Научная статья
УДК 342.733
https://doi.org/10.33874/2072-9936-2024-0-4-145-154

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ ЦИФРОВЫМ УГРОЗАМ*

Татьяна Анатольевна Полякова

Институт государства и права Российской академии наук,
119019, Россия, г. Москва, ул. Знаменка, д. 10

polyakova_ta@mail.ru

Аннотация

В статье обращено внимание на правовые проблемы, связанные с обеспечением суверенитета Российской Федерации и информационной безопасности, исходя из современных подходов к противодействию новым вызовам и угрозам, в том числе цифровым, на основе результатов научных исследований и разработок междисциплинарного характера, преодоления рисков трансформации в цифровую эпоху. Целью исследования является посредством анализа новых вызовов и угроз сформулировать предложения, направленные на развитие системы правового обеспечения информационной безопасности. Для реализации поставленных задач использованы общенаучные методы (анализа, синтеза), методы индукции и дедукции, сравнительно-правовой метод и метод толкования правовых норм. Акцентировано внимание на рисках в области информационной безопасности, вызванных широким спектром правовых проблем, обоснован вывод о необходимости модернизации и согласованности актов стратегического планирования.

Ключевые слова*:* государственный суверенитет; информационная безопасность; вызовы и риски; цифровые угрозы; правовое обеспечение; искусственный интеллект; идентификация и аутентификация.

* Статья подготовлена в рамках выполнения государственного задания «Обеспечение цифрового суверенитета и информационной безопасности правовыми средствами» FMUZ-2024-0035.

Для цитирования: *Полякова Т. А.* Правовое обеспечение государственного суверенитета и информационная безопасность: вопросы противодействия цифровым угрозам // Вестник Российской правовой академии. 2024. № 4. С. 145–154. https://doi.org/10.33874/2072-9936-2024-0-4-145-154

Research Article

LEGAL SUPPORT OF STATE SOVEREIGNTY AND INFORMATION SECURITY: ISSUES OF COUNTERING DIGITAL THREATS*

Tatyana A. Polyakova

Institute of State and Law of the Russian Academy of Sciences,
10 Znamenka St., Moscow, 119019, Russia

polyakova_ta@mail.ru

Abstract

The article draws attention to the legal problems associated with ensuring the sovereignty of the Russian Federation and information security on the basis of modern approaches to counter new challenges and threats, including digital ones, based on the results of scientific research and development of interdisciplinary nature, overcoming the risks of transformation in the digital era. The purpose of the study is to analyse new challenges and threats and formulate proposals aimed at developing the system of legal support for information security. In order to realise the set tasks the general scientific methods (analysis, synthesis), induction and deduction, comparative-legal method and method of interpretation of legal norms were used. Attention is focused on the risks in the field of information security caused by a wide range of legal problems, the need for modernisation and consistency of strategic planning acts.

Keywords: state sovereignty; information security; challenges and risks; digital threats; legal support; artificial intelligence; identification and authentication.

For citation: *Polyakova T. A.* Legal Support of State Sovereignty and Information Security: Issues of Countering Digital Threats. *Herald of the Russian Law Academy*, 2024, no. 4, pp. 145–154. (In Russ.) https://doi.org/10.33874/2072-9936-2024-0-4-145-154

* The article was prepared within the framework of the state task "Ensuring Digital Sovereignty and Information Security by Legal Means" FMUZ-2024-0035.

Введение

Активное развитие цифровизации, цифровой трансформации порождает новые информационные вызовы и угрозы, имеющие в значительной степени транснациональный характер. Следует признать, что на динамику роста цифровых угроз влияют изменение миропорядка, усиление применения противоправного воздействия в информационном пространстве на государство, общество и гражданина. Как изменяется сегодня ландшафт угроз информационной безопасности, какие факторы на это влияют и каковы вызовы праву?

