Состояние интернета и цифровых прав в Российской Федерации (2019-2025)

Отчет представляет собой всесторонний анализ трансформации российского интернет-пространства за последние шесть лет. В документе подробно рассматривается, как под прикрытием "защиты суверенитета" и "борьбы с угрозами" в России была планомерно выстроена одна из самых сложных и многоуровневых систем государственной цензуры в мире. От законодательных инициатив, таких как "закон о суверенном интернете", до создания сложной технической инфраструктуры для глубокой фильтрации трафика (ТСПУ) — отчет последовательно раскрывает механизмы, которые подготовили почву для беспрецедентного контроля над цифровой сферой.

2025 год стал поворотным моментом, когда теоретические возможности системы контроля были применены на практике с невиданным размахом. Этот отчет детально освещает ключевые события этого года: переход от блокировки отдельных ресурсов к массовым отключениям мобильного интернета в десятках регионов страны, которые превратились из экстренной меры в рутинный инструмент. Более того, в документе анализируется качественно новый этап цензуры — введение так называемых "белых списков", которые фундаментально меняют саму парадигму доступа к информации по принципу "запрещено все, что не разрешено".

Что это означает для будущего интернета в России? Как новые технологии влияют на базовые права граждан и свободу слова? Настоящий отчет не просто констатирует факты, а предлагает глубокое погружение в детали, анализируя технические, правовые и социальные аспекты этих изменений. Он предоставляет читателю исчерпывающую картину того, как цифровая среда в России эволюционировала от относительно свободной к жестко контролируемой, и какие риски это несет для общества.

> **Дисклеймер**: Настоящий документ был частично сгенерирован с использованием нескольких больших языковых моделей (LLM). Информация, представленная в нем, основана на анализе и обобщении данных из указанных источников, однако процесс ее структурирования, обобщения и изложения был выполнен при помощи технологий искусственного интеллекта. Рекомендуется использовать данный текст как отправную точку для дальнейшего исследования и перепроверять критически важные данные по первоисточникам.

Оглавление

1. Общие сведения

1.1. Географическое положение

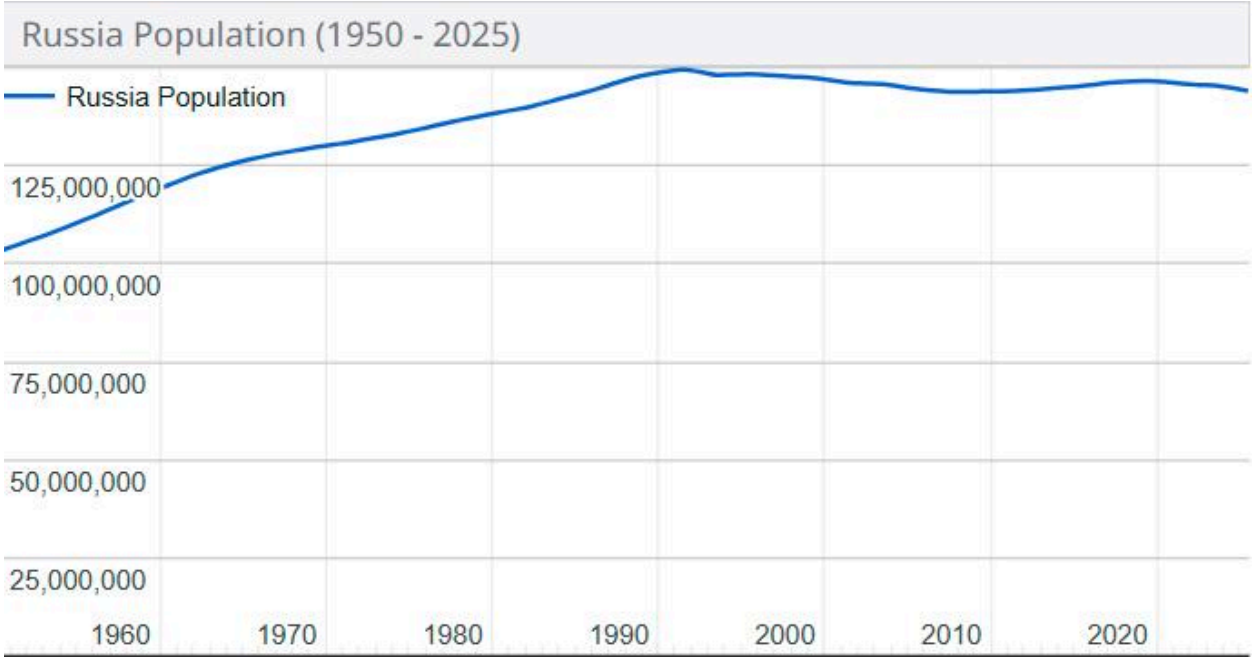
Российская Федерация – крупнейшее по площади государство мира, расположенное в Восточной Европе и Северной Азии. Страна омывается водами Тихого и Северного Ледовитого океанов, а также Балтийского, Черного, Азовского морей Атлантического океана и Каспийского моря. Российская Федерация имеет сухопутные границы с восемнадцатью странами. Географическое положение определяет многообразие климатических зон, богатые природные ресурсы и значительное геополитическое влияние страны, что, в свою очередь, оказывает воздействие на развитие инфраструктуры, включая телекоммуникационную сеть.

1.2. Население

Население Российской Федерации характеризуется значительной неравномерностью распределения по обширной территории страны, с наибольшей концентрацией жителей в европейской части. Демографическая ситуация в последние годы остается сложной. Наблюдается естественная убыль населения, которая лишь частично компенсируется миграционным приростом, причем последний также демонстрирует нестабильную динамику. Например, по данным на 2023 год, годовой прирост населения был отрицательным (-0.3%), а чистая миграция в 2024 году оценивалась как отрицательная величина, составляющая -178 042 человека.[1] Средняя ожидаемая продолжительность жизни при рождении в 2023 году достигла 73 лет [1], что свидетельствует о постепенном улучшении этого показателя, однако он все еще уступает уровням многих экономически развитых стран.

Динамика численности населения Российской Федерации представлена в таблице ниже. Данные указывают на общую тенденцию к сокращению численности населения в рассматриваемый период.

График 1: Динамика численности населения Российской Федерации (1950-2025)



Источник: worldometers.info

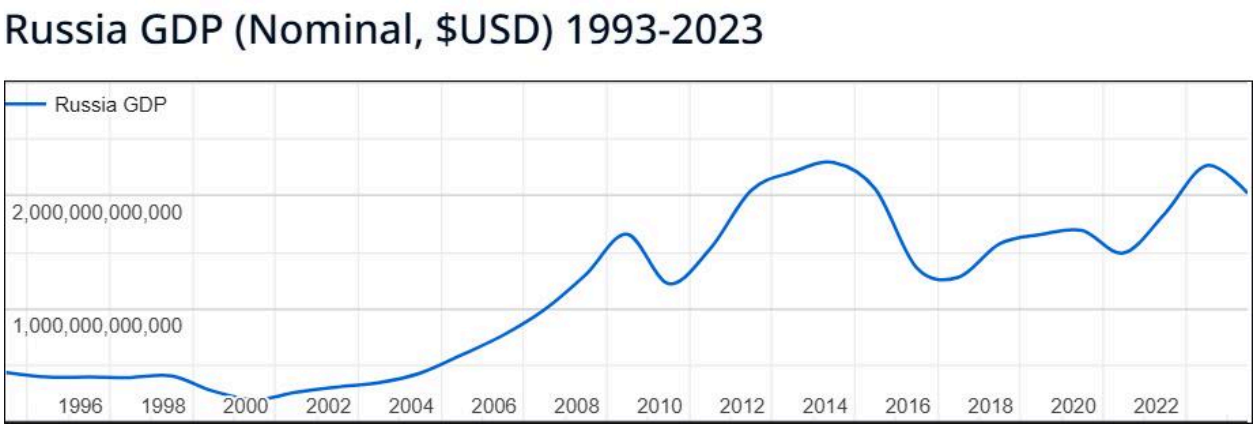
Уменьшение численности населения, особенно если оно сопровождается отрицательной чистой миграцией, как показывают данные за 2023-2024 годы [1], может в долгосрочной перспективе привести к сокращению внутреннего рынка и нехватке рабочей силы. Это, в свою очередь, способно замедлить развитие трудоемких секторов ИТ-индустрии, несмотря на государственные усилия по импортозамещению и поддержке технологического сектора. Сокращение общего числа молодых специалистов может усугубить уже существующую проблему нехватки квалифицированных кадров в высокотехнологичных отраслях.

