
ИНФОРМАЦИОННОЕ ПРАВО И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 34



СОВРЕМЕННЫЕ ПРИОРИТЕТЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ПРАВА: ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ РОССИИ

© 2025 г. Т. А. Полякова^{1, *}, А. В. Минбалеев^{1, 2, **}, В. Б. Наумов^{1, 2, ***}

¹Институт государства и права Российской академии наук, г. Москва

²Московский государственный юридический университет им. О. Е. Кутафина (МГЮА)

*E-mail: polyakova_ta@mail.ru

**E-mail: alexmin@bk.ru

***E-mail: nau@russianlaw.net

Поступила в редакцию 06.01.2025 г.

Аннотация. В статье анализируются историографические аспекты развития нового научного направления в Институте государства и права Российской академии наук и научной школы информационного права, а также развитие исследований правовых проблем обеспечения национальной и международной информационной безопасности. Исследуются приоритеты развития информационного права в условиях новых задач, расширения правового измерения и целей развития России в свете обеспечения ее национального суверенитета в информационной сфере, кибербезопасности и противодействия киберпреступности. Все это обусловлено необходимостью решения стратегических задач обеспечения национальной и международной информационной безопасности как одного из приоритетов государственной политики в информационной сфере. В связи с этим отмечено значение информационно-правового обеспечения нового национального проекта «Экономика данных и цифровая трансформация государства».

Развитие доктрины российского информационного права как публично-правовой (государственно-правовой) отрасли (права, законодательства и науки) сегодня детерминировано целями развития России, необходимостью правового обеспечения национального суверенитета в информационной сфере в условиях цифровой трансформации. Информационное право рассматривается авторами как базовая отрасль для развития правового регулирования новых информационных отношений, информационных (цифровых) пространств, а также противодействия современным информационным вызовам и угрозам государству, обществу и гражданам.

Исследованы особенности и проблемы правового обеспечения информационного суверенитета и информационной безопасности Российской Федерации. Обосновано значение кодификации информационного законодательства и рассмотрены проблемы, связанные с разработкой кодексов,

необходимых для упорядочения информационного законодательства, в том числе в целях достижения информационного суверенитета Российской Федерации, развития экономики данных и цифровой трансформации государства.

На основе анализа состояния и развития науки информационного права в Институте государства и права РАН обосновывается роль сектора информационного права и международной информационной безопасности в развитии теоретической модели Информационного кодекса и оценке проблем разработки Цифрового кодекса.

Ключевые слова: информационное право, кибербезопасность, кодификация информационного законодательства, информационная безопасность, информационный суверенитет, правовое обеспечение информационной безопасности, Цифровой кодекс Российской Федерации, цифровая трансформация государства, экономика данных.

Цитирование: Полякова Т.А., Минбалеев А.В., Наумов В.Б. (2025). Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. 2025. № 1. С. 160–173.

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

DOI: 10.31857/S1026945225010148

MODERN PRIORITIES FOR THE DEVELOPMENT OF INFORMATION LAW: LEGAL SUPPORT OF STATE SOVEREIGNTY AND INFORMATION SECURITY IN THE INFORMATION SPACE OF RUSSIA

© 2025 T. A. Polyakova^{1, *}, A. V. Minbaleev^{1, 2, **}, V. B. Naumov^{1, 2, ***}

¹*Institute of State and Law of the Russian Academy of Sciences, Moscow*

²*Kutafin Moscow State Law University (MSAL)*

*E-mail: polyakova_ta@mail.ru

**E-mail: alexmin@bk.ru

***E-mail: nau@russianlaw.net

Received 06.01.2025

Abstract. The article analyzes the historiographical aspects of the development of a new scientific field at the Institute of State and Law of the Russian Academy of Sciences and the Scientific School of Information Law, as well as the development of research on legal issues of national and international information security. The priorities of the development of Information Law in the context of new challenges, the expansion of the legal dimension and the goals of Russia's development in the light of ensuring its national sovereignty in the information sphere, cybersecurity and countering cybercrime are investigated. All this is conditioned by the need to solve strategic tasks of ensuring national and international information security as one of the priorities of state policy in the information sphere. In this regard, the importance of information and legal support for the new national project "Data Economics and Digital Transformation of the State" was noted.

The development of the doctrine of Russian Information Law as a public-law (state-legal) branch (law, legislation and science) today is determined by the goals of Russia's development, the need for legal support for national sovereignty in the information sphere in the context of digital transformation. Information Law is considered by the authors as a basic branch for the development of legal regulation of new information relations, information (digital) spaces, as well as countering modern information challenges and threats to the state, society and citizens. The features and problems of legal support of information sovereignty and information security of the Russian Federation are investigated. The importance of codification of information legislation is substantiated and the problems associated with the development of codes necessary to streamline information legislation, including in order to achieve information sovereignty of the Russian Federation, the development of the data economy and the digital transformation of the state, are considered.

Based on the analysis of the state and development of the science of Information Law at the Institute of State and Law of the Russian Academy of Sciences, the role of the Information Law and international information security sector in the development of the theoretical model of the Information Code and the assessment of the problems of developing a Digital Code is substantiated.

Key words: Information Law, cybersecurity, codification of information legislation, information security, information sovereignty, legal support of information security, Digital Code of the Russian Federation, digital transformation of the state, data economy.

For citation: Polyakova, T.A., Minbaleev, A.V., Naumov, V.B. (2025). Modern priorities for the development of Information Law: legal support of state sovereignty and information security in the Information Space of Russia // *Gosudarstvo i pravo*=State and Law, No. 1, pp. 160–173.

The article was prepared within the framework of the State Assignment FMUZ-2024-0035 “Ensuring digital sovereignty and information security by legal means”.

*К 100-летию Института государства и права
Российской академии наук*

Введение

Информационное общество и цифровая экономика во многом определили позиции информационного права не просто как нового научного направления, но и инновационной отрасли, которая продолжает активно развиваться в условиях цифровой трансформации государства и права, формирования экономики данных, а также решения стратегических задач по обеспечению национального суверенитета в информационной сфере и информационной безопасности, в том числе кибербезопасности в цифровой среде.

Развитие системы информационных, а также цифровых отношений связывают с появлением новых субъектов и объектов информационного права, развитием новых наукоемких технологий, новых информационных пространств и т.д., а также с необходимостью обеспечения состояния защищенности интересов государства, общества и граждан от новых вызовов и угроз в глобальном информационном пространстве. Эти проблемы заслуживают внимания не только со стороны государства при формировании его политики, но и широкого научного сообщества, практиков. Научные исследования подтверждают необходимость ускоренного развития российской доктрины информационного права, информационного законодательства, а также международных правовых актов, направленных на регулирование информационно-коммуникационной среды (далее — ИКТ-среда).

Роль научных исследований в этой области, безусловно, возрастает в условиях происходящих в мире изменений перехода к многополярности, роста киберпреступности. Возрастает также значение развития системы международной информационной безопасности и продвижение связанных с этим российских инициатив и проектов в ООН.

