении Российской Федерации и важной задачей является обеспечение надежной защиты информации, информационной безопасности.

Одним из ключевых направлений государственной политики является обеспечение технологического суверенитета, что нашло системное отражение в Стратегии научно-технологического развития РФ¹ и в майских указах Президента РФ.

Анализ показывает, что на укрепление ИБ направлен специальный Указ Президента РФ 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» с изменениями, внесенными в июне 2024 г.². Обращает внимание важность закрепления в данном Указе (вступает в силу с 1 января 2025 г.) требований о запрете на использование средств защиты информации, странами происхождения которых являются недружественные иностранные государства либо находящиеся под их юрисдикцией производители. Эта норма направлена на обеспечение импортозамещения и технологического суверенитета. Ранее этот запрет был направлен на иностранные сервисы (работ, услуг) по обеспечению ИБ в целях укрепления технологического суверенитета нашей страны в области информационной безопасности.

Заключение. Исследование позволяет обосновать необходимость ускорения разработки и утверждения новой национальной Доктрины информационной безопасности как ключевого акта стратегического планирования в рассматриваемой области, учитывая необходимость уточнения в нем вопросов, связанных с рисками, новыми вызовами и угрозами) в цифровую эпоху, проявившимися после утверждения действующей ныне редакции Доктрины (2016).

Среди проблем в рассматриваемой сфере можно выделить: неурегулированность вопросов юрисдикции при трансграничном информационном обмене; недостаточность международного правового регулирования, в частности, в области обеспечения МИБ (включая институты ответственности и соблюдения необязательных правил поведения государств в ИКТ-среде и международного сотрудничества);

отсутствие единого межнационального и междисциплинарного подхода к понятийному аппарату и соотношению информационной и кибербезопасности, критериев типологизации правонарушений и механизмов ответственности; а также низкий уровень в настоящее время межгосударственного диалога в данной сфере, необходимость повышения уровня доверия в информационной среде.

На основе проведенного анализа обоснована целесообразность согласования положений актов стратегического планирования, связанных с ИБ, необходимость продолжения исследований, направленных на развитие системы правового обеспечения ИБ и доктрины информационного права. Требуют уточнения приоритетные задачи и векторы правового регулирования отношений, связанных с ИБ для обеспечения национального суверенитета России в технологической сфере, как способности государства создавать и применять наукоемкие технологии, критически важные для обеспечения независимости и конкурентоспособности [20, с. 281–283], а также определить особенности безопасного и доверенного использования наиболее востребованных цифровых технологий, включая технологии ИИ, в целях защиты прав и свобод граждан, персональных данных в условиях цифрового оборота [21].

Полагаем, что для укрепления системы информационной безопасности в России необходимо определить новые научно-технологические подходы к формированию государственной системы правовой информации в Российской Федерации, разработки нового Классификатора учета правовых актов, а также проекта Информационного кодекса РФ, для упорядочения правового регулирования информационных отношений, в том числе и направленных на обеспечение информационной, цифровой и кибербезопасности, закрепление универсального для информационной сферы понятийного аппарата, системы принципов, требований. Кроме того, его разработка должна быть направлена на выявление неэффективных и устаревших информационно-правовых норм, закрепление новых институтов, включая и цифровое право, как части информационного права [22, 23].

¹ Указ Президента РФ от 28 февраля 2024 г. № 145 «О Стратегии научно-технического развития Российской Федерации» // Официальный интернет-портал правовой информации URL: <http://pravo.gov.ru>, 28.02.2024.

² На руководителей органов исполнительной власти, государственных корпораций (компаний), стратегических предприятий и иных организаций возложена персональная ответственность за обеспечение информационной безопасности и предусмотрено создание специализированного структурного подразделения, по обеспечению ИБ либо возложение данных функций на существующее структурное подразделение.

Также важное значение имеют положения об осуществлении мониторинга защищенности информационных ресурсов, принадлежащих таким органам (организациям), порядок которого регламентирован приказом ФСБ России.

Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 28.02.2024. (Изменения, внесенные Указом Президента РФ от 13.06.2024 № 500, вступили в силу с 13 июня 2024 года).

Список источников

1. Общероссийская общественная организация Ассоциация юристов России // Экономика и право: новый контекст / Текст Валерий Зорькин. URL: <https://old.alrf.ru/blog/ekonomika-i-pravo-novyj-kontekst/?ysclid=m3kpt3i0q9237807023> (дата обращения: 17.11.2024).
2. Зорькин В.Д. Цивилизация права и развитие России: монография / В.Д. Зорькин. 2-е изд., испр. и доп. М.: Норма : ИНФРА-М–2016. С.5–6.
3. Капустин А.Я. Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. 2022. Т. 18. № 6. С. 99–108.
4. Полякова Т.А., Троян Н.А. Обеспечение суверенитета в информационном пространстве – стратегическая задача национальной политики // Правовая политика и правовая жизнь. 2024. № 1. С. 41–53.
5. Трансформация информационного права: монография / отв. ред. Т. А. Полякова, А. В. Минбале-ев, В. Б. Наумов. М.: Институт государства и права РАН, 2023.
6. Полякова Т.А., Смирнов А.А. Правовые аспекты обеспечения информационной безопасности при использовании технологий искусственного интеллекта // Вестник Московского университета. Серия 26: Государственный аудит. 2024. № 3. С. 89–106.
7. Полякова Т. А., Минбале-ев А. В., Троян Н. А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С.131–144.
8. Быстрыкова С.А. Развитие правового регулирования персональных данных в условиях формирования экономики данных в России // Право и государство: теория и практика. 2024. № 2 (230). С. 179–182.
9. Троян Н.А., Петровская О.В. Принцип достоверности при распространении и предоставлении информации с использованием искусственного интеллекта // Правовая информатика. 2023. № 2. С. 75–81.
10. Быстрыкова С.А. Формирование государственной политики в системе транспортной безопасности: публично-правовые вопросы цифрового оборота персональных данных // Правовая политика и правовая жизнь. 2024. № 3(97). С. 347–351.
11. Полякова Т.А., Смирнов А.А. Использование технологий искусственного интеллекта в террористической и экстремистской деятельности: характеристика и правовые аспекты противодействия // Право.by Научно-практический журнал. 2024. №4 (90). С. 64–72.
12. Полякова Т.А., Смирнов А.А. Правовое обеспечение международной информационной безопасности: приоритеты для Союзного государства // Право.by Научно-практический журнал. 2023. №5 (85). С. 84–92.
13. Наумов В. Б. Современное правовое регулирование идентификации в России. // Трансформация информационного права: монография / отв. ред. Т. А. Полякова, А.В. Минбале-ев, В.Б. Наумов. М.: Институт государства и права РАН, 2023. С. 90–100.
14. Петровская О. В. Принцип достоверности в информационном праве в условиях цифровой трансформации // Мониторинг правоприменения. 2021. № 3 (40). С. 46–50.
15. Полякова Т. А., Минбале-ев А. В., Кроткова Н. В. Трансформация науки информационного права и информационного законодательства: новый этап в условиях научно-технологического развития России // Государство и право. 2024. № 9. С. 166–179.
16. Полякова Т. А., Минбале-ев А. В. Понятие и правовая природа «цифровой зрелости» // Государство и право. 2021. № 9. С.107–116.
17. Полякова Т.А., Зиновьева Е.С., Смирнов А.А. Международная информационная безопасность: универсальное правовое измерение // Государство и право. 2023. № 12. С. 139–149.
18. Полякова Т.А., Смирнов А.А. Развитие системы международной информационной безопасности и международное информационное право // Шестые Бачиловские чтения: сборник статей участников Международной научно-практической конференции / отв. ред. Т.А. Полякова, А.В. Минбале-ев, В.Б. Наумов. М.: Институт государства и права РАН, 2023. С. 9–18.
19. Полякова Т.А. Стратегические задачи формирования системы международной информационной безопасности и международное информационное право: проблемы и перспективы // В сборнике: Безопасность как стратегический национальный приоритет России в условиях современности. Материалы шестого международного транспортно-правового форума. М., 2024. С.53–60.
20. Полякова Т.А., Троян Н.А., Петровская О.В. Правовое обеспечение укрепления технологического суверенитета Российской Федерации на основе реализации модели импортозамещения // Правовая политика и правовая жизнь. 2024. № 3. С. 281–293.
21. Камалова Г.Г., Полякова Т.А. Правовое регулирование виртуальной и дополненной реальности: проблемы и векторы развития // Вестник Удмуртского университета. Серия Экономика и право. 2023. Т. 33. № 5. С. 872–876.
22. Минбале-ев А. В. Цифровое право как комплексный институт российского права // Проблемы пра-ва. 2019. № 4 (73). С. 58–64.

