

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ИНФОРМАЦИОННОЙ СФЕРЕ

DOI: 10.17803/1994-1471.2025.177.8.042-049

М. В. Алексеева*,
И. А. Подройкина**

Особенности правового регулирования ограничений доступа к информации, запрещенной для распространения в Российской Федерации федеральным законодательством

Аннотация. В статье рассматриваются ключевые аспекты обеспечения информационной безопасности Российской Федерации. Особое внимание уделяется совершенствованию правовых и организационных механизмов, направленных на ограничение распространения запрещенной информации и формирование безопасного информационного пространства знаний. Отмечается, что за последние годы в России достигнут значительный прогресс в области информационной политики, однако остаются неурегулированными вопросы, касающиеся терминологического аппарата, недостаточной устойчивости правового регулирования и гармонизации национального законодательства с международными нормами. В рамках рекомендаций подчеркивается необходимость проведения комплексного мониторинга законодательства, разработки юридически согласованных дефиниций, создания нормативной базы для профилактики информационных угроз, укрепления механизмов публично-правовой ответственности, обеспечения устойчивости национального законодательства в условиях глобального информационного противоборства, совершенствования способов международного сотрудничества, развития правового сопровождения контроля за социальными сетями и цифровыми платформами, создания новых регуляторов и мониторинговых структур, пересмотра акцентов государственной политики в сфере информационной безопасности.

© Алексеева М. В., Подройкина И. А., 2025

* *Алексеева Марина Владимировна*, кандидат юридических наук, заведующий кафедрой «Теория и история государства и права» Донского государственного технического университета, доцент кафедры государственно-правовых дисциплин Ростовского филиала Российской таможенной академии
Буденновский просп., д. 20, г. Ростов-на-Дону, Российская Федерация, 344002
alekseeva80@yandex.ru

** *Подройкина Инна Андреевна*, доктор юридических наук, доцент, заведующий кафедрой уголовно-правовых дисциплин Ростовского филиала Российской таможенной академии, профессор кафедры публичного и уголовного права Сургутского государственного университета
Буденновский просп., д. 20, г. Ростов-на-Дону, Российская Федерация, 344002
919820@mail.ru

Ключевые слова: информационная безопасность; информация; информационное пространство; недостоверная информация; деструктивное влияние; национальная безопасность; позитивный контент; государственная политика; информационные угрозы; блокировка.

Для цитирования: Алексеева М. В., Подройкина И. А. Особенности правового регулирования ограничений доступа к информации, запрещенной для распространения в Российской Федерации федеральным законодательством // Актуальные проблемы российского права. — 2025. — Т. 20. — № 8. — С. 42–49. — DOI: 10.17803/1994-1471.2025.177.8.042-049.

Peculiarities of the Legal Regulation of Access Restrictions to Information Prohibited from Distribution under Federal Legislation in the Russian Federation

Marina V. Alekseeva, Cand. Sci. (Law), Head of the Department of the Theory and History of the State and Law, Don State Technical University; Associate Professor, Department of State Law Disciplines, Rostov Branch, Russian Customs Academy, Rostov-on-Don, Russian Federation
alekseeva80@yandex.ru

Inna A. Podroykina, Dr. Sci. (Law), Associate Professor, Head of the Department of Criminal Law Disciplines, Rostov Branch, Russian Customs Academy; Professor, Department of Public and Criminal Law, Surgut State University, Rostov-on-Don, Russian Federation
919820@mail.ru

Abstract. The paper examines the key aspects of ensuring the information security of the Russian Federation. Particular attention is devoted to improving legal and organizational mechanisms aimed at restricting the dissemination of prohibited information and shaping a secure knowledge-based information environment. The author highlights that, in recent years, substantial progress has been achieved in the field of information policy in Russia. However, unresolved issues remain, including inconsistencies in terminology, instable and unsettled legal regulation, and the lack of alignment between national legislation and international standards. The proposed recommendations emphasize the necessity of conducting comprehensive legislative monitoring, developing legally consistent definitions, establishing a normative framework for the prevention of information threats, strengthening mechanisms of public-law accountability, ensuring the resilience of national legislation under conditions of global information confrontation, enhancing international cooperation mechanisms, improving legal support for oversight of social networks and digital platforms, creating new regulatory and monitoring bodies, and reconsidering the priorities of state policy in the domain of information security.

