Чакрян Артур Сетракович
магистр
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации
эксперт по информповестке
Фонд помощи «Русский Крест»
г. Москва

РЕАЛИЗАЦИЯ ПРИНЦИПА «СУВЕРЕННОГО ИНТЕРНЕТА» КАК ИНСТРУМЕНТ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ: ПРАВОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ

Аннотация: *статья посвящена исследованию правовых и технологических аспектов реализации принципа «суверенного интернета» в Российской Федерации. Автором анализируется Федеральный закон от 01.05.2019 №90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации», внесенные в 2025–2026 гг. изменения в законодательство, а также подзаконные акты, регламентирующие деятельность Роскомнадзора в сфере централизованного управления сетью связи общего пользования. Рассматриваются теоретические подходы к пониманию цифрового суверенитета в отечественной и зарубежной науке, выявляются проблемы правоприменения и технологической реализации нового регулирования.*

Ключевые слова: *суверенный интернет, цифровой суверенитет, информационная безопасность, Роскомнадзор, ТСПУ, государственное регулирование, централизованное управление сетью связи.*

Введение

Актуальность темы цифрового суверенитета в современной России обусловлена несколькими взаимосвязанными факторами. Во-первых, это рост геополитической напряженности и санкционное давление, сопровождающееся

угрозами отключения Российской Федерации от глобальной сети Интернет со стороны иностранных государств и негосударственных структур. Во-вторых, это необходимость обеспечения информационной безопасности и суверенитета государства в условиях, когда критическая информационная инфраструктура страны продолжает технологически зависеть от зарубежных корневых серверов доменных имен. В-третьих, это эволюция международно-правовых подходов к регулированию киберпространства, где все большее значение приобретают концепции «цифрового суверенитета» и «информационной самодостаточности».

Настоящее исследование ставит своей целью комплексный анализ правовых и технологических аспектов реализации принципа «суверенного интернета» в Российской Федерации, выявление проблем правоприменения и оценку эффективности существующих механизмов государственного регулирования в данной сфере.

1. Теоретико-правовые основы концепции цифрового суверенитета

1.1. Эволюция подходов к суверенитету в киберпространстве

В развитии суверенитета государства в цифровом пространстве выделяют три этапа. Первый – кибернигилизм (отрицание суверенитета над киберпространством), ярким выражением которого стала «Декларация независимости киберпространства» Джона Барлоу (1996 г.). Второй – юрисдикционный компромисс (применение национальной юрисдикции без формального объявления суверенитета). Третий – цифровой реализм (полное распространение государственного суверенитета на киберпространство). Международно-правовое обоснование этого подхода содержится в резолюциях Генеральной Ассамблеи ООН, где подтверждены суверенное равенство государств и невмешательство во внутренние дела в сфере информационной безопасности. Таким образом, цифровой суверенитет – не отступление от либеральных принципов, а реализация неотъемлемых прав государства.

1.2. Понятие и содержание цифрового суверенитета в российской науке

В российской юридической науке «цифровой суверенитет» – способность государства независимо от внешних акторов формировать и реализовывать национальную политику в цифровой сфере, обеспечивая безопасность личности, общества и государства (С.А. Спартак).

Ключевые элементы цифрового суверенитета:

1. Технологическая независимость (критическая ИТ-инфраструктура, системы доменных имен и адресации);

2. Регуляторная автономия (право устанавливать правила работы сети на своей территории);

3. Информационная безопасность (защита от внешних деструктивных воздействий).

Стратегические документы РФ:

- доктрина информационной безопасности (Указ №646 от 05.12.2016);

- стратегия национальной безопасности (Указ №400 от 02.07.2021).

Они закрепляют курс на обеспечение национальных интересов в информационной сфере, включая создание системы устойчивой работы российского сегмента Интернета при внешних угрозах.

2. Нормативно-правовая база реализации принципа «суверенного интернета» в РФ

2.1. Федеральный закон №90-ФЗ как основа «суверенного Рунета»

Федеральный закон от 01.05.2019 №90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» (далее – Закон №90-ФЗ) стал первым системным актом, закрепившим механизмы обеспечения устойчивости российского сегмента интернета.

Закон №90-ФЗ предусматривает два основных направления регулирования:

- *создание национальной системы доменных имен* – дублирование на территории РФ списка доменных имен и сетевых адресов, что позволяет обеспечивать работоспособность российских ресурсов даже при отключении от глобальных корневых серверов.

- *закон №90-ФЗ* предусматривает установку на сетях операторов связи технических средств противодействия угрозам (ТСПУ), которые фильтруют трафик и ограничивают доступ к запрещённой информации. Закон изначально носил рамочный характер – предполагалась последующая разработка подзаконных актов (порядок создания и сертификации ТСПУ, правила централизованного управления сетью, перечень угроз). К моменту вступления закона в силу (1 ноября 2019 г.) значительная часть этих актов отсутствовала, что вызывало опасения отрасли, но в последующие годы правовая база была систематически дополнена.

