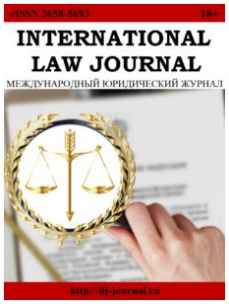
ISSN 2658-5693
https://ilj-journal.ru



Научно-исследовательский журнал «International Law Journal»
https://ilj-journal.ru
2025, Том 8, № 7 / 2025, Vol. 8, Iss. 7 https://ilj-journal.ru/archives/category/publications
Научная статья / Original article
Шифр научной специальности: 5.1.3. Частно-правовые (цивилистические) науки (юридические науки)
УДК 347.77

Роль государственных институтов в регулировании цифровой экономики с учетом политических рисков и правовых механизмов защиты данных

[1] Примак А.В., [1] Набойченко М.С., [1] Нечай Е.Е.,
[1] Дальневосточный федеральный университет

Аннотация: *развитие цифровой экономики трансформирует роль государственных институтов, переходя от пассивного наблюдения к активному регулированию для обеспечения суверенитета и минимизации политических рисков, таких как киберугрозы и санкции. Актуальность обусловлена необходимостью баланса между инновациями, защитой данных и национальной безопасностью, где правовые механизмы становятся инструментом политики, влияя на бизнес и гражданские права. Исследование опирается на федеральные законы РФ о информации и персональных данных, стратегические документы вроде Доктрины информационной безопасности, подзаконные акты и судебную практику. Применены формально-юридический анализ, системный подход, сравнительно-правовой метод и изучение правоприменения для оценки регуляторных механизмов. Выявлены ключевые механизмы: концепция цифрового суверенитета с локализацией данных, усиление штрафов за утечки, экстерриториальное применение норм, блокировка контента, "суверенный Рунет" и антимонопольный контроль над платформами, ориентированные на противодействие внешним угрозам.*

Ключевые слова: *цифровая экономика, государственные институты, защита данных, политические риски, правовое регулирование*

Для цитирования: Примак А.В., Набойченко М.С., Нечай Е.Е. Роль государственных институтов в регулировании цифровой экономики с учетом политических рисков и правовых механизмов защиты данных // International Law Journal. 2025. Том 8. № 7. С. 70 – 76.

Поступила в редакцию: 18 июля 2025 г.; Одобрена после рецензирования: 17 сентября 2025 г.; Принята к публикации: 5 ноября 2025 г.

The role of state institutions in regulating the digital economy with consideration of political risks and legal mechanisms for data protection

[1] Primak A.V., [1] Naboichenko M.S., [1] Nechai E.E.,
[1] Far East Federal University

Abstract: *the development of the digital economy is transforming the role of state institutions, shifting from passive observation to active regulation in order to ensure sovereignty and minimize political risks such as cyber threats and sanctions. The relevance is determined by the need to balance innovation, data protection, and national security, where legal mechanisms become tools of policy, influencing business and civil rights. The study is based on federal laws of the Russian Federation on information and personal data, strategic documents such as the Information Security Doctrine, by-laws, and judicial practice. Formal-legal analysis, a systemic approach, the comparative-legal method, and the study of law enforcement are applied to assess regulatory mechanisms. Key mechanisms identified include the concept of digital sovereignty with data localization, increased fines for*

breaches, extraterritorial application of norms, content blocking, the "sovereign Runet," and antitrust control over platforms, aimed at countering external threats.

Keywords: *digital economy, state institutions, data protection, political risks, legal regulation*

For citation: Primak A.V., Naboichenko M.S., Nechai E.E. The role of state institutions in regulating the digital economy with consideration of political risks and legal mechanisms for data protection. International Law Journal. 2025. 8 (7). P. 70 – 76.

The article was submitted: July 18, 2025; Approved after reviewing: September 17, 2025; Accepted for publication: November 5, 2025.