Keywords: information security; information; information space; unreliable information; destructive influence; national security; positive content; state policy; information threats; blocking.

Cite as: Alekseeva MV, Podroykina IA. Peculiarities of the Legal Regulation of Access Restrictions to Information Prohibited from Distribution under Federal Legislation in the Russian Federation. *Aktual'nye problemy rossiyskogo prava*. 2025;20(8):42-49. (In Russ.). DOI: 10.17803/1994-1471.2025.177.8.042-049.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы¹ определяет необходимость совершенствования механизмов ограничения

доступа к информации, запрещенной для распространения на территории страны, а также ее удаления. В частности, ее подпункт «п» п. 26 ставит задачу повышения результативности

¹ 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.

правового и организационного воздействия на общественные отношения, формирующие информационное пространство знаний.

Механизм ограничения доступа к определенным видам информации — важный элемент системы правового регулирования, обеспечивающий условия для формирования благоприятного информационного пространства на основе качественного правового оформления отношений между субъектами права. По сути, это способствует сохранению баланса между правом на доступ к информации и ее безопасностью, оказывая значительное влияние на информационную политику государства².

Неслучайно в теории так много внимания уделяется различным вопросам, касающимся необходимости ограничения доступа к той или иной информации, включая ограничения по кругу лиц. Так, например, Р. О. Опалев затрагивает проблему доступа к информации в сети Интернет³, О. Ю. Ситкова подробно рассматривает те угрозы, с которыми может столкнуться ребенок при ознакомлении с той или иной информацией, в связи с чем считает необходимым устанавливать определенные ограничения в части доступа к получению информации несовершеннолетними⁴.

В одной из своих работ мы также писали о необходимости совершенствования механизмов обеспечения безопасной информационной среды для противодействия распространению негативного контента, которые бы влияли на распространение традиционных российских ду-

ховно-нравственных ценностей⁵. Тем не менее, несмотря на значительное количество публикаций и принятых нормативных правовых актов, признать, что предпринятые меры достаточны для обеспечения информационной безопасности, пока нельзя. Именно поэтому считаем необходимым продолжить исследования в данной области.

Информационное пространство, являясь не только средой передачи знаний, но и ареной информационного противоборства, требует четкого правового оформления. В современных условиях информационная безопасность занимает одно из ключевых мест в государственной политике Российской Федерации. Согласно Закону «Об информации, информационных технологиях и о защите информации»⁶ (2006 г.), в законодательном поле выделяются термины, касающиеся регулирования доступа к информации, включая такие ключевые понятия, как:

- информация, распространение которой подлежит ограничению или запрещению⁷;
- недостоверная информация;
- информация, распространяемая с нарушением закона.

Однако важный момент заключается в том, что классификация этих понятий, равно как и их правовые основания, до сих пор остается недостаточно определенной и подвергается частым изменениям. Например, порядок регулирования доступа к информации в сети Интернет определен рядом норм законодательства, включая ст. 15.1–15.6.1 Закона «Об информа-

² Чаннов С. Е. Ограничение доступа к отдельным видам информации в сети Интернет // Власть. 2013. № 6. С. 83–86.

³ Опалев Р. О. Проблемы ограничения доступа к информации в сети Интернет // Арбитражный и гражданский процесс. 2019. № 9. С. 48–52.

⁴ Ситкова О. Ю. Правовая природа права ребенка на доступ к информации и его ограничения в целях защиты ребенка от информации, наносящей вред психическому здоровью и развитию несовершеннолетних // Семейное и жилищное право. 2021. № 1. С. 27–30.