1.3. Внутренний валовый продукт

Экономика Российской Федерации в значительной степени ориентирована на экспорт сырьевых товаров, в первую очередь нефти и газа. Эта структурная особенность делает динамику ВВП страны чувствительной к колебаниям мировых цен на энергоносители, а также к изменениям геополитической обстановки, включая международные санкции.[6] В рассматриваемый период экономика России переживала как фазы роста, так и периоды спада, что отражало как глобальные экономические циклы, так и специфические вызовы, стоящие перед страной. По данным Всемирного банка, ВВП России в 2023 году составил

2021.42 млрд долларов США.[7] В мировых рейтингах по объему ВВП Россия занимает различные позиции в зависимости от методики расчета (номинальный ВВП или ВВП по паритету покупательной способности).[6]

График 2: Динамика номинального ВВП Российской Федерации (1993-2023)



Источник: worldometers.info

Значительные колебания ВВП в долларовом эквиваленте при более стабильном, хотя и не всегда высоком, росте в рублевом выражении [9] указывают на высокую зависимость внешней оценки состояния российской экономики от курса национальной валюты. Курс рубля, в свою очередь, подвержен сильному влиянию мировых цен на энергоносители и геополитических факторов, включая санкционные режимы.[6] Такая волатильность создает атмосферу неопределенности для иностранных инвесторов и компаний, оперирующих на российском рынке, что особенно актуально для технологического сектора, который часто зависит от импорта оборудования, программного обеспечения и комплектующих.

Прогнозы роста ВВП от Всемирного Банка на уровне 1.6% в 2025 году и 1.1% в 2026 году [11] свидетельствуют об ожидаемом замедлении темпов экономического развития. Это, в сочетании с упоминаемыми банком "ограничениями производственных мощностей, включая трудовые ресурсы" [11], может привести к тому, что государство будет вынуждено более избирательно подходить к финансированию крупных инфраструктурных проектов. В число таких проектов входят и те, что связаны с обеспечением так называемого "суверенного интернета".[13] Потенциальное сокращение доступных ресурсов может замедлить реализацию этих инициатив или потребовать перераспределения средств из других важных секторов экономики и социальной сферы.

1.4. Основные экономические характеристики

Российская экономика в период с 2019 по 2025 год характеризовалась чередованием периодов роста и рецессии, что во многом было обусловлено внешними шоками, такими как пандемия COVID-19 и введение масштабных международных санкций. Ключевыми отраслями, формирующими ВВП страны, остаются добыча полезных ископаемых (прежде всего нефти и газа), обрабатывающая промышленность, сельское хозяйство и динамично развивающаяся сфера услуг, включая информационные технологии и телекоммуникации.[6] Несмотря на определенные успехи в отдельных секторах, экономика продолжает сталкиваться с рядом системных структурных проблем. К ним относятся высокая зависимость от экспорта сырьевых ресурсов, недостаточный уровень диверсификации экономической структуры, технологическое отставание в ряде отраслей, сложности с привлечением инвестиций, проблемы коррупции и неблагоприятные демографические

тенденции.[6]

В 2023 году, по предварительным оценкам, рост ВВП составил 3.6%, однако Всемирный банк прогнозирует замедление этого показателя до 3.4% в 2024 году и до 1.6% в 2025 году.[6] Наблюдается тенденция к снижению доли внешнеторгового оборота в структуре ВВП: по итогам 2023 года доля импорта сократилась до 19.1%, а доля экспорта товаров и услуг достигла рекордно низкого уровня в 23.3%.[6] Эта динамика, отчасти обусловленная санкционным давлением и государственной политикой импортозамещения, может свидетельствовать о растущей изоляции российской экономики. Хотя такая ситуация способна стимулировать внутреннее производство в некоторых отраслях, включая ИТ-сектор, как отмечено в ряде обзоров [6], в долгосрочной перспективе она несет риски снижения общей конкурентоспособности из-за ограниченного доступа к передовым мировым технологиям, глобальным рынкам капитала и международной кооперации.

Несмотря на декларируемый рост в отдельных высокотехнологичных секторах, таких как информационные технологии [6], фундаментальные структурные проблемы экономики, включая сырьевую зависимость и институциональные ограничения [15], могут сдерживать устойчивость этого роста и его реальное влияние на диверсификацию национальной экономики. Локальные успехи в ИТ-сфере могут не приводить к кардинальному решению системных проблем без проведения глубоких структурных реформ, направленных на улучшение инвестиционного климата, защиту прав собственности и развитие конкуренции.

1.5. Общая политическая обстановка

Российская Федерация, согласно Конституции, является демократическим федеративным правовым государством с республиканской формой правления.[17] Государственный строй характеризуется как смешанная (президентско-парламентская) республика, однако с выраженным доминированием президентской власти. Президент Российской Федерации является главой государства, определяет основные направления внутренней и внешней политики и обладает широкими полномочиями.[17] Законодательную власть осуществляет двухпалатное Федеральное Собрание, состоящее из Государственной Думы (нижняя палата) и Совета Федерации (верхняя палата). Исполнительная власть принадлежит Правительству Российской Федерации. Судебная власть представлена системой судов, высшими из которых являются

Конституционный Суд РФ и Верховный Суд РФ.[17] Политическая система характеризуется доминированием партии «Единая Россия» и тенденцией к централизации власти.

Административно-территориальное деление страны включает различные типы субъектов федерации: республики, края, области, города федерального значения, автономную область и автономные округа.[18] Эти субъекты объединены в восемь федеральных округов, которые не являются конституционными единицами, а служат для координации деятельности федеральных органов исполнительной власти на местах.[19]

В период с 2019 по 2025 год в политической жизни России наблюдалась устойчивая тенденция к дальнейшей централизации государственной власти и усилению контроля государства над различными сферами общественной жизни, включая экономику, средства массовой информации и информационное пространство в целом. Международные организации и эксперты по-разному оценивают политический режим в России, при этом некоторые характеризуют его как авторитарный.[17] Эта тенденция к централизации и усилению государственного контроля напрямую коррелирует с законодательными инициативами в сфере регулирования интернета. Принятие таких законов, как закон "о суверенном интернете" [13] и поправки в Уголовный кодекс, вводящие ответственность за распространение "фейков" [20], является отражением стратегического стремления государства распространить и укрепить свой контроль над цифровой сферой.

Формально Российская Федерация определяется как смешанная президентско-парламентская республика [17], однако фактическое доминирование исполнительной ветви власти во главе с Президентом и его Администрацией, а также значительное влияние пропрезидентской партии в парламенте, могут объяснять относительную легкость и скорость принятия законодательных актов, направленных на ужесточение регулирования, в том числе в сфере интернета. Ослабление роли парламента как независимой и равновесной ветви власти снижает барьеры для инициатив, исходящих от исполнительной власти или силовых структур, что создает среду, в которой законодательство, усиливающее государственный контроль над интернетом, может быть быстро принято и реализовано.

2. Интернет

2.1. Национальный домен

Национальным доменом верхнего уровня (ccTLD) для Российской Федерации является **.RU**. Также существует кириллический национальный домен **.РФ**. Домен.RU предназначен для интернет-ресурсов, имеющих отношение к Российской Федерации, хотя строгих ограничений по тематике размещаемых сайтов не установлено.[22] Регистрация доменных имен в зонах.RU и.РФ осуществляется через сеть аккредитованных регистраторов.

Домен.RU был официально делегирован России 7 апреля 1994 года. Управление и координацию развитием национальных доменов.RU и.РФ осуществляет Координационный центр национального домена сети Интернет (КЦ).[22] Важным событием в истории управления национальным доменом стало вхождение Российской Федерации в лице Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) в состав учредителей КЦ 3 июня 2020 года.[23] Этот шаг рассматривается как элемент общей государственной политики, направленной на усиление контроля над критической информационной инфраструктурой и "суверенизацию" российского сегмента интернета.