1. Новые вызовы и угрозы информационной безопасности

В настоящее время совокупность таких угроз включает уже как крупномасштабные информационные операции, основанные на вмешательстве во внутренние дела государств, так и нарушения их суверенных прав, попытки многофункционального влияния на экономику, особенно при этом привлекают внимание объекты критической информационной инфраструктуры (далее – КИИ). Особый алармизм вызывает рост угроз деструктивного характера, оказывающих информационно-психологическое воздействие на все стороны жизни общества, государства и каждого гражданина. На это обращалось особое внимание А. А. Смирновым в его научном исследовании [1, с. 40–45]. Обеспокоенность вызывают попытки оказать влияние на молодежь, будущие поколения, а также стремление различными способами разрушить традиционные духовно-нравственные и культурные ценности. Отмечается значительный рост компьютерных атак на российские информационные системы и ресурсы, а также цифровую среду, которая активно используется для пропаганды экстремистами своих идей, вербовки новых участников и стимулирования преступных действий, диверсионно-террористических актов. Угрозами информационной безопасности и соответственно, технологическому суверенитету, является попытки использования недружественными государствами своего технологического доминирования, а также прямых попыток тем самым сдерживания цифрового развития других государств, их технологической зависимости и цензуры в цифровом пространстве. В целях противодействия этим угрозам возрастает роль национального суверенитета (цифрового, научно-технологического и т.д.). Безусловно, тревогу вызывает рост недостоверной информации (фейки), их массовое распространение, особенно опасными являются угрозы распространения в цифровой среде деструктивных молодежных субкультур, а также более чем в два раза увеличение за последние пять лет противоправных деяний в киберпространстве увеличилось более чем вдвое (около 40% и наибольшее среди них количество составляют мошенничества и кражи денежных средств со счетов). Активно используются уже в противоправной деятельности голосовые и звуковые дипфейки, которые используются и в информационном противоборстве, а также ИИ (например, *ChatGPT*) широко уже используются для дезинформации, разжигания вражды, распространения деструктивного контента, написания вредоносного кода и фишинговых электронных писем и т.д. Поэтому, как справедливо отмечается, «динамика и беспрецедентная глубина происходящих преобразований предопределяют необходимость научных исследований

характера угроз собственности, жизни и здоровью человека, функционированию государственных и общественных институтов» [2, с. 32–33].

Угрозы представляет применение технологий ИИ, имеющих информационно-техническое измерение и относящиеся к наукоемким технологиям. Так, уже возможности *ChatGPT* и иных подобных нейросетей используются даже для написания вредоносного кода и фишинговых электронных писем. В рамках настоящей статьи автором не ставилась задача представить полный перечень угроз информационной безопасности, поскольку они постоянно эволюционируют по мере научно-технологического развития. К чему же приводит рост таких угроз? Как минимум к потере доверия в ИКТ-среде, так как использование информационных (цифровых) технологий приводит к колоссальному росту объема цифровых данных, а тем самым обострению рисков, связанных с информационной безопасностью, вызывают сомнения необходимости использования наукоемких (в том числе сквозных и критических) технологий.

Такие вызовы и угрозы, многочисленные риски свидетельствуют о необходимости принятия комплекса мер по усилению организационной, технологической и правовой защищенности при росте цифровизации (это касается идентификации объектов и субъектов в цифровой среде [3, с. 90–100], принятия мер по усилению защиты каналов связи, обеспечению конфиденциальности информации, а также повышению уровня достоверности информации [4, с. 46–50] и знаний в цифровых коммуникациях). Полагаем, в этих условиях стратегической задачей является необходимость повышения роли науки и технологий в обеспечении устойчивого будущего и развитии России, а также ее конкурентоспособности и, соответственно, определения ее положения в мире. На это обращено внимание Президентом РФ в Стратегии научно-технологического развития Российской Федерации, в соответствии с которой именно российская наука «в настоящее время служит основой суверенного развития государства, создавая необходимые предпосылки и условия для обоснованного, сбалансированного и эффективного решения всего комплекса стоящих перед Российской Федерацией социальных, экономических, культурных и иных задач, обеспечения безопасности страны и ее значимого вклада в интеллектуальное достояние человечества. Вместе с тем отмечены и негативные тенденции…» [5].

2. Развитие системы международной информационной безопасности

В современных условиях, как справедливо отмечается в научной работе, подготовленной в Институте государства и права Российской академии наук, и это подтверждается активизацией деятельности региональных объединений (БРИКС, ШОС, ОДКБ, СНГ и др.), для эффективного противодействия информационным вызовам сегодня особенно требуется интеграция мировых правовых усилий и организация эффективного международного сотрудничества в области международной информационной безопасности (далее – МИБ) [6]. Учитывая глобальный и трансграничный характер многих информационных угроз, нормы и принципы международного права, безусловно, играют важную роль в обеспечении безопасности в ИКТ-среде, необходима консолидация действий государств для эффективного решения данной проблемы в целях противодействия угрозам в информацион-

ном пространстве, при этом полагаем, как справедливо уже отмечалось, «ключевую роль в механизме обеспечения международной информационной безопасности играет правовое регулирование» [7].