⁵ Алексеева М. В., Подройкина И. А. Правовой аспект формирования безопасной информационной среды, способствующей распространению традиционных российских духовно-нравственных ценностей // Правовой порядок и правовые ценности. 2023. Т. 1. № 2. С. 24–33.

⁶ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3448.

⁷ Зарубин А. А., Воробей С. Н., Лунева А. В. О правовой регламентации ограничения распространения в сети Интернет запрещенной информации // Закон и право. 2019. № 12. С. 46–49.

ции, информационных технологиях и о защите информации», но этот правовой механизм нередко изменяется для адаптации к текущим вызовам, включая киберугрозы.

По данным за 2023 г., более 500 тыс. информационных ресурсов были внесены в единый реестр запрещенной информации. В частности, блокировке подвергались сайты с экстремистским и террористическим контентом, а также ресурсы, распространяющие недостоверную информацию. Эта статистика показывает масштабы государственной работы по защите информационного пространства⁸.

Определение термина «недостоверная информация» остается особенно значимой задачей. В КоАП РФ⁹ (ст. 13.15) и УК РФ¹⁰ (ст. 207) соответствующие нарушения описаны, однако отсутствует ясность в правовом определении самого объекта защиты — недостоверной информации.

Одной из ключевых угроз выступает распространение деструктивной информации, включая экстремистскую и террористическую деятельность в сети Интернет.

Законы «О противодействии терроризму»¹¹ (2006 г.) и «О противодействии экстремистской деятельности»¹² (2002 г.) вводят такие термины, как «экстремистские материалы» и «информационная поддержка терроризма», подчеркивая, что информационно-психологическое воздействие может носить вредоносный характер.

Стратегические документы, такие как Доктрина информационной безопасности Российской Федерации¹³ (2016 г.) и Стратегия национальной безопасности Российской Федерации¹⁴ (2021 г.), отмечают важность защиты от внешнего деструктивного информационно-психологического воздействия. Например, пункт 25 Стратегии национальной безопасности определяет развитие безопасного информационного пространства, свободного от угроз, связанных с манипулированием сознанием граждан и подрывом традиционных российских ценностей.

Несмотря на явный прогресс в правовом регулировании «защиты от информации», остается множество нерешенных вопросов. Так, Ю. Б. Носова справедливо утверждает, что в законодательстве отсутствует терминологическая ясность в определении ряда понятий, таких, например, как «деструктивное информационное воздействие» или «информация, причиняющая вред общественным интересам», что создает сложности для правоприменительной практики¹⁵.

Кроме того, сегодня необходимо учитывать возрастающую роль информационного пространства как инструмента государственной и культурной политики, а также как площадки для противодействия внешнему информационному давлению. Например, в Основах государственной политики по сохранению традиционных

⁸ Роскомнадзор пошел на снижение // URL: <https://www.kommersant.ru/doc/6428080?ysclid=m70v16z73b127047547> (дата обращения: 21.02.2025).

⁹ СЗ РФ. 2002. № 1 (ч. 1). Ст. 1.

¹⁰ СЗ РФ. 1995. № 25. Ст. 2954.

¹¹ Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» // СЗ РФ. 2006. № 11. Ст. 1146.

¹² Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» // СЗ РФ. 2002. № 30. Ст. 3031.

¹³ Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

¹⁴ Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

¹⁵ Носова Ю. Б. Основания для признания информации, размещенной в сети Интернет, запрещенной к распространению: некоторые проблемы правоприменительной практики // Вестник ВГУ. Серия «Право». 2022. № 2 (49). С. 169–175.

российских духовно-нравственных ценностей¹⁶ (2022 г.) тема защиты от деструктивной информации и недостоверного контента получает особое внимание.

За последние годы Россия предприняла значительные шаги для улучшения нормативной основы регулирования в информационной сфере. Введенные инициативы включают:

- развитие законодательства, направленного на борьбу с фейковыми новостями и недостоверными данными;
- ужесточение контроля за распространением информации экстремистского и террористического характера;
- внесение изменений в правила блокировки информации в сети Интернет для защиты граждан от противоправного контента.