3. *Актуальные изменения законодательства* (*2025–2026 гг*.)

Значительные изменения в законодательство об информации и информационных технологиях были внесены в конце 2025 г. Федеральным законом от 29.12.2025 №568-ФЗ. Данный нормативный правовой акт, вступающий в силу с 1 сентября 2026 г., вносит корректировки в Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Среди наиболее значимых новелл следует выделить:

1.1. *Детализацию правового режима государственных информационных систем* (*ГИС*). Закон вводит новую категорию «иные информационные системы государственных органов», создаваемые для организационного, информационного, документационного и иного обеспечения деятельности госорганов. При этом установлено, что для обеспечения создания и эксплуатации ГИС допускается использование технических средств и программ, доступ к которым предоставляется с использованием информационно-телекоммуникационных сетей в порядке, установленном Правительством РФ.

1. 2. *Усиление требований к информационной безопасности ГИС*. Операторы государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий и учреждений обязаны обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), включая информирование о компьютерных инцидентах, повлекших

неправомерную передачу содержащейся в указанных информационных системах информации.

Уточнение перечня угроз устойчивости Рунета. Постановлением Правительства РФ от 27 октября 2025 г. (вступает в силу 1 марта 2026 г.) утверждена новая редакция Правил централизованного управления сетью связи. В перечень угроз для вмешательства Роскомнадзора в маршрутизацию трафика включены: пропуск трафика от автономных систем-нарушителей; доступ к ресурсам по продаже средств связи без подтверждения соответствия; отказ хостинг-провайдера от учений по устойчивости Рунета. Эксперты называют изменения эволюционными, формализующими уже сложившуюся практику.

Роль Роскомнадзора в механизме реализации цифрового суверенитета

Ключевая роль отведена Роскомнадзору, который выступает центральным элементом управления российским сегментом сети Интернет. Полномочия включают: централизованное управление сетью связи при угрозах устойчивости; ведение реестров точек обмена трафиком и автономных систем; координацию установки и эксплуатации ТСПУ; выдачу предписаний об ограничении доступа к ресурсам. С 1 марта 2026 г. за Роскомнадзором закрепляется статус «единого центра управления» российским интернет-трафиком – из правил исчез чёткий перечень участников управления, всё замыкается на Роскомнадзор.

Технологические аспекты

Технические средства противодействия угрозам (ТСПУ). ТСПУ устанавливаются на сетях операторов за счёт государства и предназначены для фильтрации трафика. Функции: глубокий анализ пакетов (DPI); блокировка доступа к запрещённым ресурсам; перенаправление трафика при угрозах. Современные ТСПУ позволяют вычислять обходные сервисы (VPN, прокси). Роскомнадзору выделено 2,27 млрд руб. на внедрение машинного обучения для блокировки контента по смысловому содержанию.

Инфраструктурная независимость. Создаётся национальная система доменных имён – копия глобального реестра для доступа к зонам.ru и.рф при отключении от корневых серверов. В России уже функционирует 11 корневых серверов.

Оценка эффективности и проблемы правоприменения

Правовая и технологическая база «суверенного интернета» в целом сформирована: ТСПУ установлены у всех крупных операторов, создана нормативная основа для централизованного управления. Системные проблемы:

1. Зависимость от зарубежных технологий (сохраняются потенциальные уязвимости).

2. Проблемы эффективности фильтрации (переблокировка легальных ресурсов, сохранение доступа к запрещённой информации).

3. Правовая неопределённость понятия «угрозы» (оценочные формулировки, риски произвольного правоприменения).

4. Нагрузка на операторов связи.

Баланс безопасности и прав человека

Возникает вопрос о соотношении мер по обеспечению цифрового суверенитета с конституционными правами на свободу информации (ст. 29) и неприкосновенность частной жизни (ст. 23). Цифровой суверенитет ограничен обязательствами по международному праву в сфере прав человека. В российской системе баланс обеспечивается через судебный контроль и ведомственное нормотворчество, однако существующие механизмы, по мнению экспертов, не всегда эффективно защищают права граждан в условиях массовой фильтрации трафика.

Заключение

Проведенное исследование позволяет сформулировать следующие основные выводы.

1. Реализация принципа «суверенного интернета» в Российской Федерации представляет собой комплексную систему правовых и технологических мер, направленных на обеспечение национальной информационной безопасности в условиях геополитической нестабильности и технологической зависимости. Ключевым нормативным актом в данной сфере является Федеральный закон №90-ФЗ, на основе которого создана и постоянно совершенствуется правовая база централизованного управления сетью связи общего пользования.