Вхождение Роскомнадзора, основного государственного органа, ответственного за регулирование и блокировку интернет-ресурсов [24], в состав учредителей Координационного центра национального домена [23] является значимым фактором, свидетельствующим об усилении государственного влияния на управление ключевой интернет-инфраструктурой страны. Это может потенциально привести к ужесточению политики регистрации доменных имен и использованию доменной системы как одного из инструментов для цензуры или оперативной блокировки ресурсов, признанных нежелательными. Усиление государственного контроля над национальным доменом, в сочетании с положениями Федерального закона № 90-ФЗ ("о суверенном интернете"), который предусматривает создание национальной системы доменных имен [13], формирует техническую и административную базу для потенциальной изоляции российского сегмента интернета или выборочного отключения от глобальной системы DNS в случае возникновения определенных "угроз".

2.2. Число пользователей

По состоянию на начало 2025 года, по данным Datareportal, в Российской Федерации насчитывалось 133 миллиона интернет-пользователей, что соответствует уровню проникновения интернета в 92.2% от общей численности населения.[4] Несколько иные данные представляет Mediascope: в октябре 2024 года месячная аудитория интернета в России составила 103 миллиона человек, или 85% населения в возрасте 12 лет и старше.[26] Данные Федерального резервного банка Сент-Луиса (FRED) указывают на 92.2 интернет-пользователя на 100 человек населения в 2023 году.[28]

Источники данных о числе пользователей интернета и уровне его проникновения включают: Datareportal [2], Mediascope [26] и FRED (St. Louis Fed).[28]

Динамика числа интернет-пользователей и уровня проникновения интернета в России по годам:

Год	Число интернет-пользователей (млн человек)	Уровень проникновения интернета (%)	Источник(и)
2019	118.0 (январь 2020)	81.0 (январь 2020) / 82.6 (год)	[2] (Datareportal)[28] (FRED)
2020	118.0	81.0 / 85.0 (год)	[2] (Datareportal)[28] (FRED)
2021	124.0	85.0 / 88.2 (год)	[2] (Datareportal)[28] (FRED)
2022	129.8	89.0 / 90.4 (год)	[2] (Datareportal)[28] (FRED)
2023	127.6	88.2 / 92.2 (год)	[2] (Datareportal)[28] (FRED)
2024 (начало)	130.4	90.4	[3] (Datareportal)
2025 (начало)	133.0	92.2	[4] (Datareportal)

Примечание: Данные от разных источников могут незначительно отличаться

из-за различий в методологиях подсчета и периодах исследования. Например, Datareportal обычно предоставляет данные на начало года, FRED - среднегодовые.

Высокий уровень проникновения интернета, превышающий 90% по последним доступным данным [4], означает, что интернет является основным источником информации и ключевой платформой для коммуникации для подавляющего большинства населения России. Этот фактор делает контроль над интернет-пространством критически важным для государственных органов, стремящихся оказывать влияние на общественное мнение и информационные потоки, особенно в условиях ограниченного доступа к независимым традиционным СМИ.

Некоторое расхождение в абсолютных цифрах числа пользователей от различных исследовательских агентств (например, Mediascope [26] и Datareportal [3]) может быть связано с различиями в методологиях подсчета, такими как учитываемые возрастные группы, частота использования интернета или определение "активного" пользователя. Тем не менее, общая тенденция к практически полному охвату населения интернет-услугами очевидна. Небольшое снижение абсолютного числа пользователей, отмеченное Datareportal в отдельные периоды (например, на 711 тысяч человек между январем 2024 и январем 2025 года [4]), при общем росте относительного уровня проникновения, вероятно, связано с демографическими факторами, такими как общая убыль населения, или с методологическими корректировками в исследованиях, а не с реальным сокращением использования интернета. Важно отметить, что доля населения, не пользующегося интернетом, остается небольшой (7.8% на начало 2025 года [4]), что подтверждает тотальный охват страны интернет-доступом.

2.2.1 Фиксированный интернет

Рынок фиксированного широкополосного доступа в интернет (ШПД) в Российской Федерации характеризуется высоким уровнем конкуренции в крупных городах и областных центрах. Однако в малых населенных пунктах и удаленных районах страны уровень проникновения ШПД и выбор доступных провайдеров могут быть существенно ниже. Государственные программы, такие как проект устранения цифрового неравенства (УЦН), направлены на повышение доступности современных услуг связи, включая ШПД, для жителей малых и отдаленных поселений. Основными технологиями, используемыми для предоставления услуг фиксированного ШПД, являются различные варианты FTTx

(оптоволокно до здания/квартиры), обеспечивающие высокие скорости передачи данных.

По данным аналитической компании "ТМТ Консалтинг", во втором квартале 2024 года количество абонентов ШПД в B2C-сегменте в России достигло 36,5 миллионов, показав рост на 0,4% по сравнению с аналогичным периодом предыдущего года.[29] Динамика числа пользователей фиксированного ШПД за более ранние годы в предоставленных материалах детализирована недостаточно для построения полной таблицы с 2019 года.

Крупнейшими операторами на российском рынке фиксированного ШПД, на долю которых, по данным "ТМТ Консалтинг" на второй квартал 2023 года, приходилось около 71% абонентской базы [30], являются:

- **«Ростелеком»**: Является лидером рынка. В первом квартале 2023 года абонентская база компании выросла на 0.6%.[30] Сайт: https://rt.ru/
- **МТС**: Один из ведущих игроков, демонстрирующий рост абонентской базы за счет расширения сетей в регионах и предложения конвергентных услуг. Во втором квартале 2024 года рост абонентской базы составил 0.9%.[29] Сайт: https://mts.ru/
- **«ЭР-Телеком» (работает под брендами Дом.ру, ранее также «Акадо»)**: После консолидации активов, включая московского оператора «Акадо» в 2023 году, компания укрепила свои позиции, увеличив рыночную долю по абонентам до 12% в первом квартале 2023 года.[30] Сайт: https://dom.ru/, https://www.akado.ru/
- **«Вымпелком» (бренд «Билайн»)**: Входит в число крупнейших операторов ШПД. Сайт: https://beeline.ru/
- **ТТК (ТрансТелеКом)**: Занимает пятое место на рынке, с долей около 2% по абонентам и выручке.[30] Сайт: https://ttk.ru/

Процессы консолидации на рынке ШПД, такие как приобретение компании «Акадо» холдингом «ЭР-Телеком» [30], ведут к усилению позиций крупнейших игроков. С одной стороны, это может способствовать улучшению качества предоставляемых услуг и ускорению модернизации сетей за счет больших инвестиционных возможностей консолидированных компаний. С другой стороны, сокращение числа независимых операторов может привести к ослаблению конкуренции и, как следствие, потенциальному росту тарифов для конечных

пользователей в долгосрочной перспективе, особенно в тех сегментах рынка, где выбор провайдеров ограничен.

Несмотря на высокий общий уровень проникновения интернета в стране, темпы роста абонентской базы фиксированного ШПД замедляются (например, рост на 0.4% во втором квартале 2024 года [29]). Это может указывать на постепенное насыщение рынка в крупных городах, где уровень проникновения уже высок (например, в Москве – 87.5% [30]). Дальнейший рост рынка ШПД будет во многом зависеть от успешности подключения абонентов в удаленных и труднодоступных территориях, где экономическая целесообразность строительства инфраструктуры для операторов ниже. Это, в свою очередь, может потребовать более активного государственного участия, включая программы субсидирования и поддержки операторов, работающих в таких регионах.

2.2.2. Мобильный интернет

Мобильный интернет играет ключевую роль в обеспечении доступа к сети для значительной части населения Российской Федерации. Его значение особенно велико в регионах с недостаточным покрытием фиксированных сетей ШПД, а также для пользователей, нуждающихся в доступе в интернет вне дома или офиса. Рынок мобильной связи и мобильного интернета в России характеризуется высокой степенью конкуренции между операторами так называемой "большой четверки". Операторы продолжают развивать сети стандарта 4G/LTE, обеспечивая все более широкое покрытие и увеличение скоростей передачи данных. Внедрение технологии 5G находится на начальном этапе и сталкивается с рядом трудностей, включая ограниченный доступ к необходимому оборудованию из-за санкций и вопросы выделения частотного ресурса.