Введение

Стремительное развитие цифровой экономики трансформировало не только экономические процессы, но и фундаментальные основы функционирования общества и государства. Переход к цифровым платформам, большим данным, искусственному интеллекту и интернету вещей стал определяющим фактором глобальной конкурентоспособности и национальной безопасности. В этом контексте роль государственных институтов претерпевает кардинальные изменения: от пассивного наблюдателя и создателя рамочных условий государство переходит к активному регулированию, стремясь одновременно стимулировать инновации и минимизировать возникающие угрозы. Центральной проблемой современного государственного управления в цифровой сфере становится поиск баланса между необходимостью обеспечения технологического суверенитета, защиты критической информационной инфраструктуры и прав граждан, с одной стороны, и созданием благоприятной среды для развития бизнеса и свободного обмена информацией, с другой. Эта дилемма усугубляется растущими политическими рисками, такими как санкционное давление, информационные войны и киберугрозы, которые заставляют государства пересматривать свои подходы к регулированию трансграничных потоков данных и деятельности глобальных технологических компаний.

Актуальность данного исследования обусловлена тем, что правовые механизмы, создаваемые для регулирования цифровой экономики, зачастую являются прямой реакцией на политические вызовы. Законодательство в области персональных данных, требования к локализации информации, правила модерации контента и регулирование деятельности IT-гигантов все чаще рассматриваются не только через призму защиты прав субъектов данных или добросовестной конкуренции, но и как инструменты обеспечения национального суверенитета в цифровом пространстве. Это порождает комплекс правовых, экономических и этических вопросов. Как государственные институты, такие как регуляторы, суды и правоохранительные органы, адаптируют свою деятельность к новым реалиям? Насколько существующая нормативная база способна эффективно отвечать на вызовы, связанные с экстерриториальным характером цифровых отношений и асимметрией власти между государством и глобальными технологическими корпорациями? Анализ взаимодействия политических рисков и правовых механизмов защиты данных позволяет вскрыть глубинные мотивы и тенденции в государственной политике, а также оценить долгосрочные последствия выбранной регуляторной модели для развития цифровой экономики и гражданского общества.

Материалы и методы исследований

Материалом для настоящего исследования послужил широкий комплекс источников, включающий нормативно-правовые акты Российской Федерации, доктринальные документы стратегического планирования, а также материалы правоприменительной, в том числе судебной, практики. Основополагающую базу составили федеральные законы, непосредственно регулирующие отношения в цифровой среде, в частности Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», а также положения Гражданского кодекса РФ, Кодекса РФ об административных правонарушениях и Уголовного кодекса РФ в частях, касающихся правонарушений в информационной сфере. Особое внимание было уделено подзаконным актам, изданным Правительством РФ, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Федеральной антимонопольной службой и другими уполномоченными органами. Кроме того, в качестве материалов были использованы стратегические документы, определяющие векторы государственной политики, такие как Доктрина информационной безопасности Российской Федерации и национальная программа «Цифровая экономика Российской Федерации». Анализ судебной практики

ISSN 2658-5693
https://ilj-journal.ru

включал изучение постановлений и определений Конституционного Суда РФ, Верховного Суда РФ и судов общей юрисдикции по делам, связанным с блокировкой интернет-ресурсов, привлечением к ответственности за нарушения законодательства о персональных данных и оспариванием действий государственных регуляторов.

Методологическая основа исследования базируется на совокупности общенаучных и частнонаучных методов познания. Ключевым методом выступил формально-юридический анализ, позволивший исследовать содержание правовых норм, выявить их структуру, взаимосвязи и возможные коллизии. Системный подход применялся для рассмотрения государственных институтов и правовых механизмов как единой, взаимосвязанной системы, направленной на достижение определенных политических и правовых целей в сфере регулирования цифровой экономики. Сравнительно-правовой метод использовался для сопоставления отдельных российских правовых институтов с зарубежными аналогами, в частности с Общим регламентом по защите данных (GDPR) Европейского союза, что позволило выявить специфику российского подхода, обусловленную национальными политическими и экономическими реалиями. Также применялся метод анализа правоприменительной практики, который дал возможность оценить, как абстрактные нормы права реализуются на практике, с какими трудностями сталкиваются правоприменители и субъекты права, и какие тенденции формируются в судебных и административных решениях. Комплексное применение указанных методов позволило провести всестороннее исследование роли государственных институтов в контексте заявленной темы, выявив взаимовлияние политических факторов и правовых конструкций в процессе регулирования цифровой среды.