Стратегический характер имеют задачи обеспечения государственного суверенитета в условиях цифровой трансформации; обеспечения безопасности в киберпространстве. Необходимо обеспечение культурного суверенитета, включая защиту русского языка, и культурных ценностей,

информационно-психологической безопасности, развитие культуры информационной безопасности, формирование среды доверия и мер по обеспечению защиты цифровых данных при их обороте. Эта тема заслуживает самостоятельных исследований. Все эти и иные вопросы являются предметом информационно-правовых исследований¹.

При активном развитии фундаментальной юридической науки и укрупнении научных юридических специальностей, включении информационного права в публично-правовые (государственно-правовые) науки информационное право подвержено определенной трансформации в связи с активизацией процессов цифровизации, что обуславливает развитие соответствующих доктринальных положений информационного права, необходимых для формирования государственной политики.

Как справедливо отмечает член-корр. РАН А.Н. Савенков, «в условиях... усиливающейся динамики развития информационного общества, “электронного государства”, цифровой экономики, роста вызовов и угроз информационной безопасности особую роль играет формирование и реализация государственной политики, направленной на учет современных информационных тенденций развития всех сфер жизни общества и государства, выработку научно обоснованных, выверенных, взвешенных подходов регулирования новых информационных отношений»².

Информационно-правовое обеспечение национального суверенитета информационной безопасности в условиях цифровой трансформации государства

Одной из ключевых задач и функций государства является обеспечение и защита национального суверенитета в информационном пространстве. В условиях возрастающих вызовов и угроз,

¹ См.: Polyakova T.A., Naumov V.B., Minbaleev A.V. Trust in the law during the digital transformation // *Государство и право*. 2022. № 11. С. 139–147; Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Основные тенденции и проблемы развития науки информационного права // *Государство и право*. 2022. № 9. С. 94–104.

² Савенков А.Н. Философия права и становление российского государства-цивилизации. М., 2024. С. 64.

активизации противоправных действий различных субъектов деструктивного характера³, направленных на нарушение защищенности интересов государства, общества и каждого гражданина, пристального внимания заслуживают вопросы обеспечения национальной и международной информационной безопасности. Возрастает значение одного из базовых принципов международного права, требующего доктринального развития, расширения в информационном пространстве. Это неоднократно отмечалось Президентом РФ, особенно роль технологического суверенитета как стратегической задачи, связанной с обеспечением реализации политики импортозамещения, одной из ключевых для обеспечения киберстабильности.

Кроме того, активно обсуждаются различные вопросы, касающиеся цифрового суверенитета, сетевого, научно-технологического и многих других видов суверенитета⁴. Но все это связано с системным правовым обеспечением национальной и международной информационной безопасности как научного направления⁵. Рост киберпреступности как динамично развивающаяся тенденция нашего времени, особенно в условиях специальной военной операции, требует развития теории суверенитета государства в информационном пространстве, включая обеспечение цифрового суверенитета и киберсуверенитета (проблем атрибуции в информационном пространстве при совершении противоправных действий). Необходимым условием обеспечения информационного национального суверенитета являются: противодействие распространению фейков, защита русского языка и культурного суверенитета, формирование среды доверия и соблюдение конфиденциальности цифровых данных.

Характер и виды суверенитета государства в информационной сфере требуют комплексных научных исследований, поскольку носят дискуссионный, межотраслевой характер.

Исследованиям вопросов суверенитета государств или государственного суверенитета посвящены, например, работы теоретиков права.

³ См.: Информационные технологии в уголовно-правовой сфере / под ред. А.И. Бастрыкина, А.Н. Савенкова. М., 2023.

⁴ См.: Полякова Т.А., Смирнов А.А. Правовое обеспечение международной информационной безопасности: приоритеты для Союзного государства // Право.ру. 2023. № 5(85). С. 84–92; 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. С. 131–144; и др.

⁵ См.: 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. С. 166–179.

Так, А.Б. Венгеров, один из первых теоретиков права, признавших наличие информационных отношений, рассматривал государственный суверенитет как одну из важнейших черт государства, которая заключается в верховенстве и независимости от какой-либо иной власти, «обладании правом и возможностью осуществлять внутреннюю и внешнюю политику от имени всего общества внутри и вне страны»⁶.

Вместе с тем особую природу этого свойства государства Н.А. Ушаков отмечал так: с позиции международного права «суверенитет представляет собой необходимое политико-юридическое свойство всякого государства, неразрывно связанное с его особой природой»⁷. Суверенитет связывают как с понятием государственной власти, так и классически определяют его как «лишь определенное ее свойство, в силу которого она является высшей и независимой властью»⁸. Цифровая трансформация, несомненно, существенно влияет на правовую систему, определяет необходимость существенных изменений⁹.

Полагаем, что заслуживает особого внимания позиция Президента Российской ассоциации международного права А.Я. Капустина, который на основе анализа понятия «суверенитет государства» и приведенной им классификации подходов в международно-правовой доктрине оценивает правовое измерение и роль суверенитета в киберпространстве¹⁰. Кроме того, представляет научный интерес системный анализ различных подходов к защите суверенитета в информационном пространстве, проведенный А.А. Ефремовым, рассматривающим государственный суверенитет в информационном пространстве как юридическое свойство (признак) государства, являющегося особым субъектом информационно-правовых отношений, который осуществляет их правовое регулирование не только в пределах своей территории (внутригосударственное информационное пространство), но и экстерриториально при

⁶ Венгеров А.Б. Теория государства и права. М., 2005. С. 92.

⁷ Ушаков Н.А. Суверенитет в современном международном праве. М., 1963. С. 23.

⁸ Палиенко Н.И. Суверенитет. Историческое развитие идеи суверенитета и ее правовое значение. Ярославль, 1903. С. 438, 439.

⁹ Увеличение объемов правовой информации, цифровизации правового управления, использование искусственного интеллекта во всех сферах деятельности и обслуживания не только модернизируют всю систему права, но также вызывают новые общественные отношения, в значительной степени касающиеся, например, правового регулирования в области информационной безопасности.

¹⁰ См.: Капустин А.Я. Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. 2022. Т. 18. № 6. С. 99–108.

участии в международно-правовом регулировании. В связи с этим им предложено в информационно-правовой механизм обеспечения государственного суверенитета включать системы организационных, нормативно-функциональных и инструментально-процедурных элементов, осуществляющих регулирующее влияние на общественные отношения¹¹.

Исследования в данной области показывают также, что понятие суверенитета наиболее часто принято определять как «свойство государства, предполагающее верховенство государственной власти на его территории и независимость в международных отношениях»¹². Хотя в нормативных правовых актах термин «суверенитет» используется достаточно широко (к примеру, в Декларации о государственном суверенитете 1990 г.)¹³. При этом обращает внимание, что в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы в разделе, посвященном информационной безопасности, указано, что основной целью «является укрепление суверенитета России в условиях новых вызовов, угроз и рисков»¹⁴. В качестве одной из задач развития военной организации еще в Военной доктрине Российской Федерации¹⁵ также определено обеспечение суверенитета, как и в других актах стратегического планирования.