2. В 2025–2026 гг. российское законодательство в сфере информационных технологий и информационной безопасности претерпело значительные изменения, направленные на расширение полномочий Роскомнадзора, детализацию перечня угроз и упорядочение правового режима государственных информационных систем. Эти изменения эксперты оценивают как «эволюционное развитие» уже существующей системы, а не как революционный пересмотр подходов к регулированию.

3. Основной технологической составляющей «суверенного интернета» является система технических средств противодействия угрозам (ТСПУ), позволяющая осуществлять глубокую фильтрацию трафика и централизованное управление маршрутизацией в сети. Дополнительным механизмом обеспечения устойчивости выступает создание национальной инфраструктуры доменных имен.

4. Несмотря на достигнутые результаты, сохраняется ряд проблем, требующих дальнейшего решения: технологическая зависимость от зарубежных решений, неабсолютная эффективность фильтрации, правовая неопределенность отдельных понятий. Кроме того, сохраняется актуальность поиска баланса между мерами государственного регулирования и конституционными правами граждан на свободу информации и неприкосновенность частной жизни.

В качестве перспективных направлений дальнейших исследований могут быть выделены: анализ практики применения новой редакции Правил централизованного управления сетью связи (с 1 марта 2026 г.), оценка эффективности технологий машинного обучения при фильтрации контента, сравнительно-правовой анализ подходов к цифровому суверенитету в России и зарубежных государствах.

Список литературы

1. Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 29.12.2025) // СПС «КонсультантПлюс».

3. Федеральный закон от 29.12.2025 № 568-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // Официальный интернет-портал правовой информации. – URL: http://kremlin.ru/acts/bank/52812 (дата обращения: 10.05.2026).

4. Спартак С.А. Особенности цифрового суверенитета: международно-правовой подход / С.А. Спартак // Пробелы в российском законодательстве. – 2025. – Т. 18, № 6. – С. 150–159. DOI 10.33693/2072-3164-2025-18-6-150-159. EDN SNMGKL

5. Спартак С.А. Legal foundations of digital sovereignty in the Russian Federation / С.А. Спартак // Пробелы в российском законодательстве. – 2025. – Т. 18, № 5. – С. 25–34. DOI 10.33693/2072-3164-2025-18-5-25-34. EDN SENMDB

6. Вавилин М.В. State regulation of the «digital sovereignty» in Russia: On the role of the federal service for communications, information technologies and mass media / М.В. Вавилин, Д.И. Башкин // Пробелы в российском законодательстве. – 2025. – Т. 18, № 7. – С. 17–24. DOI 10.33693/2072-3164-2025-18-7-17-24. EDN YXGSLV

7. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

8. Постановление Правительства РФ от 27.10.2025 «Об утверждении Правил централизованного управления сетью связи общего пользования» (ред. от 2025 г.) // СПС «КонсультантПлюс».

9. Капустин А.Я. Суверенитет государства в киберпространстве: международно-правовое измерение / А.Я. Капустин // Журнал зарубежного законодательства и сравнительного правоведения. – 2022. – Т. 18, № 6. – С. 99–108. DOI 10.12737/jflcl.2022.079. EDN LJJMUS

10. О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» : Федеральный закон от 01.05.2019 № 90-ФЗ // Собрание законодательства РФ. – 2019. – № 18. – Ст. 2214.

11. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» : Федеральный закон от 29.12.2025 № 568-ФЗ // Собрание законодательства РФ. – 2026. – № 1 (часть I). – Ст. 15.

12. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

13. Об утверждении Правил централизованного управления сетью связи общего пользования : Постановление Правительства РФ от 27.10.2025 № 1423 // Собрание законодательства РФ. – 2025. – № 44. – Ст. 6215.

14. Спартак С.А. Особенности цифрового суверенитета: международно-правовой подход / С.А. Спартак // Пробелы в российском законодательстве. – 2025. – Т. 18, № 6. – С. 150–159. DOI 10.33693/2072-3164-2025-18-6-150-159. EDN SNMGKL

15. Вавилин М.В. Государственное регулирование «цифрового суверенитета» в России: о роли Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций / М.В. Вавилин, Д.И. Башкин // Пробелы в российском законодательстве. – 2025. – Т. 18, № 7. – С. 17–24. DOI 10.33693/2072-3164-2025-18-7-17-24. EDN YXGSLV

16. Капустин А.Я. Суверенитет государства в киберпространстве: международно-правовое измерение / А.Я. Капустин // Журнал зарубежного законодательства и сравнительного правоведения. – 2022. – Т. 18, № 6. – С. 99–108. DOI 10.12737/jflcl.2022.079. EDN LJJMUS