23. Полякова Т.А., Троян Н.А. Актуальные проблемы систематизации законодательства России под влиянием цифровых технологий в период цифровой трансформации // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 2 (102). С. 25–33.

References

1. Obshcherossiyskaya obshchestvennaya organizatsiya Assotsiatsiya yuristov Rossii [All-Russian public organization Association of Lawyers of Russia], *Ekonomika i pravo: noviy kontekst [Economics and Law: a new context]*; Text by Valery Zorkin. (In Russ.). Available at: <https://old.alrf.ru/blog/ekonomika-i-pravo-noviy-kontekst/?ysclid=m3kpt3i0q9237807023> (accessed 17.11.2024).
2. Zorkin V.D. Tsivilizatsiya prava i razvitie Rossii: monografiya [The civilization of law and the development of Russia: monograph], V.D. Zorkin. 2nd ed., ispr. and add. Moscow: Norma : INFRA-M Publ., 2016, pp. 5–6. (In Russ.).
3. Kapustin A.Ya. Suverenitet gosudarstva v kiberprostranstve: mezhdunarodno-pravovoe izmerenie [State sovereignty in cyberspace: international legal dimension], *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya [Journal of Foreign Legislation and Comparative Jurisprudence]*, 2022, vol. 18, no. 6, pp. 99-108. (In Russ.).
4. Polyakova T.A., Troyan N.A. Obespechenie suvereniteta v informatsionnom prostranstve – strategicheskaya zadacha natsional'noy politiki [Ensuring sovereignty in the information space is a strategic task of national policy], *Pravovaya politika i pravovaya zhizn' [Legal policy and legal life]*, 2024, no. 1, pp. 41-53. (In Russ.).
5. Transformatsiya informatsionnogo prava: monografiya [Transformation of information law: monograph], ed. T. A. Polyakova, A.V. Minbaleev, V. B. Naumov. Moscow: Institute of State and Law of the Russian Academy of Sciences Publ., 2023, p. 256. (In Russ.).
6. Polyakova T.A., Smirnov A.A. Pravovye aspekty obespecheniya informatsionnoy bezopasnosti pri ispol'zovanii tekhnologiy iskusstvennogo intellekta [Legal aspects of information security when using artificial intelligence technologies], *Vestnik Moskovskogo universiteta. Seriya 26: Gosudarstvenniy audit [Bulletin of the Moscow University. Series 26: State Audit]*, 2024, no. 3, pp. 89–106. (In Russ.).
7. Polyakova T. A., Minbaleev A.V., Troyan N. A. Formirovanie kul'tury informatsionnoy bezopasnosti grazhdan Rossiyskoy Federatsii v usloviyakh novykh vyzovov: publichno-pravovye problemy [Formation of the culture of information security of citizens of the Russian Federation in the context of new challenges: public law problems], *Gosudarstvo i pravo [State and law]*, 2023, no. 5, pp. 131–144. (In Russ.).
8. Bystryakova S.A. Razvitie pravovogo regulirovaniya personal'nykh dannykh v usloviyakh formirovaniya ekonomiki dannykh v Rossii [The development of legal regulation of personal data in the context of the formation of the data economy in Russia], *Pravo i gosudarstvo: teoriya i praktika [Law and the State: theory and practice]*, 2024, no. 2 (230), pp. 179-182. (In Russ.).