Анализ показывает, что сегодня в условиях цифровой трансформации необходимо развитие доктринального понятия в связи с развитием информационного (кибер)пространства, реализации стратегических задач обеспечения национальной безопасности, включая и информационную безопасность, как состояния защищенности национальных интересов России для защиты конституционных ценностей в целях обеспечения суверенитета Российской Федерации в информационном пространстве, включая технологический суверенитет, социально-экономическое развитие и достижение гражданского согласия. Система правового

обеспечения национальной информационной безопасности Российской Федерации определяется сегодня многовекторностью общественных отношений в информационной сфере.

Следует признать, что многие новые категории, концепты, необходимые для правового регулирования, пока не имеют однозначных юридических дефиниций. К ним можно отнести и понятие «цифровой суверенитет», которое при значительном расширении сферы его использования до сих пор не обрело необходимой правовой определенности. Это относится и к таким понятиям, как «противодействие кибератакам», «киберпреступность», «киберстабильность», «атрибуция в информационном пространстве» и многим другим, имеющим стратегическое значение как на национальном, так и международном уровне для противодействия информационно-психологическим воздействиям террористического и экстремистского характера, а также деструктивной политике государств коллективного Запада, направленной на разрушение традиционных духовно-нравственных и культурных ценностей, попыткам компьютерных атак на российские информационные ресурсы и цифровую среду.

Требует отдельного анализа соотношение понятия государственного суверенитета, концепта «цифровой суверенитет», а также места и роли культурного суверенитета с учетом того обстоятельства, что огромное количество граждан давно стали пользователями информационного пространства и различных цифровых сервисов и осуществляют доступ к информации и знаниям преимущественно в цифровой форме.

Отдельное значение для системы различных взаимоувязанных понятий суверенитетов приобретает глубокая междисциплинарная оценка роли доминирующих в цифровом пространстве цифровых платформ и сервисов, по большей части иностранных, и степень их участия в происходящем сейчас в мире геополитическом противостоянии.

Недружественные по отношению к Российской Федерации государства предпринимают попытки использования своего технологического доминирования, направленного на сдерживание или подчинение цифрового развития других государств, и «внешней» цензуры в информационном пространстве. В целях противодействия таким угрозам несомненно значение научного обоснования развития системы правового обеспечения национального суверенитета в информационной сфере (цифрового, технологического, культурного, как связанного с информацией и знаниями, и т.д.), принятия комплекса мер для усиления организационной, технологической и правовой защищенности в условиях цифровой трансформации. Это касается идентификации объектов и субъектов в цифровой среде,

¹¹ См.: Ефремов А.А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации: дис. ... д-ра юрид. наук. М., 2021; *Его же*. Защита государственного суверенитета Российской Федерации в информационном пространстве. М., 2017.

¹² Философия права. Словарь. 2-е изд., дораб. и доп. / под ред. и сост. В.Н. Жуков. М., 2021. С. 704.

¹³ В Конституции РФ, а также практически во всех документах стратегического планирования — Стратегии национальной безопасности Российской Федерации (2021 г.), в Доктрине информационной безопасности Российской Федерации (утв. Президентом РФ в 2016 г.), в Основах государственной политики в области международной информационной безопасности (2021 г.).

¹⁴ См.: Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20, ст. 2901.

¹⁵ См.: Военная доктрина Российской Федерации (утв. Президентом РФ 25.12.2014 № Пр-2976) // Росс. газ. 2014. 30 дек.

политики усиления защиты каналов связи, обеспечения конфиденциальности информации, а также достоверности социально значимой информации, приобретения необходимых знаний, а также воспитания культуры информационной безопасности и «цифровой гигиены» и т.д.

Однако для эффективного противодействия таким информационным вызовам в условиях трансграничности необходима консолидация усилий всего мирового сообщества и активизация эффективного международного сотрудничества в области международной информационной безопасности. Сегодня многие вызовы и угрозы имеют глобальный и трансграничный характер, поэтому нельзя отрицать значение правовых норм и общепризнанных принципов международного права в ИКТ-среде. Одним из приоритетов внешней политики Российской Федерации в информационном пространстве закономерно является усиление интеграции и взаимодействия именно в форматах региональных объединений (ШОС, БРИКС, СНГ, ОДКБ и Союзного государства Республики Беларусь и Российской Федерации) для эффективного решения противодействия указанным угрозам в информационном пространстве. Российская позиция относительно развития системы международной информационной безопасности отражена в проекте Конвенции об обеспечении международной информационной безопасности, внесенном в ООН в 2023 г., в котором заложен принцип суверенного равенства государств и невмешательства во внутренние дела (в том числе для наращивания сил информационной безопасности).

В фокусе внимания мирового сообщества находится важное событие, связанное с принятием 24 декабря 2024 г. Генеральной Ассамблеей ООН универсальной Конвенции, направленной на противодействие киберпреступности. Впервые в мировой истории был одобрен проект универсальной международной Конвенции о противодействии использованию ИКТ в преступных целях. Эту Конвенцию по праву можно отнести к международным актам нового поколения не только потому, что это первый более чем за 20 лет XXI в. международный правовой документ ООН в виде универсальной конвенции, но и в связи с тем, что это новый правовой инструмент для борьбы с растущей угрозой киберпреступности, противодействия новому противоправному явлению в киберпространстве, представляющему угрозу и национальному суверенитету¹⁶, в который включены вопросы защиты

персональных данных и сбора цифровых доказательств. Особенно важно закрепление в данном проекте принципа государственного суверенитета, что его значительно отличает от европейской, т.н. Будапештской конвенции (2001), которую Российская Федерация не подписала. В Конвенции детально регламентированы вопросы международного сотрудничества в сфере борьбы с информационной преступностью (включая киберпреступления), оказание взаимной правовой помощи по уголовным делам, сбора электронных доказательств, защиты детей от сексуального насилия, совершаемого с использованием информационных технологий, помощи пострадавшим (жертвам) киберпреступлений. Важно, что принятая Конвенция ООН содержит требования к государствам о разработке мер по снижению рисков и угроз киберпреступности и т.д.¹⁷

В связи с активизацией в последнее время дискуссий относительно утраты роли международного права в мировом сообществе следует обратить внимание, что в действующем российском паспорте научных специальностей по праву в международное публичное право (5.1.5) впервые включено такое научное направление, как международное информационное право. Кроме того, несмотря ни на какие санкции в отношении России, отмечается рост международного сотрудничества Российской Федерации в области международной информационной безопасности в региональных и двусторонних форматах, в том числе по укреплению потенциала многосторонних региональных объединений и интеграционных структур с участием Российской Федерации, включая БРИКС, ШОС, СНГ, ЕАЭС, ОДКБ¹⁸.

Дальнейшая консолидация усилий заинтересованного международного сообщества по развитию международно-правовой базы сотрудничества в области международной информационной безопасности в форматах региональных международных организаций и объединений — задача стратегического характера. Не случайно Российской Федерацией на двустороннем уровне заключено более 30 межправительственных соглашений с Бразилией, Вьетнамом, Индией, КНР, Кубой, Туркменистаном и рядом других государств.