Результаты и обсуждения

Центральным элементом государственной политики в области регулирования цифровой экономики в последние годы стала концепция «цифрового суверенитета». Данное понятие, не имея строгого легального определения, на практике воплощается в комплексе законодательных мер, направленных на усиление контроля государства над информационными потоками, инфраструктурой и данными, циркулирующими на его территории. Это является прямым ответом на политические риски, связанные с доминированием иностранных технологических платформ и возможностью их использования в целях, противоречащих национальным интересам [7]. Одним из наиболее ярких проявлений этой политики стало введение требований о локализации персональных данных российских граждан.

Федеральный закон № 242-ФЗ, обязавший операторов при сборе персональных данных граждан РФ обеспечивать их запись, систематизацию, накопление и хранение с использованием баз данных, находящихся на территории России, является краеугольным камнем в построении цифрового суверенитета. Изначально заявленная цель – защита прав субъектов персональных данных [2] – на практике дополнилась задачей обеспечения доступа к этой информации для национальных правоохранительных и специальных служб, а также вывода этих данных из-под юрисдикции иностранных государств. Правоприменительная практика Роскомнадзора и судов демонстрирует последовательную линию по привлечению к ответственности иностранных компаний, игнорирующих данное требование, что выразилось в многомиллионных оборотных штрафах и блокировке отдельных ресурсов [11]. Однако эффективность данной меры остается предметом дискуссий: технически требование о локализации не препятствует последующей трансграничной передаче данных и не гарантирует их стопроцентной защиты от утечек.

Параллельно с ужесточением требований к хранению данных, эволюционирует и сам институт защиты персональных данных, регулируемый ФЗ-152. Законодатель постоянно вводит новые составы административных правонарушений и многократно увеличивает размеры штрафов за утечки данных. Если ранее ответственность была скорее символической, то введение оборотных штрафов для компаний, допустивших повторные утечки, ставит их перед реальной угрозой серьезных финансовых потерь. Это заставляет бизнес, в том числе средний и малый, пересматривать свои подходы к кибербезопасности [14]. Вместе с тем, правовой механизм компенсации вреда самим субъектам, чьи данные утекли в сеть, остается крайне неэффективным. Судебная практика по взысканию морального вреда в таких случаях складывается не в пользу граждан, присуждая им минимальные суммы, несоизмеримые с потенциальным ущербом.

Особую сложность представляет проблема экстерриториальности цифровых отношений. Глобальные интернет-платформы, не имея физического присутствия в России, тем не менее активно работают с российской аудиторией. Для распространения на них действия российского законодательства был разработан критерий «направленности деятельности на территорию РФ». Суды трактуют его достаточно широко, включая наличие русскоязычного интерфейса, возможность расчетов в рублях или показ рекламы, нацеленной на российских пользователей [5]. Это позволило применять к иностранным IT-гигантам требования так называемого закона «о приземлении», обязывающего их открывать в России полноценные

ISSN 2658-5693
https://ilj-journal.ru

представительства. Однако механизм реального принуждения к исполнению решений российских судов, особенно в условиях санкционного противостояния, остается ограниченным.

Государственные институты активно используют и механизмы контроля за содержанием информации. Федеральный закон № 149-ФЗ предоставляет Роскомнадзору и Генеральной прокуратуре широкие полномочия по внесудебной и судебной блокировке интернет-ресурсов, содержащих противоправную информацию – от экстремистских материалов до «фейковых новостей» о действиях государственных органов. Законодательство о «фейках» и «дискредитации» Вооруженных Сил РФ, принятое в ответ на обострение геополитической обстановки, стало мощным инструментом информационного контроля [9]. Судебная практика по таким делам показывает крайне низкий процент оспаривания решений регулятора, что свидетельствует о приоритете задач государственной безопасности над принципом свободы распространения информации.