Однако перечисленные шаги — лишь начало пути.

В целом анализ текущего состояния правового регулирования ограничений доступа к информации, подлежащей запрету для распространения на территории РФ, указывает на существенные достижения в этой сфере. Вместе с тем имеется и ряд нерешенных проблем, связанных с дефинитивной частью. Несмотря на то что в последние годы в Российской Федерации был создан значительный массив нормативных актов, направленных на борьбу с противоправным и вредоносным контентом, сложности возникают из-за следующих факторов:

- отсутствия унифицированных и четких дефиниций ключевых понятий, таких как «недостоверная информация», «деструктивная информация», «деструктивное воздействие» и др. Это создает правовую неопределенность, усложняет правоприменительную практику и затрудняет выработку единых подходов к регулированию информационного пространства;
- частых изменений законодательства и отсутствия устойчивости нормативно-правового регулирования в области борьбы с информационными угрозами, особенно в контексте регулирования содержимого, распространяемого

через сеть Интернет. Это существенно влияет на предсказуемость правового регулирования;

- ограниченного характера гармонизации положений национального законодательства о защите информационного пространства с международными нормами и стандартами, что может ослабить эффективность правового регулирования в условиях глобального информационного взаимодействия;

- недостаточной разработанности механизмов, направленных на предупреждение и профилактику распространения вредной и недостоверной информации. В большей степени акцент сделан на блокировке, удалении или противодействии уже распространенному контенту, в то время как меры упреждающего характера, включая образовательные инициативы, остаются фрагментарными;

- проблем с юридическим оформлением прав субъектов информационных отношений, а также гарантий их реализации в контексте защиты права на достоверную и объективную информацию.

Частично решить обозначенные проблемы можно, по нашему мнению, посредством введения в действующее законодательство соответствующих дефиниций с определением их содержания:

- недостоверная информация — сведения (сообщения, данные), которые содержат фактические ошибки, умышленные искажения либо не соответствуют объективной реальности в силу заведомой неполноты представления, вводящие лиц, знакомящихся с ними, в заблуждение и препятствующие формированию объективного представления о происходящих событиях, фактах или явлениях;

- деструктивная информация — сведения (сообщения, данные), содержание которых направлено на подрыв существующих социальных, политических, культурных или моральных устоев общества, провокацию конфликтов, разжигание вражды или ненависти либо на иное негативное воздействие на гармоничное раз-

¹⁶ Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // СЗ РФ. 2022. № 46. Ст. 7977.

витие общественного взаимодействия личности и различных социальных групп;

— информационно-психологическое воздействие — целенаправленный процесс передачи и распространения информации с целью оказания влияния на эмоциональное, когнитивное и поведенческое состояние индивида или социальных групп посредством методов убеждения, внушения, манипуляции, провоцирующих изменения в восприятии событий, фактов и явлений, в мировоззрении и мотивации;

— деструктивное информационно-психологическое воздействие — целенаправленный процесс передачи и распространения информации с применением таких методов информационного и психологического манипулирования, которые приводят к разрушительным последствиям для эмоционального состояния, когнитивного восприятия или поведения, наносящим вред индивиду, группам либо обществу путем нарушения социальной согласованности, усиления конфликтов, снижения уровня доверия или формирования неблагоприятных установок.

В условиях ускоренного развития цифровых технологий и угроз информационного противоборства, на наш взгляд, также необходимо:

1. Внести поправки в уголовное и административное законодательство, а именно пересмотреть статьи, регулирующие ответственность за распространение заведомо ложной, экстремистской и деструктивной информации. Для этого предлагаем:

1.1. Определить новую категорию правонарушений («инфотоксичные действия»): введение термина «инфотоксичность» необходимо для обозначения намеренного создания дезинформации или манипулятивного контента, способного нанести вред общественным институтам, национальной безопасности или личным правам.