¹⁷ См.: там же.

¹⁸ За последние 20 лет был принят ряд значимых международно-правовых актов в области международной информационной безопасности, включая Соглашение между правительствами государств — членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 г., Соглашение о сотрудничестве государств — участников СНГ в области обеспечения информационной безопасности от 20.11.2013 г., Соглашение о сотрудничестве государств — членов ОДКБ в области обеспечения информационной безопасности от 30.11.2017 г.

¹⁶ Следует отметить, что указанный проект, внесенный в ООН Российской Федерацией совместно с рядом государств, был одобрен в августе 2024 г. специальным комитетом ООН (см.: URL: <https://news.un.org/ru/story/2024/12/1459716> (дата обращения: 24.12.2024)).

В год 25-летия создания Союзного государства Республики Беларусь и Российской Федерации нельзя не отметить значение сотрудничества России и Беларуси¹⁹. Значительным шагом на пути нашего сотрудничества в области международной информационной безопасности стало утверждение в 2023 г. Концепции информационной безопасности Союзного государства Республики Беларусь и Российской Федерации²⁰.

В последнее время в российской государственной политике отмечается усиление внимания к правовому регулированию в области обеспечения информационной безопасности как одному из стратегических национальных приоритетов, направленных на противодействие вызовам и угрозам в этой сфере в соответствии со Стратегией национальной безопасности Российской Федерации (2021 г.).

Так, особо следует отметить развитие российского законодательства в области защиты информации ограниченного доступа (с февраля 2024 г. вступила в силу новая редакция Федерального закона «О государственной тайне»)²¹. С 1 января 2025 г. начинает действовать Федеральный закон от 8 июня 2020 г. № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации», в котором интегрируется совокупность сведений о населении Российской Федерации, содержащихся в государственных информационных системах органов государственной власти Российской Федерации, органов управления государственными внебюджетными фондами. В связи с этим важной задачей является обеспечение защиты информации, содержащейся в данном федеральном регистре, ведение которого осуществляется ФНС России.

¹⁹ 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.

²⁰ Концепция 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. В документе определены основные угрозы информационной безопасности Союзного государства, общие принципы, цель и задачи обеспечения информационной безопасности Союзного государства.

²¹ См. более подр.: Полякова Т.А., Камалова Г.Г. Государственная тайна как институт правового обеспечения национального суверенитета и безопасности Российской Федерации // Государство и право. 2024. № 7. С. 174—183.

Ключевое значение имеет реализация государственной политики в сфере технологического и инновационного развития Российской Федерации. Основными стратегическими документами в этой области являются Стратегия научно-технологического развития Российской Федерации (утв. Указом Президента РФ от 28.02.2024 г.), а также Концепция технологического развития на период до 2030 года (утв. распоряжением Правительства РФ от 20.05.2023 № 1315-Р), которая определяет вызовы, принципы и цели технологического развития на период до 2030 г. в соответствии с национальными целями развития Российской Федерации²².

Указом Президента РФ от 01.05.2022 г. № 250 (с изм., внесенными в июне 2024 г.) «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»²³ 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 информационной безопасности либо возложение данных функций на существующее структурное подразделение²⁴. С 1 января 2025 г. вступили в силу закрепленные в данном Указе требования относительно запрета на использование средств защиты информации, «странами происхождения которых являются недружественные иностранные государства либо находящиеся под их юрисдикцией производители». Указанная правовая норма также направлена на обеспечение технологического суверенитета²⁵.

С января 2025 г. в Российской Федерации начинают действовать новые национальные проекты, которые в целом прямо или опосредованно направлены на обеспечение национального суверенитета. Одним из ключевых направлений развития

²² Создана Межведомственная комиссия по технологическому суверенитету и структурной адаптации экономики Российской Федерации. В структуре Совета Безопасности Российской Федерации также функционирует Межведомственная комиссия по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации.

²³ См.: СЗ РФ. 2022. № 18, ст. 3058.

²⁴ Ключевой характер имеют также положения об осуществлении мониторинга защищенности информационных ресурсов, принадлежащих таким органам (организациям), порядок которого регламентирован приказом ФСБ России.

²⁵ В 2024 г. этот запрет был распространен и в отношении иностранных сервисов (работ, услуг) по обеспечению информационной безопасности. Этот сложный, но непростой шаг необходимо сделать для укрепления технологического суверенитета нашей страны в области информационной безопасности.

информационного права и его доктрины является переход к новым приоритетным наукоемким технологиям, а также начало реализации национального проекта «Экономика данных и цифровая трансформация государства». Анализ паспортов новых национальных проектов показывает, что реализация поставленных задач во многом связана с необходимостью развития доктрины информационного права и системы информационного законодательства.

Цифровой кодекс Российской Федерации как вызов информационному праву

В научном сообществе продолжают дискуссии относительно целесообразности (возможности) разработки и принятия в ближайшее время Цифрового кодекса РФ, хотя позиция Правительства РФ нашла отражение в соответствующем поручении о его разработке. Кодификация законодательства процесс сложный и долговременный, в рамках которого происходит не только обсуждение, моделирование проекта кодифицированного акта, но и прогнозирование последствий его принятия и дальнейшего существования. Позиция авторов данной статьи относительно перспектив разработки Цифрового кодекса нашла отражение в статье «К вопросу о кодификации информационного законодательства в условиях цифровой трансформации»²⁶. Продолжающиеся обсуждения и попытки осмысления в различных форматах этих вопросов не позволяют сегодня рассматривать формирующееся цифровое законодательство («Цифровой кодекс») как самостоятельную отрасль законодательства, поскольку именно в рамках информационного законодательства в настоящее время происходит развитие правового регулирования цифровых процессов. Несмотря на то что большинство информационных процессов переводится в цифровой формат, правовое регулирование в цифровой сфере есть и будет частью информационного права. Хотя высказываются позиции об отождествлении информационного и цифрового права, полагаем, что это методологическая и предметная ошибка, поскольку информационное право не ограничивается тем или иным форматом существования информации, а включает правовое регулирование информации независимо от конкретного носителя, а также устанавливает особенности правового регулирования той или иной информации в любой форме ее существования.

В связи с этим очевидно, что априори Цифровой кодекс не может включить (систематизировать) все

информационное законодательство, охватывающее правовое регулирование широкого круга общественных отношений, в том числе связанных с информацией в неэлектронной форме. Таким образом, обоснованным представляется вывод о том, что Цифровой кодекс ни в коей мере не может заменить Информационный. Представляется, что при попытке реализации такого подхода Цифровой кодекс буквально «утонул» бы в огромном объеме правовых норм, регулирующих отдельные виды информации. Вместе с тем информационное право имеет значительный потенциал для своего развития, поскольку цифровой формат также не является конечной стадией эволюционного развития форм существования информации. Современные процессы эволюции наукоемких технологий позволяют прогнозировать, что наука приближается к реализации возможностей использования света (фотоники) и внедрения квантовых технологий²⁷, биоинформационных технологий, которые могут использовать еще скрытые возможности человеческого организма, в том числе телепортационные пространственно-временные возможности передачи информации. Исследования показывают, что быстро развиваются и иные формы существования и передачи информации в киберпространстве.