Реализация так называемого закона «о суверенном Рунете» является еще одним направлением укрепления государственного контроля. Создание национальной системы доменных имен, требование к операторам связи устанавливать технические средства противодействия угрозам (ТСПУ) для централизованного управления трафиком – все это направлено на обеспечение работоспособности российского сегмента сети Интернет в случае его отключения извне [3]. Критики этой системы указывают на риски использования данной инфраструктуры для тотальной фильтрации трафика и ограничения доступа к информации уже по внутриполитическим причинам, а не только в ответ на внешние угрозы.

Важную роль в регулировании цифровой экономики играет Федеральная антимонопольная служба (ФАС). Ее деятельность направлена на борьбу со злоупотреблениями доминирующим положением со стороны крупных цифровых экосистем. Дела против Apple, связанные с правилами магазина приложений App Store, или против Google из-за предустановки его сервисов на устройствах Android, показывают, что антимонопольное регулирование становится инструментом не только защиты конкуренции, но и продвижения национальных программных продуктов [15]. ФАС все чаще рассматривает доступ к данным как один из ключевых факторов доминирования на рынке, что сближает антимонопольное и информационное право.

Деятельность правоохранительных органов в цифровой среде также претерпевает изменения. Нормы «пакета Яровой» обязали операторов связи и организаторов распространения информации хранить огромные объемы данных о коммуникациях пользователей и предоставлять их по запросу спецслужб, включая ключи для дешифровки сообщений [1]. Это положение вызвало ожесточенные споры и привело к известному конфликту с мессенджером Telegram. Решение Конституционного Суда РФ по этому вопросу, по сути, подтвердило конституционность данных требований, указав на необходимость соблюдения баланса интересов безопасности и частной жизни, однако на практике этот баланс часто смещается в сторону интересов государства [10].

Для бизнеса сложившаяся регуляторная среда создает серьезные вызовы. Высокая стоимость комплаенса, связанная с необходимостью локализации данных, внедрения систем СОРМ и хранения трафика, ложится тяжелым бременем на компании. Правовая неопределенность, обусловленная широкими и оценочными формулировками в законодательстве (например, что считать «недостоверной общественно значимой информацией»), создает риски произвольного правоприменения [13]. Быстро меняющееся законодательство требует от компаний постоянного мониторинга и адаптации своих бизнес-процессов, что особенно сложно для малого и среднего бизнеса.

Судебная система в этой конструкции выполняет двоякую роль. С одной стороны, суды в большинстве случаев поддерживают позицию государственных регуляторов в спорах с бизнесом, особенно когда речь идет о вопросах национальной безопасности или информационной политики. Решения о блокировках или наложении штрафов на IT-компании редко отменяются в вышестоящих инстанциях [6]. С другой стороны, именно через судебную практику происходит уточнение и конкретизация размытых законодательных норм. Например, в спорах о защите персональных данных суды постепенно формируют подходы к определению размера причиненного морального вреда или к оценке достаточности мер, принятых оператором для защиты информации.

Международный контекст также оказывает существенное влияние. Российская модель регулирования, ориентированная на суверенитет и контроль, заметно отличается от европейской модели GDPR, в центре которой находится защита прав и свобод физического лица как субъекта данных [4]. Это создает проблемы совместимости правовых режимов и усложняет трансграничную передачу данных. Компании, работающие на нескольких рынках, вынуждены выстраивать сложные системы комплаенса, чтобы соответствовать порой противоречащим друг другу требованиям разных юрисдикций.

ISSN 2658-5693
https://ilj-journal.ru

Политические риски напрямую конвертируются в правовые нормы. Введение санкций против российского IT-сектора стимулировало принятие мер государственной поддержки для отечественных разработчиков и введение преференций для российского программного обеспечения при государственных закупках [8]. Угроза технологической блокады подталкивает к разработке собственных операционных систем, платформ и стандартов, что в долгосрочной перспективе может привести к частичной изоляции российского цифрового пространства.

Таким образом, государственные институты в России выстроили сложную, многоуровневую систему регулирования цифровой экономики. Эта система характеризуется доминированием императивных методов, приоритетом целей государственной безопасности над экономическими свободами и правами личности, а также высокой степенью зависимости правовых норм от текущей политической конъюнктуры [12]. Роль Роскомнадзора трансформировалась от технического надзорного органа до мощного политико-правового регулятора, обладающего широчайшими полномочиями в цифровой сфере.