Такая политико-правовая позиция нашла отражение в последовательном продвижении Россией начиная с 1998 г. на площадке ООН инициатив, связанных с обеспечением МИБ, деятельностью групп открытого состава по данным вопросам и т.д. Особо сегодня следует отметить внесение Россией в 2023 г. в ООН нового проекта Конвенции об обеспечении международной информационной безопасности, в основе которой заложен принцип суверенного равенства государств и невмешательства во внутренние дела, в том числе для наращивания сил информационной безопасности. Следует также обратить внимание, что в августе 2024 г. – специальным комитетом ООН одобрен проект первой в истории всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях, направленный на укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме. Данному вопросу, безусловно, еще предстоит довольно дискуссионное обсуждение в ООН. Однако его значение как в том, что это по своей сути и содержанию первый универсальный международный договор в области борьбы с информационной преступностью[1], так и в том, что это проект конвенции нового поколения, в который включены вопросы защиты персональных данных и сбора цифровых доказательств. И представляется особенно важным закрепление в данном проекте принципа государственного суверенитета, а это существенно отличает его от вышеназванной Будапештской конвенции (2001 г.). В данном проекте, предложенном Россией, достаточно детально регламентирован порядок международного сотрудничества в сфере борьбы с информационной преступностью (включая киберпреступления, а также вопросы оказания взаимной правовой помощи по уголовным делам).

В условиях развивающихся в мире дискуссий относительно утраты позиций международного права[2], направленных на его отрицание, отмечается рост международного сотрудничества России в области МИБ в региональных и двусторонних форматах. Предпринимаются последовательные меры по укреплению потенциала многосторонних региональных объединений и интеграционных структур с участием России, включая БРИКС, ШОС, СНГ, ЕАЭС, ОДКБ.

В рамках перечисленных региональных организаций за последние двадцать лет был принят ряд значимых международных правовых актов в области МИБ[3]. Кроме

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

[2] Сегодня следует отметить, в российском паспорте научных специальностей по праву включено в международное публичное право (5.1.5) такое направление, как международное информационное право.

[3] 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.

того, принят ряд международных соглашений в области борьбы с отдельными угрозами МИБ: Шанхайская Конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г., Конвенция Шанхайской организации сотрудничества по противодействию экстремизму от 9 июня 2017 г., Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г. и др.

Представляется, что наращивание усилий по развитию международно-правовой базы сотрудничества в области МИБ в форматах региональных международных организаций и объединений является одной из наиболее перспективных тенденций, важно дальнейшее развитие двустороннего сотрудничества России в рассматриваемой сфере с конструктивно настроенными дружественными государствами. В настоящее время Россией заключено более 30 межправительственных двусторонних соглашений (с Бразилией, Вьетнамом, Индией, Китаем, Кубой, Туркменистаном и др.).

Несомненно, особое значение в условиях гибридной войны коллективного Запада против России имеет сотрудничество с Республикой Беларусь – нашим стратегическим союзником[1].

3. Противодействие угрозам нового цифрового мира и правовое обеспечение государственного суверенитета России

Способность России успешно противостоять угрозам нового цифрового мира в значительной мере зависит от состояния развития нормативной правовой базы в сфере информационной безопасности, которая определена в Стратегии национальной безопасности Российской Федерации от 2 июля 2021 г. в качестве стратегического национального приоритета. Следует отметить, что с начала XXI – информационного века был принят ряд доктрин информационной безопасности Российской Федерации (как специализированных документов стратегического планирования в данной области), сформирована обширная правовая основа обеспечения информационной безопасности[2].

[1] В 2021 г. 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 информационной безопасности в финансовой сфере. Важным шагом на пути сотрудничества наших государств в области МИБ стало утверждение в 2023 г. Концепции информационной безопасности Союзного государства Республики Беларусь и России, которая определяет основы для формирования согласованной государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также выработки мер по совершенствованию систем обеспечения информационной безопасности государств-участников Договора о создании Союзного государства.

[2] Был принят ряд важнейших законодательных актов, включая 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». Постоянно 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. был принят отдельный Феде-

В рамках последнего законодательного акта в России создана и успешно 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 критической информационной инфраструктуры.