В связи с этим вполне возможно, что вслед за попытками выделения в качестве отрасли права интернет-права, телекоммуникационного, электронного права, сетевого, цифрового права²⁸ поднимутся вопросы о самостоятельности квантового, биоинформационного, телепортационного и других отраслей права. В лучшем случае следует считать указанные конструкции подотраслями информационного права либо межотраслевыми категориями для нескольких отраслей права. В связи с этим концептуально видится, что фундаментальный характер имеет разработка теоретической модели Информационного кодекса, который мог бы установить общие подходы регулирования информационных отношений независимо от формы.

Задачи нормативного правового обеспечения происходящих процессов цифровизации связываются, вероятно, с разработкой Цифрового кодекса

²⁷ См.: Полякова Т.А., Минбалева А.В., Наумов В.Б. Правовое регулирование квантовых коммуникаций в России и в мире // Государство и право. 2022. № 5. С. 104–114; Минбалева А.В., Берестнев М.А., Евсиков К.С. Обеспечение информационной безопасности оборудования добывающей промышленности в квантовую эпоху // Известия Тульского гос. ун-та. Науки о Земле. 2023. № 1. С. 567–584.

²⁸ См., напр.: Малько А.В., Афанасьев С.Ф., Борисова В.Ф., Кроткова Н.В. Обзор методологического семинара на тему «Цифровое право: методология исследования» (18 апреля 2019 г., Саратовская государственная юридическая академия, Саратовский филиал Института государства и права РАН) // Государство и право. 2019. № 8. С. 122–128.

²⁶ Полякова Т.А., Минбалева А.В., Наумов В.Б. К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // Государство и право. 2024. № 1. С. 81–91.

в надежде, что этот формат позволит оперативно их решить. Однако следует признать, что нормативно-правовая составляющая программы «Цифровая экономика» явно не достигла всех поставленных целей и задач. Множество принятых, но, как показывает практика применения, недостаточно хорошо проработанных с позиции оценки регуляторного воздействия правовых актов, уже сегодня показывает их недостаточную эффективность. В связи с этим решение большинства сложных задач в рамках единого цифрового кодифицированного акта возможно было бы удобнее и позволило бы урегулировать ряд цифровых процессов, обеспечить коммерциализацию данных, в том числе персональных. Следует отметить, что представителями крупного бизнеса в ИТ-секторе принятие непосредственно Цифрового кодекса после неудачной попытки разработки и принятия Информационно-коммуникационного кодекса рассматривается с определенной настороженностью.

Обсуждение разработки Цифрового кодекса РФ продолжается, но у него появляется все больше противников, которые видят серьезную опасность в том, что поспешное его принятие может привести к созданию нормативных положений, сложных для правоприменения, регулирующих технологические процессы, создающие проблемы единообразия на практике, связанные с непониманием многих технологических процессов при их закреплении в Цифровом кодексе. Эти проблемы касаются и разработки понятийного информационно-правового аппарата, который по-разному может интерпретировать значения многих технических и технологических терминов. К тому же указанный понятийный аппарат практически не подвергается переработке и не выстраивается иерархически с учетом дефиниций информационного права, а в определенной части заимствуется из нормативных актов технического регулирования.

Проблемы разработки Цифрового кодекса также связаны с тем, что действующее законодательство пока не содержит целого ряда правовых норм, которые нужны как основа такого кодификационного процесса. Принятие таких норм (о цифровых сервисах, платформах, услугах, профилировании, цифровых пространствах и др.) в значительной степени ограничивается интересами крупных цифровых гигантов в отсутствии национального цифрового законодательства, обеспечивающего гарантии прав граждан при их взаимодействии с глобальной цифровой средой. Вероятно им выгоднее, чтобы отношения с пользователями регулировались на основе пользовательских соглашений и платформенного права, на базе которого такие соглашения и готовятся, поскольку это позволяет заранее спрогнозировать действия пользователей в цифровой среде, принять меры по их ограничению и фактическому принуждению к отказу от использования тех или иных инструментов

защиты (например, установление юрисдикции определенного штата США, обязательного предварительного урегулирования спора и др.).

В то же время продвигаемые транснациональными корпорациями идеи невозможности правового регулирования цифровых процессов создают риски дополнительных административных барьеров, необходимости и приоритетности этического регулирования технологий над правовым регулированием и т.д.

Невзирая на отсутствие ряда базовых правовых норм для регулирования процессов цифровизации, имеется обширный нормативно-правовой массив управления данными, развития инфраструктуры и связи, а также, что представляется особенно важным в данной статье отметить, касающихся обеспечения информационной безопасности²⁹.

Несмотря на отсутствие теоретико-методологического обоснования и указанные выше обстоятельства, сегодня продолжают предлагаться различные подходы к модели Цифрового кодекса и его предмету.

1. Объектный подход, при котором Цифровой кодекс рассматривается как основа для регулирования совокупности объектов цифровой среды, в том числе цифровых данных, цифровых технологий (с учетом их специфики).

2. Сервисный подход, при котором акцент делается на цифровые сервисы и услуги, а базовый постулат — отсутствие регулирования контента.

3. Комплексный подход: правовая характеристика цифровых объектов, основные требования к цифровым платформам, сервисам, услугам, телекоммуникациям, а также частичное регулирование контента с отсылкой к специальным законам, регулирующим отдельные объекты, процессы.

Однако во всех случаях спорным является ключевой вопрос о предмете Цифрового кодекса — информационных отношениях³⁰, и при этом он фактически выступает формой кодифицированного регулирования информационных отношений в цифровой среде. И это еще больше подтверждает объективную невозможность выделения цифрового права как самостоятельной отрасли, отличной от информационного права.

²⁹ К ним можно отнести базовые законы об информации, защите персональных данных, связи, электронной подписи, экспериментальных правовых режимах и целый ряд ведомственных подзаконных актов, принятых в целях их реализации.

³⁰ Это отношения, которые возникают в связи с существованием и использованием той или иной информации в цифровой среде. Чаще всего это данные, хотя и цифровые сообщения также активно развиваются в рамках развертывания различных способов передачи информации в цифровой среде.

**Роль сектора информационного права
и международной информационной
безопасности Института государства и права
Российской академии наук в развитии
доктрины информационного права**

Проведенное исследование проблем, рассмотренных авторами в настоящей статье, свидетельствует об их актуальности и подтверждает необходимость развития теории информационного права и продолжения в сложившихся реалиях предметных исследований правового обеспечения национального (государственного) суверенитета во всех его проявлениях, включая правовое обеспечение информационной безопасности.

Отмеченные проблемы кодификации информационного и цифрового законодательства (включая цифровое), на наш взгляд, требуют внимания и обращения к гносеологическим вопросам (корням) развития научного направления информационного права в Институте государства и права Российской академии наук. Это представляется особенно важным в год его столетия. Официально признание этого научного направления в Институте связывают с его выделением из административного права, которое произошло в конце 90-х годов XX в.