По данным на начало 2025 года, в России насчитывалось 216 миллионов активных мобильных подключений, что эквивалентно 150% от общей численности населения. Однако следует учитывать, что не все эти подключения обеспечивают доступ в интернет (некоторые могут использоваться только для голосовой связи и SMS) и один пользователь может иметь несколько активных SIM-карт.[4] Число мобильных подключений сократилось на 3.3 миллиона (-1.5%) в период с начала 2024 по начало 2025 года.[4] Аналогичная тенденция наблюдалась и годом ранее: на начало 2024 года было зафиксировано 219.8 миллионов мобильных подключений (152.5% от населения), что на 4.6 миллиона (-2.0%) меньше, чем в начале 2023 года.[3]Крупнейшими операторами мобильной связи и

мобильного интернета в России являются:

- **МТС**: По состоянию на конец 2023 года компания обслуживала 81.8 миллиона мобильных абонентов [31], а по данным на третий квартал 2024 года – 81.9 миллиона.[32] Сайт: https://mts.ru/
- **МегаФон**: Число мобильных абонентов на конец 2023 года составляло 67.7 миллионов [31], а во втором квартале 2024 года – 77.26 миллионов.[32] Сайт: https://megafon.ru/
- **«Вымпелком» (бренд «Билайн»)**: На конец 2023 года оператор имел 44.1 миллиона мобильных абонентов [31], эта же цифра приводится и для третьего квартала 2023 года.[32] Сайт: https://beeline.ru/
- **Tele2 (входит в группу «Ростелеком»)**: «Ростелеком» совокупно (включая Tele2) обслуживал 48.1 миллиона мобильных абонентов на конец 2023 года.[31] Отдельно по Tele2 данные на третий квартал 2024 года – 48.0 миллионов абонентов.[32] Сайт: https://tele2.ru/

Значительное превышение числа мобильных подключений над общей численностью населения (более 150% [3]) свидетельствует о широком распространении практики использования нескольких SIM-карт одним абонентом (например, для разных тарифов, для работы и личных нужд) или об активном использовании SIM-карт в различных устройствах M2M (machine-to-machine) и IoT (Internet of Things). Наблюдаемое в 2024-2025 годах снижение общего числа мобильных подключений [3] может быть связано с насыщением рынка, оптимизацией расходов пользователями (отказ от избыточных SIM-карт) или влиянием общих экономических и демографических факторов.

Зависимость развития сетей нового поколения 5G от доступности иностранного телекоммуникационного оборудования и выделенных частот, особенно в условиях действия международных санкций и государственной политики импортозамещения, может привести к замедлению темпов внедрения этой технологии в России по сравнению с другими странами. Это, в свою очередь, способно ограничить развитие новых цифровых сервисов и приложений, требующих сверхвысоких скоростей передачи данных и минимальных задержек (например, в сферах промышленного интернета вещей, беспилотного

транспорта, передовых технологий виртуальной и дополненной реальности). Такое отставание потенциально может усилить "цифровой разрыв" России с технологически более продвинутыми государствами и повлиять на конкурентоспособность российской цифровой экономики в долгосрочной перспективе.

2.3. Скорость доступа в интернет и качество оказываемых услуг

Скорость доступа в интернет в России демонстрирует устойчивый рост как в мобильном, так и в фиксированном сегментах, однако страна все еще уступает лидерам мировых рейтингов. По данным Ookla Speedtest Global Index на апрель 2025 года, медианная скорость загрузки в мобильных сетях в России составляла 50.50 Мбит/с, что соответствовало 90-му месту в мире. В сегменте фиксированного ШПД медианная скорость загрузки достигала 158.89 Мбит/с.[33] Данные Datareportal, также основанные на измерениях Ookla, на начало 2025 года показывали медианную мобильную скорость 26.21 Мбит/с (рост на 9.3% за год) и медианную фиксированную скорость 89.39 Мбит/с.[4] Годом ранее, в начале 2024 года, эти показатели составляли 23.97 Мбит/с для мобильного и 84.74 Мбит/с для фиксированного интернета соответственно.[3] Более ранние данные от Роскачества (начало 2022 года) указывали на среднюю мобильную скорость 17.84 Мбит/с и среднюю фиксированную скорость 61.65 Мбит/с.[34]

Региональные различия в скоростях доступа также существенны. По данным оператора «Дом.Ру» на март 2024 года, лидерами по средней скорости ШПД среди российских городов являлись Краснодар (240.5 Мбит/с), Ростов-на-Дону (179 Мбит/с) и Санкт-Петербург (177.8 Мбит/с), в то время как Москва занимала пятое место с результатом 168.5 Мбит/с.[35]

Наблюдаемый устойчивый рост медианных скоростей доступа [3] свидетельствует о продолжающихся инвестициях операторов связи в модернизацию и развитие сетевой инфраструктуры. Тем не менее, отставание России от стран-лидеров в мировых рейтингах скоростей интернета [33] указывает на наличие значительного потенциала для дальнейшего улучшения. Это может быть связано с масштабами территории страны, необходимостью обновления устаревших участков сетей или экономическими ограничениями, влияющими на темпы инвестиций.

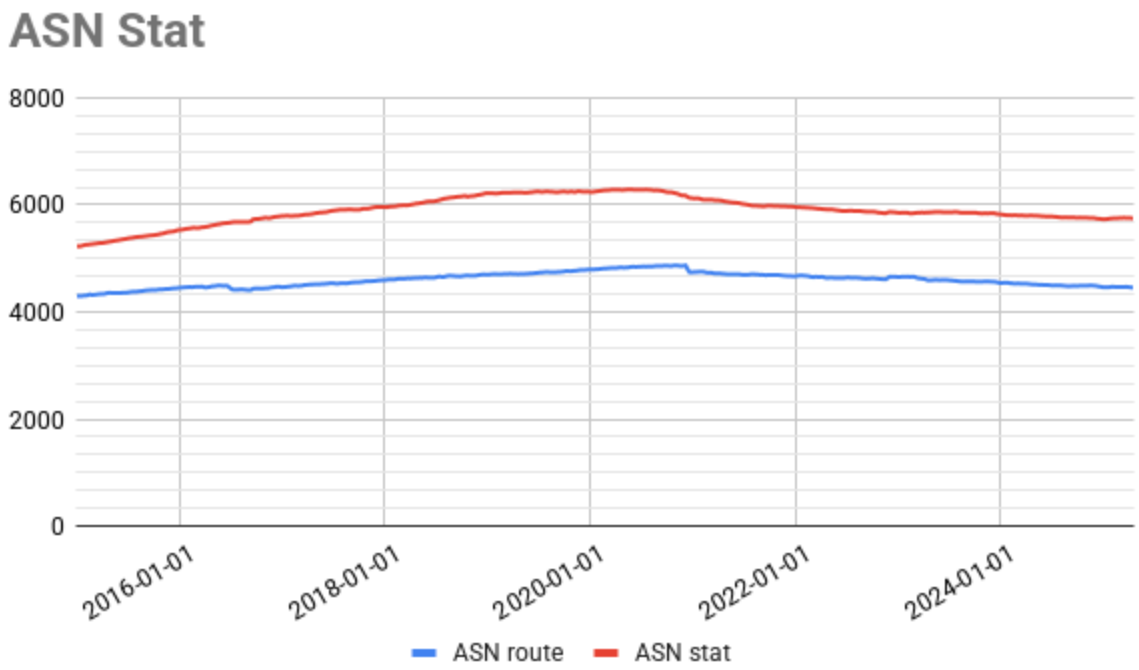
Значительная разница в скоростях интернет-доступа между крупными

агломерациями [35] и средними показателями по стране в целом [4] подчеркивает сохраняющуюся проблему "цифрового неравенства" внутри России. Такое неравенство может ограничивать равный доступ граждан к современной информации, онлайн-образованию, государственным услугам в цифровом формате и возможностям, предоставляемым цифровой экономикой. Это, в свою очередь, способно усугублять существующие региональные диспропорции в социально-экономическом развитии и ограничивать реализацию цифровых прав для части населения.