В 2025 г. вступает в силу принятый в 2020 г. Федеральный закон № 168-ФЗ о едином федеральном регистре сведений о населении Российской Федерации и важной задачей является обеспечение надежной защиты информации, содержащейся в нем информации (Больших данных).

В связи с агрессивной санкционной кампанией Запада жизненно важное значение, как уже отмечалось, приобретает государственная политика, направленная на обеспечение технологического суверенитета, что нашло отражение в Стратегии научно-технологического развития Российской Федерации (указ от 28 февраля 2024 г. № 145) и о национальных целях развития Российской Федерации на период и на перспективу до 2030 года и на перспективу до 2036 года. И одной из приоритетных национальных целей развития определено технологическое развитие, обеспечить которое должно обеспечение технологического суверенитета государства.

На укрепление национальной информационной безопасности направлен также специальный указ Президента РФ 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» с изменениями, внесенными в июне 2024 г.), которым 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.

Обращает внимание важность закрепления в данном Указе требований (вступают в силу с 1 января 2025 г.) 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 не только импортозамещения, но 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.

ральный закон № 527, регулирующий отношения, возникающие при осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных с использованием специализированной государственной информационной системы.

Заключение

В заключение хотелось бы обратить внимание на вопрос необходимости ускорения разработки и утверждения новой национальной Доктрины информационной безопасности как ключевого документа стратегического планирования в рассматриваемой области, поскольку за последние восемь лет с момента ее принятия произошли кардинальные изменения как в области появления и усиления новых вызовов и угроз области обеспечения информационной, так и трансформации в цифровую эпоху рисков цифровой среды, которые должны находиться в фокусе внимания.

Это касается вопросов: неурегулированности юрисдикции при трансграничном информационном обмене; недостаточности международного правового регулирования в направлении обеспечения международной информационной безопасности, включая институты ответственности и соблюдения правил поведения государств в ИКТ-среде и международного сотрудничества; отсутствия единого межнационального подхода к понятийному аппарату и соотношению информационной и кибербезопасности, критериев типологизации правонарушений и механизмов ответственности; а также снижения уровня межгосударственного диалога в данной сфере, и отсутствия дипломатических решений конфликтов, важность повышения уровня доверия в информационной среде с недружественными странами.

Полагаем, на это также должен быть направлен национальный документ стратегического планирования в области информационной безопасности, поэтому так важна его модернизация в современных условиях. В нем должны быть спроецированы задачи в области обеспечения информационной безопасности, связанные с реализацией политики научно-технологического развития России, уже закрепленные в Стратегии, утвержденной указом Президента РФ от 28 февраля 2024 г. Пристального, системного анализа и точного определения требуют приоритетные задачи и векторы правового регулирования отношений, связанных с информационной безопасностью для обеспечения национального суверенитета России в технологической сфере, как способности государства создавать и применять наукоемкие технологии, критически важные для обеспечения независимости и конкурентоспособности [5], а также определить особенности безопасного и доверенного использования наиболее востребованных цифровых технологий, включая технологии ИИ.

Полагаем, что в целях укрепления системы информационной безопасности в России в качестве одного из приоритетов необходимо определить развитие с учетом новых научно-технологических подходов национальной системы правовой информации на основе разработки нового Классификатора правовых актов, а также проекта Информационного кодекса РФ, который позволит упорядочить правовое регулирование информационных отношений, в том числе и направленных на обеспечение информационной, цифровой и кибербезопасности, закрепление понятийного аппарата, системы принципов, требований [8–12].

Пристатейный библиографический список

1. *Смирнов А. А.* Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации : дис. ... докт. юрид. наук. М., 2022.

2. Информационные технологии в уголовно-правовой сфере : монография / под ред. А. И. Бастрыкина, А. Н. Савенкова. М. : ЮНИТИ-ДАНА, 2023.

3. *Наумов В. Б.* Современное правовое регулирование идентификации в России. Трансформация информационного права : монография / отв. ред. Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов. М. : Институт государства и права РАН, 2023.

4. *Петровская О. В.* Принцип достоверности в информационном праве в условиях цифровой трансформации // Мониторинг правоприменения. 2021. № 3.