1.2. Начать разработку комплекса мер административной и уголовной ответственности за формирование и распространение деструктивного контента через алгоритмы искусственного интеллекта (ИИ). В частности, необходимым видится введение ответственности за нарушения, совершаемые посредством использования автоматизированных систем (ботов), языковых

моделей ИИ для распространения недостоверной информации, а также за умышленный обход систем государственной модерации.

1.3. Внести поправки в статьи УК РФ (например, в ст. 280 «Публичные призывы к экстремистской деятельности», ст. 207 «Заведомо ложное сообщение об акте терроризма» и др.), направленные на ужесточение ответственности в случаях совершения преступлений посредством распространения информации через трансграничные интернет-ресурсы.

1.4. Установить административную ответственность для компаний, предоставляющих хостинговые услуги, VPN-сервисы или иные технологии, обеспечивающие сокрытие личности субъекта, связанного с распространением незаконного контента.

2. Внести поправки в Закон «Об информации, информационных технологиях и о защите информации». Современные интернет-реалии требуют модернизации действующего законодательства в области взаимодействия с трансграничными ресурсами, которые зачастую не подчиняются российскому праву. Для этого необходимо:

2.1. Проводить обязательную сертификацию иностранных цифровых платформ, в частности ввести обязательный процесс регистрации транснациональных платформ в России, включая блокчейн-реестры, социальные сети и мессенджеры. Законодательно можно рекомендовать установить запрет на деятельность платформ, игнорирующих российские информационные нормативы.

2.2. Ввести обязательное требование для интернет-компаний использовать алгоритмы, распознающие деструктивный контент и маркирующие недостоверные материалы пояснением о проверке источников.

2.3. Установить стандарты прозрачности ИИ, а именно ввести обязательный механизм маркировки материалов, созданных алгоритмами ИИ. Это поможет бороться с дезинформацией, которая создается и распространяется с использованием высокотехнологичных решений.

3. Внести изменения в стратегические документы, касающиеся информационной безопасности, такие как Стратегия национальной

безопасности РФ и Доктрина информационной безопасности РФ:

3.1. Актуализировать цели и задачи стратегического управления, а именно включить в содержание нормативного документа положения о противодействии трансграничным информационным атакам и деструктивному контенту как одному из приоритетных направлений обеспечения национальной безопасности. При этом сделать акцент на необходимости формирования правовых механизмов, регулирующих транснациональный поток данных и ответственность трансграничных платформ.

3.2. Ускорить процесс подготовки разработок по вопросам «киберсуверенитета»: расширить положения о «суверенном Интернете», включая требования об обязательности локального хранения данных для транснациональных платформ и мессенджеров, и создать концепт «национальной информационной границы», включающий набор инструментов фильтрации, анализа и санкционирования трансграничного контента.

3.3. Сформировать центральный орган управления интернет-пространством: создать федеральный центр анализа и мониторинга распространения деструктивной информации в информационном пространстве (включая ИИ-инструменты машинного обучения) с правом оперативного вмешательства на базе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

4. Разработать инновационные правовые механизмы для адаптации законодательства к новым вызовам:

4.1. Ввести в законодательство механизм «облегченной модификации правовых норм» в сфере информационной безопасности, что позволит оперативно реагировать на технологические изменения (например, создание

новых алгоритмов ИИ или форм дезинформации). Для этого можно использовать институт административного нормотворчества в рамках государственной экспертизы и общественного обсуждения.

4.2. Законодательно закрепить необходимость проведения анализа содержания новых правовых актов в области информационной безопасности с привлечением междисциплинарных экспертов — специалистов в области юриспруденции, социологии, информационных технологий и международных отношений.

На наш взгляд, вышеуказанные поправки и предложения позволят более эффективно адаптировать правовую систему к новым вызовам цифровой эпохи, обеспечивая баланс между безопасностью и свободой информации.

Создание безопасного, структурированного и основанного на правовой определенности информационного пространства знаний является важной задачей стратегии развития информационного общества. Это гарантирует укрепление информационного суверенитета России, реализацию государственной политики по защите граждан от вредоносного контекста, способствует культурному, образовательному и технологическому развитию. Реализация предложенных мер обеспечит повышение уровня достоверности и безопасности информации, минимизацию угроз информационного манипулирования, а также укрепление доверия граждан к механизмам государственной защиты в информационной среде.