Выводы

В результате проведенного исследования можно заключить, что государственные институты Российской Федерации играют ключевую и все более активную роль в регулировании цифровой экономики. Эта роль формируется под значительным влиянием политических рисков и стратегической цели по обеспечению национального суверенитета в информационном пространстве. Созданная нормативно-правовая база представляет собой сложную систему, в которой механизмы, формально направленные на защиту данных и прав граждан, тесно переплетены с инструментами государственного контроля над информацией и технологической инфраструктурой. Такие институты, как локализация данных, централизованное управление трафиком, обязательное «приземление» иностранных IT-компаний и широкие полномочия по блокировке контента, являются прямым воплощением политики цифрового суверенитета. Деятельность регуляторов, в первую очередь Роскомнадзора, и складывающаяся судебная практика свидетельствуют о последовательном усилении государственного контроля, где соображения безопасности зачастую превалируют над принципами свободы информации и экономической целесообразности.

Сформировавшаяся модель регулирования, будучи эффективной для решения тактических задач по противодействию внешним угрозам и укреплению контроля над национальным цифровым сегментом, в долгосрочной перспективе порождает ряд системных проблем. Для бизнеса она означает рост издержек на соответствие требованиям, правовую неопределенность и риски, связанные с жестким правоприменением, что может сдерживать инновационное развитие и инвестиционную привлекательность. Для гражданского общества – сужение пространства для свободного выражения мнений и потенциальное ограничение доступа к глобальному информационному полю. Дальнейшее развитие правового регулирования цифровой экономики будет зависеть от способности государства найти устойчивый баланс между защитой национальных интересов и созданием условий для открытого, конкурентного и основанного на уважении прав человека цифрового будущего. Без такого баланса существует риск технологического отставания и самоизоляции, что может нивелировать достижения в области цифровизации.

Список источников

1. Gutbrod M. Phenomenon of digital platforms and legal regulation // Digital Law Journal. 2023. Vol. 4. № 2. P. 73 – 79.

2. Соловяненко Н.И. Устойчивое развитие и защита прав участников экономической деятельности в условиях цифровой трансформации // Право и практика. 2024. № 4. С. 151 – 157.

3. Овсянникова А.В. Институциональные основы цифровой экономики: от теории к институциональному проектированию // Вестник евразийской науки. 2025. Т. 17. № S2. С. 69FAVN225.

4. Печегин Д.А. Правовые механизмы защиты цифрового суверенитета государства: сравнительно-правовой аспект // Российский журнал правовых исследований. 2022. Т. 9. № 2. С. 9-20.

5. Габов А.В. Изменения в праве как следствие развития цифровой экономики // Пермский юридический альманах. 2020. № 3. С. 39 – 47.

6. Куц А.В., Фирсов В.С., Маклакова В.Е. Стратификация обеспечения цифровых механизмов обеспечения инфраструктурной безопасности // Modern Economy Success. 2022. № 1. С. 84 – 90.

7. Годзенко О.А. Направления совершенствования правового регулирования цифровизации государственного управления // Юрист спешит на помощь. 2021. № 2. С. 18 – 21.

8. Нехорошев С., Попов А., Капральный Ю. Цифровая эволюция регионов // Гражданская защита. 2021. № 10 (554). С. 36 – 37.

9. Затулина Т.Н. Государственное публичное управление цифровой средой: реализация идеи в условиях выявления и устранения конституционных рисков // Государственная власть и местное самоуправление. 2024. № 10. С. 38 – 42.

10. Овсянникова А.В. Институциональные основы цифровой экономики: от теории к институциональному проектированию // Вестник евразийской науки. 2025. Т. 17. № S2. С. 69FAVN225.

11. Гриценко Е.В. Право на хорошее управление в условиях цифровой трансформации // Сравнительное конституционное обозрение. 2022. № 4 (149). С. 15 – 36.