2.4. Развитие провайдеров и автономных систем

Автономные системы (AS) являются ключевыми компонентами глобальной интернет-инфраструктуры, представляя собой совокупность IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами и имеющих единую политику маршрутизации. Количество зарегистрированных и активно маршрутизируемых AS в стране является важным показателем развития и сложности ее интернет-экосистемы. По данным RIPE NCC (Региональный интернет-регистратор для Европы, Ближнего Востока и части Центральной Азии) на апрель 2017 года, в России было зарегистрировано 1404 локальных интернет-регистратора (LIR) и назначено 5822 номера автономных систем (ASN). Из них 4509 AS активно анонсировали 26320 IP-префиксов.[37]

График 3: Динамика Автономных Систем в Российской Федерации (2015-2025)



Традиционно рост числа автономных систем свидетельствует о развитии конкуренции на рынке интернет-провайдеров и увеличении децентрализации интернет-инфраструктуры. Однако в контексте российского законодательства, в частности, Федерального закона "о суверенном интернете" [13], который предусматривает создание реестра точек обмена трафиком и возможность централизованного управления маршрутизацией, сам по себе количественный рост AS не обязательно гарантирует повышение устойчивости сети к произвольным блокировкам или большую степень свободы. Напротив, существует вероятность, что эти автономные системы могут быть более эффективно подчинены требованиям национального регулятора.

График демонстрирует две четко выраженные фазы в динамике числа автономных систем в России. В период с 2015 по начало 2021 года наблюдалась устойчивая положительная динамика, свидетельствующая об экстенсивном росте числа субъектов интернет-инфраструктуры. Однако, начиная с 2021 года, данная тенденция сменяется стагнацией с последующим незначительным снижением как общего числа зарегистрированных AS, так и числа активных AS. По состоянию на апрель 2025 года, в Российской Федерации зафиксировано 5720 автономных

систем, из которых 4434 анонсируют маршруты в глобальной сети.

При численности населения около 146 млн человек, коэффициент плотности активных автономных систем для России составляет **30,4 AS на 1 млн жителей**.

Для контекстуализации полученных данных был проведен сравнительный анализ с показателями стран Восточной Европы. Установлено, что Российская Федерация значительно уступает по данному параметру ряду государств.

В **Украине** наблюдается наиболее высокий уровень децентрализации интернет-инфраструктуры в регионе: коэффициент плотности активных AS достигает **76,7 на 1 млн человек**. Высокий показатель также демонстрирует **Польша — 63,1 AS на 1 млн человек**. Столь существенное превышение российских значений указывает на более высокую степень конкуренции между поставщиками интернет-услуг и большее разнообразие независимых сетевых операторов в указанных странах.

Показатели **Республики Беларусь** сопоставимы с российскими и составляют **30,2 AS на 1 млн жителей**, что свидетельствует о схожей структуре рынка. В то же время **Казахстан** демонстрирует более низкий уровень проникновения независимых сетей с коэффициентом **12,6 AS на 1 млн человек**.

Если бы актуальные данные показали стагнацию или уменьшение числа активно маршрутизируемых AS в последние годы, это могло бы служить индикатором процессов консолидации на рынке интернет-провайдеров или ухода с рынка более мелких игроков. Такие процессы могут быть вызваны ужесточением регуляторных требований, например, значительными затратами на внедрение и обслуживание систем СОРМ (Системы оперативно-розыскных мероприятий), а также оборудования для глубокой проверки пакетов (DPI) в соответствии с требованиями "закона Яровой" и "закона о суверенном интернете".[25] Подобные финансовые и административные барьеры могут приводить к снижению конкуренции и усилению позиций крупных, зачастую аффилированных с государством, провайдеров, что, в свою очередь, может повлиять на выбор и качество услуг для конечных пользователей.

Таблица 2: Топ 10 крупнейших Автономных Систем Российской Федерации

#	Number of AS	Name	Web Site	Foreign neighbour count	Local neighbour count	Total neighbour count	Foreign neighbours share
1	20764	CJSC RASCOM ISP	https://rascom.ru/en/	4902	1077	5979	81%
2	20485	TRANSTELECOM	https://www.ttk.ru	3771	2136	5907	63%
3	3216	Beeline, VimpelCom, Sovintel, Golden Telecom, Sovam	https://beeline.ru	1786	1730	3516	50%
4	57304	RETNRU-AS	https://www.retn.ru	2706	450	3156	85%
5	31133	PJSC MegaFon	https://www.megafon.ru	1245	1854	3099	40%
6	12389	Rostelecom	https://www.company.rt.ru/en/	454	2312	2766	16%
7	48858	Milecom-as	https://www.milecom.ru	2006	200	2206	90%
8	8359	Mobile TeleSystems PJSC	https://ir.mts.ru/	846	958	1804	46%
9	43727	KVANT-TELECOM CJSC	https://www.kvant-telecom.ru	884	572	1456	60%
10	9049	Dom ru, Дом.ru	https://ertelecom.ru	80	1010	1090	7%

Анализ топ-10 крупнейших автономных систем Российской Федерации подтверждает и дополняет вывод о высокой концентрации рынка интернет-доступа. Данные таблицы позволяют выявить структуру российского сегмента сети Интернет и определить роли ключевых игроков.

Основные выводы по структуре рынка:

Высокая степень концентрации. Интернет-магистраль России контролируется ограниченным числом крупных телекоммуникационных компаний. В их число

входят операторы "большой тройки" (МТС, МегаФон, Билайн), государственный оператор Ростелеком, а также крупные провайдеры, такие как ТрансТелеКом (ТТК) и ЭР-Телеком (Дом.ру). Этот факт объясняет стагнацию в росте общего числа автономных систем: новым игрокам чрезвычайно сложно конкурировать с инфраструктурными гигантами, обладающими тысячами пиринговых соединений.

Функциональная специализация операторов. Таблица четко разделяет операторов на несколько категорий по их роли в сетевой инфраструктуре:

- Международные транзитные операторы: Компании RETN (85% зарубежных соединений), Milecom (90%) и RASCOM (81%) выступают в роли основных шлюзов, связывающих Рунет с глобальной сетью. Их бизнес-модель ориентирована на предоставление международного транзита трафика, что подтверждается доминирующей долей зарубежных пиров.
- Национальные операторы с фокусом на внутренний рынок: Ростелеком (лишь 16% зарубежных соединений) и Дом.ру (7%) являются классическими примерами гигантов "последней мили". Они обладают максимально широким покрытием внутри страны (особенно Ростелеком с его 2312 локальными соединениями — абсолютно доминирующий показатель), но для выхода в глобальную сеть преимущественно используют услуги транзитных операторов.
- Универсальные операторы: Крупнейшие мобильные операторы (МТС, МегаФон, Билайн) поддерживают сбалансированную сетевую политику. Они обладают разветвленной сетью пиринговых соединений как внутри России для обмена трафиком между своими абонентами, так и за рубежом для оптимизации маршрутов и снижения затрат на покупку транзита.

- Особая роль Ростелекома. Абсолютное лидерство Ростелекома по числу локальных соединений (2312) подчеркивает его статус инфраструктурного монополиста и системообразующего оператора. Значительная часть внутреннего российского трафика так или иначе проходит через его сети.

