

Правовое регулирование суверенизации интернета в России: современные вызовы и приоритеты

Научный руководитель – Зуева Анна Сергеевна

Матвеев Аркадий Андреевич

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия

E-mail: ark.matv1@gmail.com

Правовое регулирование суверенизации интернета в Российской Федерации представляет собой институционализированное направление государственной политики, закреплённое в системе нормативных правовых актов, направленных на обеспечение устойчивости, безопасности и автономности функционирования национального сегмента сети Интернет. Актуальность данной проблематики обусловлена необходимостью правового обеспечения защиты критической информационной инфраструктуры, минимизации рисков внешнего воздействия на сетевые ресурсы, а также реализации принципа государственного суверенитета в цифровой среде. В отличие от декларативных подходов, современная модель регулирования основывается на конкретных законодательных механизмах, закрепляющих полномочия органов государственной власти и устанавливающих обязательные требования для участников информационных отношений.

Ключевым нормативным актом в данной сфере является Федеральный закон от 1 мая 2019 г. № 90-ФЗ, внесший изменения в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации». Указанный закон сформировал правовую основу для создания механизма централизованного управления сетями связи общего пользования, включая внедрение технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования сети Интернет на территории Российской Федерации. Существенным элементом правового регулирования является закрепление полномочий федерального органа исполнительной власти в области связи, прежде всего Роскомнадзора, в части координации функционирования инфраструктуры, управления маршрутизацией трафика и осуществления контроля за операторами связи.

Развитие положений указанного закона осуществляется посредством подзаконного нормативного регулирования, включая постановления Правительства Российской Федерации и акты уполномоченных органов, в частности Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Данные акты устанавливают порядок установки, эксплуатации и модернизации технических средств противодействия угрозам, требования к взаимодействию операторов связи с государственными органами, а также процедуры мониторинга и реагирования на угрозы устойчивости сети. Важное значение имеет формирование национальной системы доменных имен, включая создание инфраструктуры, обеспечивающей независимость функционирования доменной зоны .ru и иных национальных доменов.

Особое место в системе правового регулирования занимает Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который устанавливает правовые основы защиты значимых объектов информационной инфраструктуры, включая сети связи, информационные системы

и автоматизированные системы управления. Данный закон вводит режим категорирования объектов, определяет обязанности субъектов критической информационной инфраструктуры по обеспечению безопасности, а также закрепляет полномочия государственных органов в сфере контроля и надзора. Его положения находятся в тесной взаимосвязи с законодательством о суверенном интернете, формируя комплексный механизм обеспечения устойчивости цифровой среды.

Вместе с тем правовое регулирование суверенизации интернета сопряжено с необходимостью соблюдения конституционных гарантий, закреплённых в Конституции Российской Федерации, в частности права на свободный поиск, получение, передачу, производство и распространение информации, а также тайны связи. Ограничения указанных прав допускаются исключительно на основании федерального закона и при соблюдении принципа соразмерности, что обуславливает необходимость чёткого нормативного определения оснований и процедур применения мер по ограничению доступа к информации, фильтрации трафика и управлению сетевой инфраструктурой. В этой связи значительную роль играет правоприменительная практика, включая акты судебных органов, оценивающих законность и обоснованность действий уполномоченных субъектов.

Дополнительным элементом правового регулирования выступают нормы, направленные на локализацию данных и обеспечение хранения информации на территории Российской Федерации, закреплённые, в частности, в законодательстве о персональных данных. Установление обязанности операторов по хранению и обработке данных российских пользователей на территории государства рассматривается как инструмент укрепления цифрового суверенитета, однако вызывает дискуссии с точки зрения соотношения с международными обязательствами и принципами трансграничного обмена информацией.

Особенного внимания в контексте правового регулирования суверенизации интернета заслуживает институт ограничения доступа к информации, реализуемый на основании положений Федерального закона «Об информации, информационных технологиях и о защите информации». В рамках данного закона сформирован механизм ведения единого реестра запрещённой информации, а также установлен порядок ограничения доступа к информационным ресурсам, распространяющим сведения, запрещённые законодательством Российской Федерации. Существенным элементом данного регулирования является закрепление процедурного порядка взаимодействия между Роскомнадзором, операторами связи и владельцами информационных ресурсов, включая сроки исполнения требований и основания для включения ресурсов в реестр. При этом правовая конструкция данных мер продолжает вызывать дискуссии в части достаточности процессуальных гарантий для владельцев сайтов и пользователей, а также прозрачности принимаемых решений.

Отдельным направлением нормативного регулирования выступает правовое закрепление обязанностей организаторов распространения информации в сети Интернет, включая требования по хранению сообщений пользователей и предоставлению их по запросу уполномоченных органов. Указанные положения, вытекающие из так называемого «пакета Яровой» (Федеральный закон № 374-ФЗ и № 375-ФЗ от 6 июля 2016 г.), усиливают контроль государства за цифровыми коммуникациями и направлены на обеспечение задач в сфере противодействия терроризму и обеспечения государственной безопасности. Вместе с тем их реализация сопряжена с существенными затратами для бизнеса и вызывает правовые вопросы, связанные с обеспечением тайны связи и защитой персональных данных.

Следует также отметить развитие регулирования в части использования средств криптографической защиты информации и установления требований к их сертификации и применению. Законодательство предусматривает необходимость использования сертифицированных средств защиты информации в ряде сфер, а также закрепляет полномочия уполномоченных органов по контролю за соблюдением данных требований. Это направ-

ление правового регулирования непосредственно связано с задачами обеспечения технологического суверенитета и защиты информации от несанкционированного доступа.

Важным аспектом является и формирование правового режима функционирования иностранных цифровых платформ на территории Российской Федерации. В последние годы принят ряд нормативных актов, обязывающих крупные иностранные IT-компании открывать представительства на территории Российской Федерации, соблюдать требования национального законодательства в части удаления запрещённой информации и взаимодействовать с государственными органами. Данные меры направлены на устранение правового вакуума в отношении транснациональных субъектов цифровой экономики и укрепление юрисдикционного контроля государства над информационным пространством.

Таким образом, нормативная модель суверенизации интернета в Российской Федерации характеризуется высокой степенью формализации и опирается на совокупность федеральных законов и подзаконных актов, регулирующих как организационно-технические, так и правовые аспекты функционирования сети. Современные вызовы связаны преимущественно с необходимостью адаптации действующего законодательства к быстро меняющимся технологическим условиям, устранения правовых неопределённостей и обеспечения баланса между публичными интересами государства и конституционными правами субъектов информационных отношений. Перспективы развития правового регулирования в данной сфере предполагают дальнейшую детализацию механизмов реализации уже принятых норм и повышение их юридической определённости.

Источники и литература

- 1) Залоило М.В. Правовые проблемы обеспечения технологического суверенитета. *Journal of Digital Technologies and Law*. 2024;2(3):500-520.
- 2) Степанов П. В. Подходы к пониманию цифрового суверенитета России. 2024; Журнал российского права, 28(4), 37-51.
- 3) Тихомиров Ю. А. Правовое управление в кризисных ситуациях: монография. 2022; Москва: Проспект. <https://elibrary.ru/medwfm>
- 4) Ваховский А.М. Политико-правовые вопросы регулирования Интернета: мировой опыт и российская практика // Известия Тульского государственного университета. 2016. Вып.2. С.3-11.