По сути, это связано не только с созданием сектора информационного права, но и началом формирования академической научной школы информационного права под руководством И.Л. Бачило³¹. В период с 2000 по 2013 г. были заложены основы правового регулирования информационных отношений и концепции кодификации информационного законодательства³². Научные исследования сектора информационного права позволили выявить ряд закономерностей и обосновать выводы, положенные в основу развития доктрины современного информационного права: разработать подход к классификации проблем информатизации как процесса создания и использования продукции информационных технологий, формирования информационных ресурсов, освоения и использования средств коммуникаций. Был обоснован научный подход к комплексному правовому регулированию составляющих элементов информационной инфраструктуры, социально значимых явлений и отношений, что позволило выработать концепцию правового регулирования информатизации и выстроить основы развития информационного законодательства, включая

правовое регулирование обеспечения информационной безопасности.

Работа сектора информационного права в соответствии с направлениями исследования правовых проблем развития информационного общества была направлена, прежде всего, на упорядочение системы российского информационного законодательства. Не утрачивает своего значения и актуальности исследование проблем состояния информационного законодательства, его систематизации и направлений развития с учетом социально-экономических и политических процессов развития Российской Федерации, а также глобальных тенденций эволюции мирового информационного пространства. С 2015 г. сектор продолжает развиваться. В этот период выделено в отдельное направление исследование проблем правового обеспечения информационной безопасности с учетом вызовов и угроз в глобальном информационном обществе, а также включая вопросы развития системы международной информационной безопасности³³. С 2018 г. сектор (переименован в сектор информационного права и международной информационной безопасности) активно участвовал в проведении научных мероприятий и исследований в этой области по грантам РФФИ, а также государственным заданиям по указанной тематике, а ныне принимает активное участие в экспертной деятельности по вопросам информационного права и информационной безопасности, искусственного интеллекта³⁴. Опубликована серия научных статей по проблемам правового обеспечения международной информационной безопасности³⁵.

Среди проблем научно-технологического развития выделяются системные проблемы правового регулирования обеспечения информационной безопасности, противодействия новым вызовам

³³ См.: Бачило И.Л., Полякова Т.А., Демьянец М.В. и др. Об основных направлениях информационного права за 2000–2015 гг. // Государство и право. 2017. № 1. С. 79.

³⁴ Сектором осуществляется подготовка материалов к заседаниям секции по проблемам информационной безопасности Научного совета при Совете Безопасности Российской Федерации, а также Национальной ассоциации международной информационной безопасности и Научно-консультативного совета при Антитеррористическом центре государств – участников СНГ. Сотрудники сектора участвовали в проведении фундаментальной научно-исследовательской работы на тему «Проблема применения норм, правил и принципов ответственного поведения государств в ИКТ-среде», проведенной под эгидой Национальной ассоциации международной информационной безопасности.

³⁵ См.: Полякова Т.А., Зиновьева Е.С., Смирнов А.А. Международная информационная безопасность: универсальное правовое измерение // Государство и право. 2023. № 12. С. 139–149; Полякова Т.А., Смирнов А.А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Росс. юрид. журнал. 2022. № 3. С. 7–15.

³¹ См.: Троян Н.А., Полякова Т.А., Кроткова Н.В. Бачило Илларию Лаврентьевну // Портал. Большая российская энциклопедия. URL: <https://bigenc.ru/c/bachilo-illariia-lavrent-evna-36a9bd> (дата обращения: 10.11.2024).

³² См.: Концепция Информационного кодекса Российской Федерации / под ред. И.Л. Бачило. М., 2014. С. 9.

и угрозам³⁶. Сектором была исследована классическая модель системы правового регулирования обеспечения информационной безопасности, а также отдельные уровни, элементы этой системы, в том числе международное правовое регулирование обеспечения информационной безопасности, федеральное правовое регулирование и возможности законодательного обеспечения информационной безопасности на уровне субъектов Российской Федерации и муниципальных образований.

На этапе цифровой трансформации, особенно в связи с новым паспортом научных специальностей, теоретико-правовые вопросы развития информационного права нуждаются в фундаментальных правовых исследованиях, осмыслении проблем с позиции философии, теории права и государства, иных смежных отраслей российской правовой доктрины. Как справедливо отмечено А. Н. Савенковым, «единственной успешной стратегией научного поиска в настоящее время является сотрудничество ученых-правоведов с представителями широкого спектра научных дисциплин, изучающих человека и общество»³⁷. Синергетические процессы в информационном праве коснулись практически всех отраслей права, и неслучайно оно отнесено к публично-правовым (государственно-правовым) наукам. Развитие информационного пространства (системы новых субъектов и объектов общественных правоотношений, активизации использования наукоемких технологий во всех сферах жизни) определяет необходимость модернизации существующих правовых подходов к регулированию новых отношений.

Сектор информационного права и международной информационной безопасности ИГП РАН является ведущим научным центром по исследованию проблем информационного права и правового обеспечения информационной безопасности не только в Российской Федерации, но и за рубежом. Перспективные исследования сектора связаны с разработкой: теоретических оснований и закономерностей правового регулирования экономики данных и идентификации в информационном пространстве, а также новейших наукоемких технологий, в том числе искусственного интеллекта; проблем международной информационной безопасности в свете реализации новых международных норм в сфере противодействия киберпреступности; понятийного

аппарата и возможных моделей правового регулирования в сфере цифровых отношений; вопросов систематизации российского законодательства с применением информационных технологий и др. Приоритетными являются исследования в сфере стратегического планирования в связи с разработкой новой редакции Доктрины информационной безопасности Российской Федерации, а также правовым обеспечением цифрового суверенитета, информационной безопасности в процессе стратегического планирования³⁸. Отдельное направление связано с обеспечением правовой защиты прав и интересов граждан в сфере использования цифровых технологий. Научный потенциал сектора позволяет решать стоящие перед ним задачи, определять и осваивать новые горизонты информационного права в XXI веке.

Заключение

Исследование показывает, что для правового обеспечения информационной безопасности в Российской Федерации сформирована правовая база, которая, тем не менее, требует постоянного совершенствования, учитывая национальные проекты и стратегические задачи развития Российской Федерации. Полагаем, что приоритетами должны стать: разработка доктрины информационного права, включая правовое обеспечение информационной (национальной и международной) безопасности, в том числе кибербезопасности и киберстабильности, в свете принятия универсальных международных документов по противодействию киберпреступности; доктринальная модель развития системы информационного законодательства (включая цифровое), направленная на научное обоснование, упорядочение правового регулирования информационных отношений, связанных с обеспечением информационной, цифровой и кибербезопасности. Отдельного внимания заслуживает понятийный аппарат, система основных положений, направленных на решение государственных задач в информационной сфере в рамках последних актов стратегического планирования, а также обеспечения функционирования национального проекта «Экономика данных и цифровая трансформация государства»³⁹.