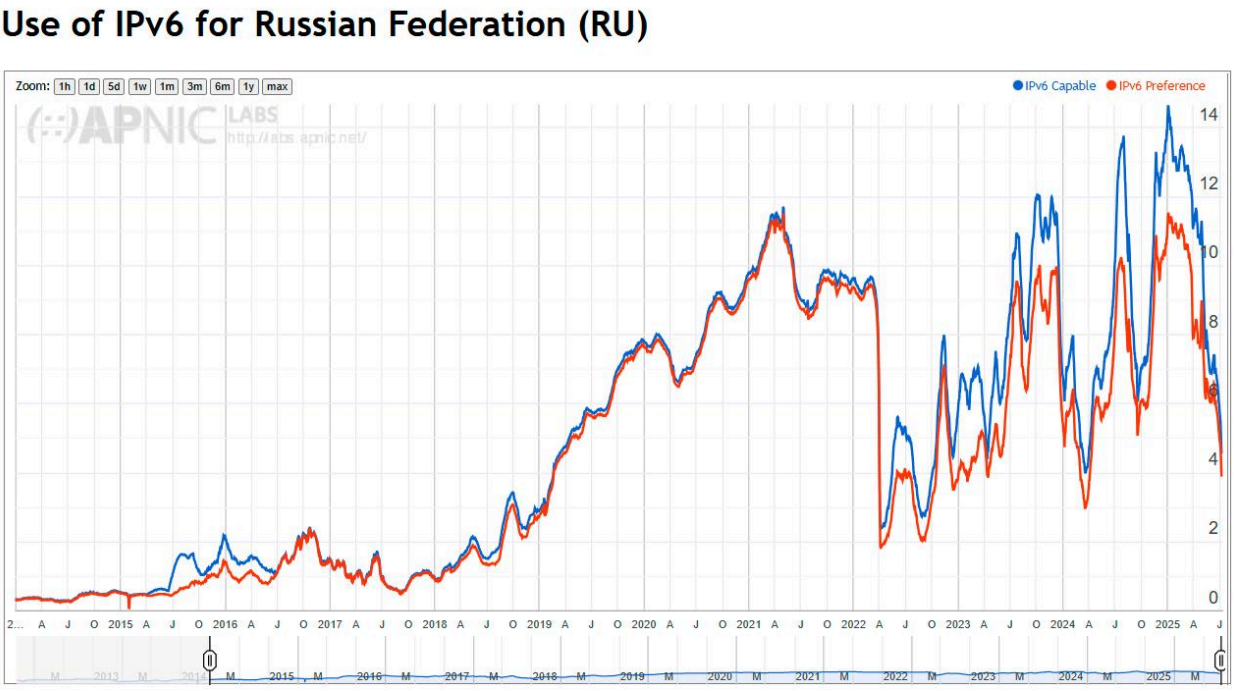
В совокупности, представленные данные рисуют картину зрелого, концентрированного рынка с несколькими доминирующими игроками и четким разделением функций между операторами международного транзита и провайдерами внутреннего доступа.

2.5. Проникновение IPv6

Переход на новую версию интернет-протокола IPv6 является глобальной необходимостью, обусловленной исчерпанием адресного пространства IPv4 и растущим числом устройств, подключаемых к сети (включая Интернет вещей, IoT). Динамика внедрения IPv6 в России представляет важный аспект развития национальной интернет-инфраструктуры.

Данные о проникновении IPv6 в России заметно различаются в зависимости от источника и методики измерения. По данным Google, на 9 июня 2025 года 44.65% пользователей Google из России использовали IPv6 для доступа к сервисам компании.[39] Аналогичные цифры (44.62% мирового трафика Google через IPv6) приводились компанией VASExperts со ссылкой на APNIC Labs по состоянию на 18 ноября 2024 года, однако без конкретизации российского показателя от APNIC в данном источнике.[40] В то же время, более ранние данные от APNIC Labs, представленные RIPE Labs в 2020 году, показывали значительно более низкий уровень проникновения IPv6 в России: 7.2% по измерениям Akamai, 7.01% по данным самого APNIC, 9.43% по данным Facebook и 3.85% по данным Google.[41] Также, по данным APNIC на 2020 год, коэффициент использования IPv6 (V6 Use ratio) для России составлял 7.78%.[42]

График 4: Динамика проникновения IPv6 в Российской Федерации (2015-2025)



Источник: stats.labs.apnic.net

Обсуждения в технических сообществах [44] предполагают, что внедрение IPv6 могло быть отложено некоторыми операторами из-за необходимости обеспечения совместимости нового протокола с системами DPI, используемыми для государственной цензуры и фильтрации трафика. После обновления этих систем развертывание IPv6 могло ускориться. Если эта гипотеза верна, то рост использования IPv6 парадоксальным образом может быть связан с усилением технических возможностей для контроля интернет-трафика в стране.

Если подтвердится значительный рост проникновения IPv6 до уровня 40-60%, это будет свидетельствовать об осознании российскими операторами связи и государством необходимости перехода на новый протокол для обеспечения долгосрочного развития Рунета и поддержки растущего числа подключенных устройств. Это также означает, что технические и, возможно, регуляторные барьеры для внедрения IPv6, включая его интеграцию с системами контроля, в значительной степени преодолены.

Ускоренное внедрение IPv6, если оно действительно происходит и

поддерживается государством (например, через регуляторные требования к операторам), может также быть использовано для усиления мер по "суверенизации" интернета. Наличие развитой IPv6-инфраструктуры, управляемой национальными операторами и полностью совместимой с системами DPI, облегчает осуществление контроля над трафиком и реализацию политик фильтрации и блокировок в новой протокольной среде, что соответствует общей государственной стратегии по усилению контроля над информационным пространством.

2.6. Индекс связности

Для оценки уровня интеграции интернет-сегмента используются два ключевых показателя, основанные на анализе попарных связей (пирингов) между Автономными Системами (ASN).

Индекс глобальной связности (Global Connectivity Index): Этот индекс представляет собой общее число уникальных связей между каждой российской ASN и каждой внешней (зарубежной) ASN. По сути, он измеряет, насколько широко и разнообразно российский интернет-сегмент подключен к остальному миру. Чем выше этот показатель, тем больше у страны "окон" в глобальную сеть.

Индекс локальной связности (Local Connectivity Index): Этот индекс рассчитывается как общее число уникальных связей между различными российскими ASN. Он отражает интенсивность и сложность внутреннего интернет-рынка, в частности, активность на точках обмена трафиком (IXP). Высокий показатель говорит о развитой внутренней экосистеме, позволяющей эффективно обмениваться трафиком внутри страны, минимизируя задержки и зависимость от внешних каналов для локальных данных.

Анализ соотношения этих двух индексов позволяет понять стратегическую ориентацию национальной сети: является ли она преимущественно самодостаточной или глубоко интегрированной в глобальную инфраструктуру.

График 5: Динамика глобальной связности Автономных Систем Российской Федерации (2019-2025)