5. Указ Президента РФ от 28 февраля 2024 г. № 145 «О Стратегии научно-технологического развития Российской Федерации» // СЗ РФ. 2024. № 10. Ст. 1373.

6. Цифровая трансформация: вызовы праву и векторы научных исследований : монография / под общ. ред. А. Н. Савенкова ; отв. ред. Т. А. Полякова, А. В. Минбалеев. М. : Институт государства и права РАН, 2020.

7. Трансформация информационного права : монография / отв. ред. Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов. М. : Институт государства и права РАН, 2023.

8. *Полякова Т. А., Минбалеев 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.

9. *Полякова Т. А., Минбалеев А. В., Кроткова Н. В.* Развитие доктрины российского информационного права в условиях перехода к экономике данных // Государство и право. 2023. № 9.

10. *Минбалеев А. В.* Проблемы цифрового права : учебное пособие. Саратов : Амирит, 2022.

11. *Полякова Т. А.* Влияние цифровой трансформации на развитие информационного права: тенденции, проблемы, перспективы // Мониторинг правоприменения. 2020. № 2 (35).

12. *Полякова Т. А., Минбалеев А. В., Троян Н. А.* Формирование культуры информационной безопасности граждан российской федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5.

References

1. *Smirnov A. A.* Formation of the System of Legal Support of Information and Psychological Security in the Russian Federation: Thesis for a Doctor Degree in Law Sciences. Moscow, 2022. (In Russ.)

2. *Bastrykin A. I., Savenkov A. N. (eds.).* Information Technologies in the Criminal Law Sphere: Monograph. Moscow: Unity-Dana, 2023. (In Russ.)

3. *Naumov V. B.; Poliakova T. A., Minbaleev A. V., Naumov V. B. (eds.).* Modern Legal Regulation of Identification in Russia. Transformation of Information Law: Monograph. Moscow: Institute of State and Law of the Russian Academy of Sciences, 2023. (In Russ.)

4. *Petrovskaia O. V.* The Principle of Reliability in Information Law in the Context of Digital Transformation. *Monitoring of Law Enforcement*, 2021, no. 3. (In Russ.)

5. Decree of the President of the Russian Federation of February 28, 2024 No. 145 "On the Strategy for Scientific and Technological Development of the Russian Federation". *Collection of Legislation of the Russian Federation*, 2024, no. 10, art. 1373. (In Russ.)

6. *Savenkov A. N., Poliakova T. A., Minbaleev A. V. (eds.)*. Digital Transformation: Challenges to Law and Vectors of Scientific Research: Monograph. Moscow: Institute of State and Law of the Russian Academy of Sciences, 2020. (In Russ.)

7. *Poliakova T. A., Minbaleev A. V., Naumov V. B. (eds.)*. Transformation of Information Law: Monograph. Moscow: Institute of State and Law of the Russian Academy of Sciences, 2023. (In Russ.)

8. *Poliakova T. A., Minbaleev A. V., Krotkova N. V.* Transformation of the Science of Information Law and Information Legislation: A New Stage in the Context of Scientific and Technological Development of Russia. *State and Law*, 2024, no. 9. (In Russ.)

9. *Poliakova T. A., Minbaleev A. V., Krotkova N. V.* Development of the Doctrine of Russian Information Law in the Context of the Transition to a Data Economy. *State and Law*, 2023, no. 9. (In Russ.)

10. *Minbaleev A. V.* Problems of Digital Law: Tutorial. Saratov: Amirit, 2022. (In Russ.)

11. *Poliakova T. A.* The Impact of Digital Transformation on the Development of Information Law: Trends, Problems, Prospects. *Monitoring of Law Enforcement*, 2020, no. 2 (35). (In Russ.)

12. *Poliakova T. A., Minbaleev A. V., Troian N. A.* Formation of a Culture of Information Security of Citizens of the Russian Federation in the Context of New Challenges: Public Law Problems. *State and Law*, 2023, no. 5. (In Russ.)

Сведения об авторе:

Т. А. Полякова – доктор юридических наук, профессор, заслуженный юрист РФ.

Information about the author:

T. A. Polyakova – Doctor of Law, Professor, Honored Lawyer of the Russian Federation.

Статья поступила в редакцию 11.11.2024; одобрена после рецензирования 09.12.2024; принята к публикации 16.12.2024.

The article was submitted to the editorial office 11.11.2024; approved after reviewing 09.12.2024; accepted for publication 16.12.2024.