³⁶ См.: Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Обзор Международной научно-практической конференции «Информационное пространство: обеспечение информационной безопасности и право» — Первые Бачиловские чтения // Государство и право. 2018. № 9. С. 138–148.

³⁷ Савенков А.Н. Трансформация парадигмы права в цивилизационном развитии человечества: доклады членов РАН / под общ. ред. А.Н. Савенкова. М., 2019. С. 6.

³⁸ См.: Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Формирование системы информационного права как научного направления: этапы развития и перспективы // Государство и право. 2019. № 2. С. 80–92; Их же. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. 2021. № 12. С. 97–108.

³⁹ Денисенко А. Названы главные задачи нацпроекта «Экономика данных и цифровая трансформация государства». URL: <https://corp.cnews.ru/news/top/2024-06-26-mishustin-nazval-osnovnye> (дата обращения: 20.11.2024).

Информационное право развивается во многом как публично-правовая отрасль, направленная на правовое обеспечение функционирования информационной, в том числе цифровой, среды, а также национального суверенитета в информационной сфере и информационной безопасности Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. Бачило И.Л., Полякова Т.А., Демьянец М.В. и др. Об основных направлениях информационного права за 2000–2015 гг. // Государство и право. 2017. № 1. С. 79.
2. Венгеров А.Б. Теория государства и права. М., 2005. С. 92.
3. Денисенко А. Названы главные задачи нацпроекта «Экономика данных и цифровая трансформация государства». URL: https://corp.cnews.ru/news/top/2024-06-26_mishustin_nazval_osnovnye (дата обращения: 20.11.2024).
4. Ефремов А.А. Защита государственного суверенитета Российской Федерации в информационном пространстве. М., 2017.
5. Ефремов А.А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации: дис. ... д-ра юрид. наук. М., 2021.
6. Информационные технологии в уголовно-правовой сфере / под ред. А.И. Бастрыкина, А.Н. Савенкова. М., 2023.
7. Капустин А.Я. Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. 2022. Т. 18. № 6. С. 99–108.
8. Концепция Информационного кодекса Российской Федерации / под ред. И.Л. Бачило. М., 2014. С. 9.
9. Малько А.В., Афанасьев С.Ф., Борисова В.Ф., Кроткова Н.В. Обзор методологического семинара на тему «Цифровое право: методология исследования» (18 апреля 2019 г., Саратовская государственная юридическая академия, Саратовский филиал Института государства и права РАН) // Государство и право. 2019. № 8. С. 122–128.
10. Минбалева А.В., Берестнев М.А., Евсиков К.С. Обеспечение информационной безопасности оборудования добывающей промышленности в квантовую эпоху // Известия Тульского гос. ун-та. Науки о Земле. 2023. № 1. С. 567–584.
11. Палиенко Н.И. Суверенитет. Историческое развитие идеи суверенитета и ее правовое значение. Ярославль, 1903. С. 438, 439.
12. Полякова Т.А., Зиновьева Е.С., Смирнов А.А. Международная информационная безопасность: универсальное правовое измерение // Государство и право. 2023. № 12. С. 139–149.
13. Полякова Т.А., Камалова Г.Г. Государственная тайна как институт правового обеспечения национального суверенитета и безопасности Российской Федерации // Государство и право. 2024. № 7. С. 174–183.
14. Полякова Т.А., Минбалева А.В., Кроткова Н.В. Обзор Международной научно-практической конференции «Информационное пространство: обеспечение информационной безопасности и право» – Первые Бачиловские чтения // Государство и право. 2018. № 9. С. 138–148.
15. Полякова Т.А., Минбалева А.В., Кроткова Н.В. Основные тенденции и проблемы развития науки информационного права // Государство и право. 2022. № 9. С. 94–104.
16. Полякова Т.А., Минбалева А.В., Кроткова Н.В. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. 2021. № 12. С. 97–108.
17. Полякова Т.А., Минбалева 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.
18. Полякова Т.А., Минбалева А.В., Кроткова Н.В. Формирование системы информационного права как научного направления: этапы развития и перспективы // Государство и право. 2019. № 2. С. 80–92.
19. Полякова Т.А., Минбалева А.В., Наумов В.Б. К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // Государство и право. 2024. № 1. С. 81–91.
20. Полякова Т.А., Минбалева А.В., Наумов В.Б. Правовое регулирование квантовых коммуникаций в России и в мире // Государство и право. 2022. № 5. С. 104–114.
21. Полякова Т.А., Минбалева 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.
22. Полякова Т.А., Смирнов А.А. Правовое обеспечение международной информационной безопасности: приоритеты для Союзного государства // Право.ру. 2023. № 5(85). С. 84–92.
23. Полякова Т.А., Смирнов А.А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Росс. юрид. журнал. 2022. № 3. С. 7–15.
24. Савенков А.Н. Трансформация парадигмы права в цивилизационном развитии человечества: доклады членов РАН / под общ. ред. А.Н. Савенкова. М., 2019. С. 6.
25. Савенков А.Н. Философия права и становление российского государства-цивилизации. М., 2024. С. 64.
26. Троян Н.А., Полякова Т.А., Кроткова Н.В. Бачило Илларию Лаврентьевна // Портал. Большая российская энциклопедия. URL: <https://bigenc.ru/c/bachilo-illariia-lavrent-evna-36a9bd> (дата обращения: 10.11.2024).
27. Ушаков Н.А. Суверенитет в современном международном праве. М., 1963. С. 23.
28. Философия права. Словарь. 2-е изд., дораб. и доп. / под ред. и сост. В.Н. Жуков. М., 2021. С. 704.

29. Polyakova T.A., Naumov V.B., Minbaleev A.V. Trust in the law during the digital transformation // Государство и право. 2022. № 11. С. 139–147.