9. Troyan N.A., Petrovskaya O.V. Printsip dostovernosti pri rasprostranении i predostavlenii informatsii s ispol'zovaniem iskusstvennogo intellekta [The principle of reliability in the dissemination and provision of information using artificial intelligence], *Pravovaya informatika [Legal informatics]*, 2023, no. 2, pp. 75-81. (In Russ.).
10. Bystryakova S.A. Formirovanie gosudarstvennoy politiki v sisteme transportnoy bezopasnosti: publichno-pravovye voprosy tsifrovogo oborota personal'nykh dannykh [Formation of state policy in the transport security system: public law issues of digital turnover of personal data], *Pravovaya politika i pravovaya zhizn' [Legal policy and legal life]*, 2024, no. 3 (97), pp. 347-351. (In Russ.).
11. Polyakova T.A., Smirnov A.A. Ispol'zovanie tekhnologiy iskusstvennogo intellekta v terrori-sticheskoy i ekstremistkoy deyatel'nosti: kharakteristika i pravovye aspekty protivodeystviya [The use of artificial intelligence technologies in terrorist and extremist activities: characteristics and legal aspects of counteraction], *Pravo.by Nauchno-prakticheskii zhurnal [Right.by Scientific and Practical Journal]*, 2024, no. 4 (90), pp. 64-72. (In Russ.).
12. Polyakova T.A., Smirnov A.A. Pravovoe obespechenie mezhdunarodnoy informatsionnoy bezopasnosti: priority dlya Soyuznogo gosudarstva [Legal support of international information security: priorities for the Union State], *Pravo.by Nauchno-prakticheskii zhurnal [Right.by Scientific and Practical Journal]*, 2023, no. 5 (85), pp. 84-92. (In Russ.).
13. Naumov V. B. Sovremennoe pravovoe regulirovanie identifikatsii v Rossii [Modern legal regulation of identification in Russia], *Transformatsiya informatsionnogo prava: monografiya [Transformation of information law: monograph]*, ed. by T. A. Polyakov, A.V. Minbaleev, V.B. Naumov. Moscow: Institute of State and Law of the Russian Academy of Sciences Publ., 2023, pp. 90-100. (In Russ.).
14. Petrovskaya O. V. Printsip dostovernosti v informatsionnom prave v usloviyakh tsifrovoy transformatsii [The principle of reliability in information law in the context of digital transformation], *Monitoring pravoprimeneniya [Monitoring of law enforcement]*, 2021, no. 3 (40), pp. 46-50. (In Russ.).
15. Polyakova T. A., Minbaleev A.V., Krotkova N. V. Transformatsiya nauki informatsionnogo prava i informatsionnogo zakonodatel'stva: noviy etap v usloviyakh nauchno-tekhnologicheskogo razvitiya Rossii [Transformation of the science of information law and information legislation: a new stage in the conditions of scientific and technological development of Russia], *Gosudarstvo i pravo [State and law]*, 2024, no. 9, pp. 166-179. (In Russ.).