12. Муцалов Ш.Ш., Дадаев Х.М. Влияние цифрового фактора на правовое регулирование в обществе // Вестник Чеченского государственного университета им. А.А. Кадырова. 2022. № 4 (48). С. 81 – 86.

13. Филипова И.А. Прямая и представительная демократия в эпоху цифровых технологий // Конституционное и муниципальное право. 2022. № 9. С. 32 – 36.

14. Овчинников А.И. Правовое стимулирование развития цифровой экономики: векторы и приоритеты // Северо-Кавказский юридический вестник. 2021. № 4. С. 15 – 24.

15. Шинкарецкая Г.Г. Взаимодействие законодательства различных государств в процессе цифровизации государственного управления // Образование и право. 2021. № 1. С. 32 – 39.

References

1. Gutbrod M. Phenomenon of digital platforms and legal regulation. Digital Law Journal. 2023. Vol. 4. No. 2. P. 73 – 79.

2. Solovyanenko N.I. Sustainable Development and Protection of the Rights of Economic Participants in the Context of Digital Transformation. Law and Practice. 2024. No. 4. P. 151 – 157.

3. Ovsyannikova A.V. Institutional Foundations of the Digital Economy: From Theory to Institutional Design. Bulletin of Eurasian Science. 2025. Vol. 17. No. S2. Pp. 69FAVN225.

4. Pechegin D.A. Legal Mechanisms for Protecting the Digital Sovereignty of the State: A Comparative Legal Aspect. Russian Journal of Legal Research. 2022. Vol. 9. No. 2. P. 9 – 20.

5. Gabov A.V. Changes in the Law as a Result of the Development of the Digital Economy. Perm Legal Almanac. 2020. No. 3. P. 39 – 47.

6. Kuts A.V., Firsov V.S., Maklakova V.E. Stratification of Providing Digital Mechanisms for Ensuring Infrastructure Security. Modern Economy Success. 2022. No. 1. P. 84 – 90.

7. Godzenko O.A. Directions for Improving the Legal Regulation of Public Administration Digitalization. A Lawyer to the Rescue. 2021. No. 2. P. 18 – 21.

8. Nekhoroshev S., Popov A., Kapralny Yu. Digital Evolution of Regions. Civil Defense. 2021. No. 10 (554). P. 36 –37.

9. Zatulina T.N. State Public Governance of the Digital Environment: Implementing the Idea in the Context of Identifying and Eliminating Constitutional Risks. State Power and Local Self-Government. 2024. No. 10. P. 38 – 42.

10. Ovsyannikova AV Institutional Foundations of the Digital Economy: From Theory to Institutional Design. Bulletin of Eurasian Science. 2025. Vol. 17. No. S2. P. 69FAVN225.

11. Gritsenko EV The Right to Good Governance in the Context of Digital Transformation. Comparative Constitutional Review. 2022. No. 4 (149). P. 15 – 36.

12. Mutsalov Sh.Sh., Dadaev Kh.M. The Influence of the Digital Factor on Legal Regulation in Society. Bulletin of the Chechen State University named after A.A. Kadyrov. 2022. No. 4 (48). P. 81 – 86.

13. Filipova I.A. Direct and Representative Democracy in the Digital Age. Constitutional and Municipal Law. 2022. No. 9. P. 32 – 36.

14. Ovchinnikov A.I. Legal Incentives for the Development of the Digital Economy: Vectors and Priorities. North Caucasian Law Bulletin. 2021. No. 4. P. 15 – 24.

15. Shinkaretskaya G.G. Interaction of the Legislation of Various States in the Process of Digitalization of Public Administration. Education and Law. 2021. No. 1. P. 32 – 39.

ISSN 2658-5693
https://ilj-journal.ru

Информация об авторах

Примак А.В., специалист-эксперт, Дальневосточный федеральный университет, Primak.av@dvfu.ru

Набойченко М.С., специалист-эксперт, Дальневосточный федеральный университет, Naboichenko.ms@dvfu.ru

Нечай Е.Е., кандидат политических наук, доцент, Дальневосточный федеральный университет, Nechai@ dvfu.ru