REFERENCES

1. Bachilo I.L., Polyakova T.A., Demyanets M.V. et al. On the main directions of information law for 2000–2015 // State and Law. 2017. No. 1. P. 79 (in Russ.).
2. Vengerov A.B. Theory of the state and law. M., 2005. P. 92 (in Russ.).
3. Denisenko A. The main objectives of the national project “Data Economy and digital transformation of the state” are named. URL: https://corp.cnews.ru/news/top/2024-06-26_mishustin_nazval_osnovnye (accessed: 20.11.2024) (in Russ.).
4. Efremov A.A. Protection of the state sovereignty of the Russian Federation in the information space. M., 2017 (in Russ.).
5. Efremov A.A. Information and legal mechanism for ensuring the state sovereignty of the Russian Federation: dis. ... Doctor of Law. M., 2021 (in Russ.).
6. Information technologies in the Criminal Law sphere / ed. by A.I. Bastrykin, A.N. Savenkov. M., 2023 (in Russ.).
7. Kapustin A. Ya. Sovereignty of the state in cyberspace: an international legal dimension // Journal of Foreign Legislation and Comparative Jurisprudence. 2022. Vol. 18. No. 6. Pp. 99–108 (in Russ.).
8. The concept of the Information Code of the Russian Federation / ed. by I.L. Bachilo. M., 2014. P. 9 (in Russ.).
9. Mal'ko A.V., Afanasyev S.F., Borisova V.F., Krotkova N.V. Review of the methodological seminar on “Digital Law: research methodology” (April 18, 2019, Saratov State Law Academy, Saratov branch of the Institute of State and Law of the Russian Academy of Sciences) // State and Law. 2019. No. 8. Pp. 122–128 (in Russ.).
10. Minbaleev A.V., Berestnev M.A., Evsikov K.S. Ensuring information security of mining industry equipment in the quantum era // Proceedings of Tula State University. Earth Sciences. 2023. No. 1. Pp. 567–584 (in Russ.).
11. Palienko N.I. Sovereignty. The historical development of the idea of sovereignty and its legal significance. Yaroslavl, 1903. Pp. 438, 439 (in Russ.).
12. Polyakova T.A., Zinovieva E.S., Smirnov A.A. International information security: a universal legal dimension // State and Law. 2023. No. 12. Pp. 139–149 (in Russ.).
13. Polyakova T.A., Kamalova G.G. State secrecy as an institution of legal support for national sovereignty and security of the Russian Federation // State and Law. 2024. No. 7. Pp. 174–183 (in Russ.).
14. Polyakova T.A., Minbaleev A.V., Krotkova N.V. Review of the International Scientific and Practical Conference “Information space: ensuring information security and law” – The First Bachilo readings // State and Law. 2018. No. 9. Pp. 138–148 (in Russ.).
15. Polyakova T.A., Minbaleev A.V., Krotkova N.V. The main trends and problems of the development of the science of Information Law // State and Law. 2022. No. 9. Pp. 94–104 (in Russ.).
16. Polyakova T.A., Minbaleev A.V., Krotkova N.V. The development of the science of Information Law and legal support for information security: the formation of a scientific school of Information Law (past and future) // State and Law. 2021. No. 12. Pp. 97–108 (in Russ.).
17. Polyakova T.A., Minbaleev A.V., Krotkova N.V. Transformation of the science of Information Law and information legislation: a new stage in the conditions of scientific and technological development of Russia // State and Law. 2024. No. 9. Pp. 166–179 (in Russ.).
18. Polyakova T.A., Minbaleev A.V., Krotkova N.V. Formation of the information law system as a scientific field: stages of development and prospects // State and Law. 2019. No. 2. Pp. 80–92 (in Russ.).
19. Polyakova T.A., Minbaleev A.V., Naumov V.B. On the issue of codification of information legislation in the context of digital transformation // State and Law. 2024. No. 1. Pp. 81–91 (in Russ.).
20. Polyakova T.A., Minbaleev A.V., Naumov V.B. Legal regulation of quantum communications in Russia and in the world // State and Law. 2022. No. 5. Pp. 104–114 (in Russ.).
21. Polyakova T.A., Minbaleev A.V., Troyan 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. Pp. 131–144 (in Russ.).
22. Polyakova T.A., Smirnov A.A. Legal support for international information security: priorities for the Union State // Право. 2023. No. 5 (85). Pp. 84–92 (in Russ.).
23. Polyakova T.A., Smirnov A.A. Legal support of international information security: problems and prospects // Journal of Russ. Law. 2022. No. 3. Pp. 7–15 (in Russ.).
24. Savenkov A.N. Transformation of the paradigm of law in the civilizational development of mankind: reports of members of the Russian Academy of Sciences / under the general ed. of A.N. Savenkov. M., 2019. P. 6 (in Russ.).
25. Savenkov A.N. Philosophy of Law and the formation of the Russian state-civilization. M., 2024. P. 64 (in Russ.).
26. Troyan N.A., Polyakova T.A., Krotkova N.V. Bachilo Illaria Lavrentievna // Portal. The Great Russian Encyclopedia. URL: <https://bigenc.ru/c/bachilo-illariiia-lavrentievna-36a9bd> (accessed: 10.11.2024) (in Russ.).
27. Ushakov N.A. Sovereignty in modern International Law. M., 1963. P. 23 (in Russ.).
28. Philosophy of Law. Dictionary. 2nd ed., rev. and add. / ed. by and comp. V.N. Zhukov. M., 2021. P. 704 (in Russ.).
29. Polyakova T.A., Naumov V.B., Minbaleev A.V. Trust in the law during the digital transformation // State and Law. 2022. No. 11. Pp. 139–147.

Сведения об авторах

ПОЛЯКОВА Татьяна Анатольевна —
доктор юридических наук, профессор,
главный научный сотрудник,
и.о. заведующей сектором информационного
права и международной информационной
безопасности Института государства и права
Российской академии наук;
119019 г. Москва, ул. Знаменка, д. 10
ORCID: 0000-0003-3791-2903

МИНБАЛЕЕВ Алексей Владимирович —
доктор юридических наук, профессор,
заведующий кафедрой информационного права
и цифровых технологий Московского
государственного юридического университета
им. О.Е. Кутафина (МГЮА); 125993 г. Москва,
ул. Садовая-Кудринская, д. 9, стр. 2;
главный научный сотрудник сектора
информационного права и международной
информационной безопасности
Института государства и права
Российской академии наук;
119019 г. Москва, ул. Знаменка, д. 10
ORCID: 0000-0001-5995-1802

НАУМОВ Виктор Борисович —
доктор юридических наук,
главный научный сотрудник сектора
информационного права и международной
информационной безопасности
Института государства и права
Российской академии наук;
119019 г. Москва, ул. Знаменка, д. 10;
профессор кафедры информационного
права и цифровых технологий Московского
государственного юридического университета
им. О.Е. Кутафина (МГЮА); 125993 г. Москва,
ул. Садовая-Кудринская, д. 9, стр. 2;
руководитель проекта «Сохраненная культура»
(Санкт-Петербург)
ORCID: 0000-0003-3453-6703

Authors' information

POLYAKOVA Tatyana A. —
Doctor of Law, Professor,
Chief Researcher,
Acting Head of the Information Law
and International Information Security Sector,
Institute of State and Law
of the Russian Academy of Sciences;
10 Znamenka str., 119019 Moscow, Russia

MINBALEEV Alexey V. —
Doctor of Law, Professor,
Head of Department of Information Law
and Digital Technologies,
Kutafin Moscow State Law University (MSAL);
9, bld. 2 Sadovaya-Kudrinskaya,
125993 Moscow, Russia;
Chief Researcher, Information Law
and International Information Security Sector,
Institute of State and Law
of the Russian Academy of Sciences;
10 Znamenka str., 119019 Moscow, Russia

NAUMOV Victor B. —
Doctor of Law,
Chief Researcher,
Information Law
and International Information Security Sector,
Institute of State and Law,
of the Russian Academy of Sciences;
10 Znamenka str., 119019 Moscow, Russia;
Professor at Department
of Information Law and Digital Technologies,
Kutafin Moscow State Law University (MSAL);
9, bld. 2 Sadovaya-Kudrinskaya,
125993 Moscow, Russia;
Head of project "Preserved Culture"
(St. Petersburg)