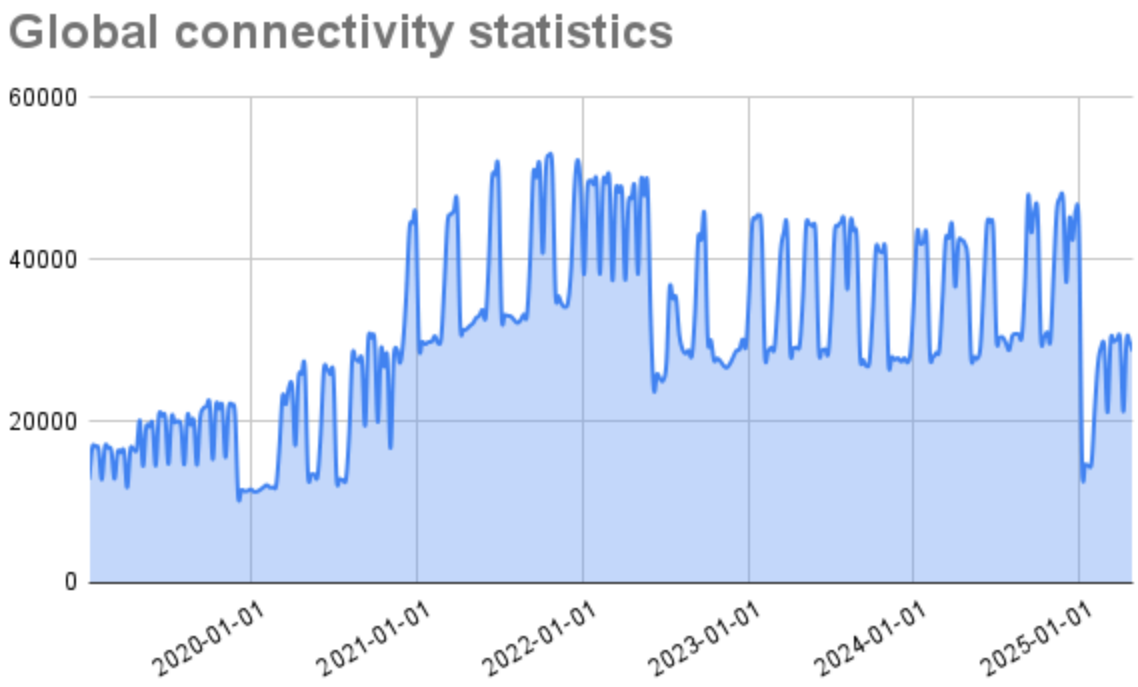
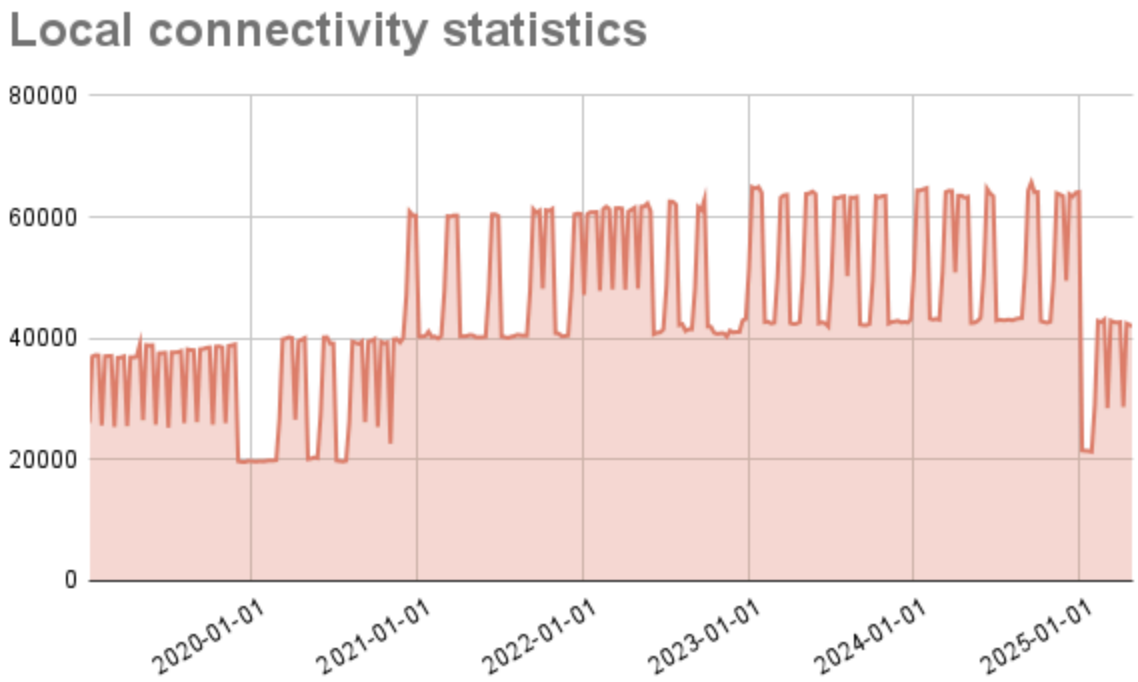


График иллюстрирует число уникальных соединений между российскими и зарубежными автономными системами. В период с 2020 по начало 2022 года наблюдался интенсивный рост показателя, который достиг пиковых значений свыше 50 000 связей, что свидетельствует об активной интеграции Рунета в глобальную сеть. Однако в первом полугодии 2022 года произошел резкий структурный сдвиг: индекс глобальной связности одномоментно сократился и стабилизировался на новом, более низком уровне в диапазоне 30 000 - 40 000 соединений, демонстрируя при этом повышенную волатильность.

Это падение напрямую отражает сокращение числа международных партнеров и маршрутов, вероятно, вследствие геополитических событий и ухода с российского рынка ряда зарубежных операторов. Исходя из текущего среднего уровня в 30 000 глобальных связей и наличия 4434 активных АС в стране, можно заключить, что **каждая активная автономная система в России в среднем имеет около 6.8 соединений с зарубежными сетями**. Это количественно подтверждает снижение разнообразия внешних каналов связи.

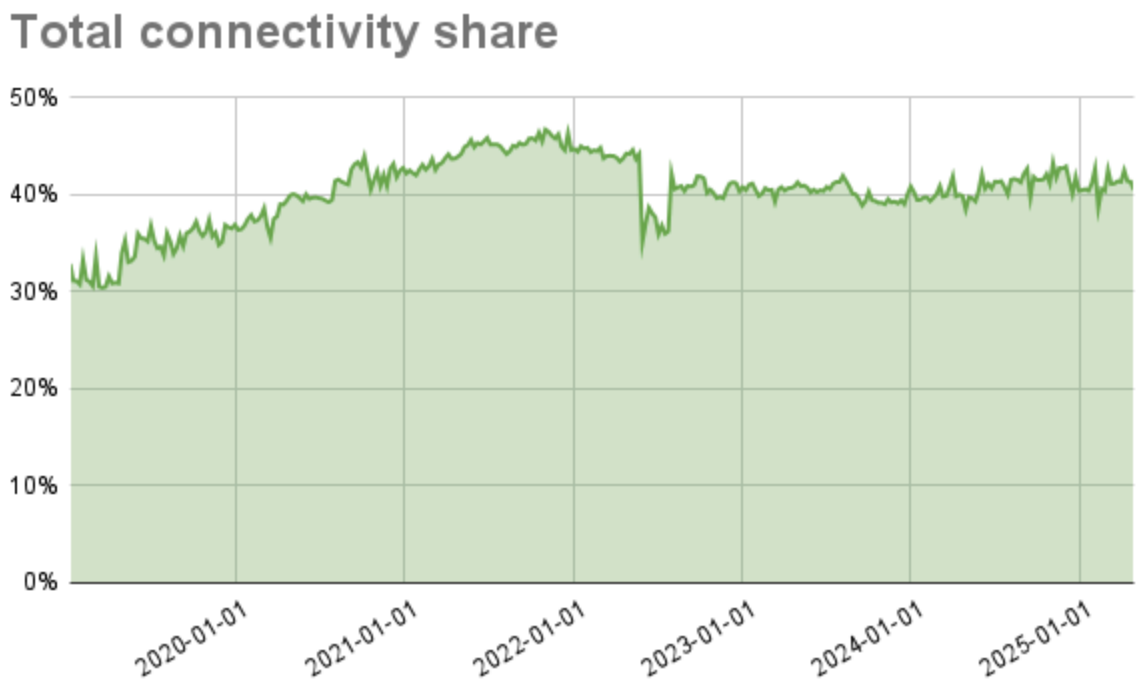
График 6: Динамика локальной связности Автономных Систем Российской Федерации (2019-2025)



Индекс локальной связности, отражающий количество уникальных пирингов внутри России, демонстрирует иную траекторию. В начале 2021 года показатель совершил скачок с ~40 000 до более чем 60 000 соединений, что говорит о качественном развитии внутренней интернет-инфраструктуры, в частности, точек обмена трафиком (IXP). Ключевым моментом является то, что, в отличие от глобального индекса, высокий уровень локальной связности сохранился на протяжении всего периода 2022-2024 гг.

Данная динамика свидетельствует о целенаправленном усилении внутренней сетевой экосистемы и развитии ее самодостаточности. В условиях сокращения внешних связей российские операторы стали активнее взаимодействовать друг с другом для оптимизации маршрутизации трафика внутри страны. При текущем показателе в ~60 000 локальных соединений, на **каждую активную АС приходится в среднем 13.5 внутренних соединений**. Этот показатель, более чем вдвое превышающий среднее число внешних связей, подтверждает ориентацию на внутреннюю связность.

График 7: Динамика отношения глобальной и локальной связности Автономных Систем Российской Федерации (2019-2025)



Этот график наиболее наглядно демонстрирует стратегический разворот в архитектуре Рунета. Он показывает долю глобальных связей в общем пуле соединений. До начала 2022 года эта доля росла, достигнув пика почти в 48%, что отражало курс на все большую глобальную интеграцию. Резкое падение показателя в 2022 году до нового стабильного уровня в районе 40% является прямым следствием описанных выше разнонаправленных тенденций: сокращения внешних пирингов при сохранении и развитии внутренних.