Полагаем, что, формируя четкое и гибкое законодательное пространство, Россия сможет эффективно противостоять глобальным вызовам в сфере информационной безопасности, добиваясь политической стабильности и социальной гармонии.

БИБЛИОГРАФИЯ

1. Алексеева М. В., Подройкина И. А. Правовой аспект формирования безопасной информационной среды, способствующей распространению традиционных российских духовно-нравственных ценностей // Правовой порядок и правовые ценности. — 2023. — Т. 1. — № 2. — С. 24–33.
2. Зарубин А. А., Воробей С. Н., Лунева А. В. О правовой регламентации ограничения распространения в сети Интернет запрещенной информации // Закон и право. — 2019. — № 12. — С. 46–49.

3. Носова Ю. Б. Основания для признания информации, размещенной в сети Интернет, запрещенной к распространению: некоторые проблемы правоприменительной практики // Вестник ВГУ. Серия «Право». — 2022. — № 2 (49). — С. 169–175.
4. Опалев Р. О. Проблемы ограничения доступа к информации в сети Интернет // Арбитражный и гражданский процесс. — 2019. — № 9. — С. 48–52.
5. Роскомнадзор пошел на снижение // URL: <https://www.kommersant.ru/doc/6428080?ysclid=m70v16z73b127047547> (дата обращения: 21.02.2025).
6. Ситкова О. Ю. Правовая природа права ребенка на доступ к информации и его ограничения в целях защиты ребенка от информации, наносящей вред психическому здоровью и развитию несовершеннолетних // Семейное и жилищное право. — 2021. — № 1. — С. 27–30.
7. Чаннов С. Е. Ограничение доступа к отдельным видам информации в сети Интернет // Власть. — 2013. — № 6. — С. 83–86.

Материал поступил в редакцию 21 февраля 2025 г.

REFERENCES (TRANSLITERATION)

1. Alekseeva M. V., Podroykina I. A. Pravovoy aspekt formirovaniya bezopasnoy informatsionnoy sredy, sposobstvuyushchey rasprostraneniyu traditsionnykh rossiyskikh dukhovno-nravstvennykh tsennostey // Pravovoy poryadok i pravovye tsennosti. — 2023. — Т. 1. — № 2. — С. 24–33.
2. Zarubin A. A., Vorobey S. N., Luneva A. V. O pravovoy reglamentatsii ogranicheniya rasprostraneniya v seti Internet zapreshchennoy informatsii // Zakon i pravo. — 2019. — № 12. — С. 46–49.
3. Nosova Yu. B. Osnovaniya dlya priznaniya informatsii, razmeshchennoy v seti Internet, zapreshchennoy k rasprostraneniyu: nekotorye problemy pravoprimenitelnoy praktiki // Vestnik VGU. Seriya «Pravo». — 2022. — № 2 (49). — С. 169–175.
4. Opalev R. O. Problemy ogranicheniya dostupa k informatsii v seti Internet // Arbitrazhnyy i grazhdanskiy protsess. — 2019. — № 9. — С. 48–52.
5. Roskomnadzor poshel na snizhenie // URL: <https://www.kommersant.ru/doc/6428080?ysclid=m70v16z73b127047547> (data obrashcheniya: 21.02.2025).
6. Sitkova O. Yu. Pravovaya priroda prava rebenka na dostup k informatsii i ego ogranicheniya v tselyakh zashchity rebenka ot informatsii, nanosyashchey vred psikhicheskomu zdorovyu i razvitiyu nesovershennoletnikh // Semeynoe i zhilishchnoe pravo. — 2021. — № 1. — С. 27–30.
7. Channov S. E. Ogranichenie dostupa k otdelnym vidam informatsii v seti Internet // Vlast. — 2013. — № 6. — С. 83–86.