16. Polyakova T. A., Minbaleev A.V. Ponyatie i pravovaya priroda "tsifrovoy zrelosti" [The concept and legal nature of "Digital maturity"], *Gosudarstvo i pravo* [State and law], 2021, no. 9, pp. 107–116. (In Russ.).
17. Polyakova T.A., Zinovieva E.S., Smirnov A.A. Mezhdunarodnaya informatsionnaya bezopasnost': universal'noe pravovoe izmerenie [International information security: a universal legal dimension], *Gosudarstvo i pravo* [State and law], 2023, no. 12, pp.139–149. (In Russ.).
18. Polyakova T.A., Smirnov A.A. Razvitie sistemy mezhdunarodnoy informatsionnoy bez-opasnosti i mezhdunarodnoe informatsionnoe pravo [Development of the international information security system and international information law], *Shestye Bachilovskie chteniya* [Sixth Bachilov readings]: collection of articles by participants of the International scientific and practical Conference; ed. T.A. Polyakova, A.V. Minbaleev, V.B. Naumov. Moscow: Institute of State and Law of the Russian Academy of Sciences Publ., 2023, pp. 9-18. (In Russ.).
19. Polyakova T.A. Strategicheskie zadachi formirovaniya sistemy mezhdunarodnoy informatsionnoy bezopasnosti i mezhdunarodnoe informatsionnoe pravo: problemy i perspektivy [Strategic objectives of the formation of the international information security system and international information law: problems and prospects], *Bezopasnost' kak strategicheskiy natsional'niy prioritet Rossii v usloviyakh sovremennosti* [Security as a strategic national priority of Russia in modern conditions]: materials of the sixth International Transport and Legal Forum. Moscow, 2024, pp. 53-60. (In Russ.).
20. Polyakova T.A., Troyan N.A., Petrovskaya O.V. Pravovoe obespechenie ukrepleniya tekhnologicheskogo suvereniteta Rossiyskoy Federatsii na osnove realizatsii modeli importozameshcheniya [Legal support for strengthening the technological sovereignty of the Russian Federation based on the implementation of the import substitution model], *Pravovaya politika i pravovaya zhizn'* [Legal policy and legal life], 2024, no. 3, pp. 281-293. (In Russ.).
21. Kamalova G.G., Polyakova T.A. Pravovoe regulirovanie virtual'noy i dopolnennoy real'nosti: problemy i vektory razvitiya [Legal regulation of virtual and augmented reality: problems and vectors of development], *Vestnik Udmurtskogo universiteta. Seriya Ekonomika i pravo* [Bulletin of the Udmurt University. Economics and Law series], 2023, vol. 33, no.5, pp. 872-876. (In Russ.).
22. Minbaleev A. V. Tsifrovoye pravo kak kompleksniy institut rossiyskogo prava [Digital law as a comprehensive institute of Russian law], *Problemy prava* [Problems of law], 2019, no. 4 (73), pp. 58-64. (In Russ.).
23. Polyakova T.A., Troyan N.A. Aktual'nye problemy sistematizatsii zakonodatel'stva Rossii pod vliyaniem tsifrovyykh tekhnologiy v period tsifrovoy transformatsii [Actual problems of systematization of Russian legislation under the influence of digital technologies in the period of digital transformation], *Vestnik Universiteta imeni O.E. Kutafina (MGYuA)* [Bulletin of the O.E. Kutafin University (MGUA)], 2023, no. 2 (102), pp. 25-33. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Полякова Татьяна Анатольевна, Главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности, Институт государства и права РАН, доктор юридических наук, профессор, Заслуженный юрист Российской Федерации, г. Москва, Российская Федерация. E-mail: polyakova_ta@mail.ru

INFORMATION ABOUT THE AUTHOR

Tatyana Anatolyevna Polyakova, Chief Researcher, Acting Head of the Information Law and International Information Security Sector of the Institute of State and Law of the Russian Academy of Sciences, Doctor of Law, Professor, Honored Lawyer of the Russian Federation, Moscow, Russian Federation. E-mail: polyakova_ta@mail.ru

Поступила в редакцию 17.11.2024 г.;
одобрена после рецензирования 25.11.2024 г.;
принята к публикации 06.12.2024 г.

Received 17.11.2024; approved after reviewing
25.11.2024; accepted for publication 06.12.2024