Таким образом, анализ соотношения индексов фиксирует фундаментальный сдвиг от модели растущей открытости к модели, ориентированной на повышение внутренней устойчивости и автономии. Произошла структурная перебалансировка российского интернет-сегмента, в результате которой относительная зависимость от внешних каналов снизилась в пользу усиления внутренних инфраструктурных связей.

3. Законодательство об интернете

3.1. Принципы управления интернетом

Управление интернетом в Российской Федерации представляет собой сложную, многоуровневую систему, включающую государственные органы, отраслевые организации (такие как Координационный центр национального домена) и представителей бизнес-сообщества. Однако определяющую роль в формировании правил и практик функционирования Рунета играет государство, политика которого в последние годы последовательно направлена на усиление контроля и регулирования цифрового пространства. Принципы управления интернетом в России претерпели значительную эволюцию: от периода относительно свободного развития в 1990-х и начале 2000-х годов к модели, где акцент сместился на обеспечение "цифрового суверенитета", информационной безопасности (в ее государственной трактовке) и расширение контроля над контентом и инфраструктурой.

Российский Форум по управлению интернетом (RIGF), ежегодно организуемый Координационным центром национального домена сети Интернет, позиционируется как площадка для диалога и выработки консенсуса между государственными органами, профессиональным телекоммуникационным сообществом, бизнесом и гражданским обществом по вопросам дальнейшего развития интернета.[45] Тем не менее, реальные решения, определяющие вектор развития регулирования, принимаются преимущественно на государственном уровне. Декларируемое на таких площадках стремление к "поиску консенсуса" [45] нередко вступает в противоречие с практикой принятия законодательных решений, где доминирует позиция государственных органов, направленная на усиление контроля. Это создает определенный разрыв между публичным обсуждением и реальной политикой в области регулирования интернета, что подтверждается принятием ряда резонансных законов, несмотря на критику со стороны части экспертного сообщества и правозащитных организаций.

3.1.1. Регулирование

Регулирование интернета в Российской Федерации осуществляется посредством обширной системы федеральных законов, подзаконных актов (постановлений Правительства, приказов профильных министерств и ведомств) и непосредственной деятельности уполномоченных государственных органов.

Ключевыми направлениями государственного регулирования интернет-сферы являются:

- **Контроль над сетевой инфраструктурой**: Наиболее ярко это проявляется в положениях Федерального закона № 90-ФЗ ("о суверенном интернете"), который направлен на обеспечение устойчивости и безопасности функционирования российского сегмента сети, но также создает технические и правовые предпосылки для его возможной изоляции и централизованного управления трафиком.[13]
- **Фильтрация и блокировка контента**: Существует разветвленная система оснований и процедур для ограничения доступа к информации, признанной запрещенной. Это включает ведение Единого реестра запрещенных сайтов Роскомнадзором.
- **Контроль над распространением информации**: Введены законы, устанавливающие ответственность за распространение "фейковой" информации (в частности, о деятельности Вооруженных Сил РФ), информации, выражающей "явное неуважение" к власти, а также за призывы к экстремизму и массовым беспорядкам.
- **Требования к локализации персональных данных**: Операторы, собирающие персональные данные российских граждан, обязаны обеспечивать их хранение и обработку на территории России.
- **Регулирование деятельности IT-компаний и социальных сетей**: Введены требования по открытию представительств иностранными IT-гигантами, модерации контента, удалению запрещенной информации.

В целом, регулирование интернет-сферы в России характеризуется тенденцией к последовательному ужесточению, расширению полномочий государственных органов и увеличению числа обязанностей, возлагаемых на операторов связи, владельцев интернет-ресурсов и самих пользователей.[25] Регулирование носит все более комплексный и всепроникающий характер, затрагивая как инфраструктурный уровень [13], так и контентный [25] и поведенческий аспекты. Это создает сложную и зачастую непрозрачную систему обязательств и запретов для всех участников интернет-пространства, что повышает риски для ведения бизнеса и ограничивает права пользователей.

3.1.2. Регулирующие ведомства и ответственные лица

Ключевую роль в регулировании и контроле интернет-пространства в России играют следующие государственные ведомства:

- **Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)**: Является основным регуляторным и надзорным органом. В его компетенцию входит блокировка сайтов, ведение различных реестров (включая реестр запрещенной информации, реестр организаторов распространения информации, реестр новостных агрегаторов), контроль за соблюдением законодательства о персональных данных, контроль и надзор в сфере СМИ и связи. Роскомнадзор подчинен Министерству цифрового развития, связи и массовых коммуникаций РФ.[24]
- **Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России)**: Ответственно за формирование и реализацию государственной политики и нормативно-правовое регулирование в сфере информационных технологий, связи и массовых коммуникаций.
- **Федеральная служба безопасности Российской Федерации (ФСБ России)**: Осуществляет контроль за соблюдением операторами связи требований по установке и функционированию Системы технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ). Участвует в решении вопросов информационной безопасности и противодействия киберугрозам.
- **Генеральная прокуратура Российской Федерации**: Обладает полномочиями направлять в Роскомнадзор требования о внесудебной блокировке интернет-ресурсов, содержащих призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в несанкционированных публичных мероприятиях, а также распространяющих недостоверную общественно значимую информацию ("фейки") и информацию, выражающую явное неуважение к органам государственной власти.
- **Министерство внутренних дел Российской Федерации (МВД России), Следственный комитет Российской Федерации (СК России)**: Занимаются расследованием преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, а также уголовных дел, возбуждаемых по фактам незаконного распространения информации в интернете (например, по статьям об экстремизме, клевете, распространении "фейков").

Руководство Роскомнадзора (по состоянию на февраль 2025 года) [24]:

- **Руководитель**: Липов Андрей Юрьевич (назначен 29 марта 2020 года).
  - Официальная биография: https://rkn.gov.ru/about/management/person/news77.htm (ссылка может меняться, актуальную следует искать на официальном сайте rkn.gov.ru в разделе "О Роскомнадзоре" -> "Руководство").
- **Заместители руководителя** [47]:
  - Логунов Владимир Викторович
    - Официальная биография: (доступна на официальном сайте Роскомнадзора)
  - Субботин Вадим Алексеевич
    - Официальная биография: (доступна на официальном сайте Роскомнадзора)
  - Терляков Олег Александрович
    - Официальная биография: (доступна на официальном сайте Роскомнадзора)
  - Вагнер Милош Эдуардович
    - Официальная биография: (доступна на официальном сайте Роскомнадзора)

Концентрация основных регуляторных и правоприменительных функций в руках Роскомнадзора [24], действующего под общим руководством Минцифры и в тесном взаимодействии с силовыми структурами (ФСБ, Генеральная прокуратура), создает мощный централизованный механизм государственного контроля над интернетом. Такая структура полномочий упрощает для государства реализацию своей политики в цифровой сфере, однако может приводить к снижению прозрачности принимаемых решений и ограничению возможностей для их независимого оспаривания.

3.2. Монополизация рынка

Формально российское законодательство, включая Федеральный закон "О защите конкуренции", направлено на предотвращение монополизации рынков, в том числе рынка услуг связи и доступа в интернет. Специальных законов, прямо поощряющих монополизацию в этой сфере, не существует. Тем не менее, ряд законодательных инициатив и сложившаяся правоприменительная практика могут косвенно способствовать усилению рыночных позиций ограниченного числа крупных игроков, многие из которых являются государственными компаниями или компаниями с государственным участием. Например, высокие

финансовые и технические требования к операторам связи, связанные с необходимостью хранения пользовательских данных ("закон Яровой") или установкой оборудования для реализации "закона о суверенном интернете" (технические средства противодействия угрозам - ТСПУ), могут оказаться более обременительными для небольших и средних провайдеров, потенциально приводя к их уходу с рынка или поглощению более крупными компаниями.[25]

На российском рынке фиксированного широкополосного доступа и мобильной связи фактически доминирует несколько крупных операторов: «Ростелеком», МТС, «МегаФон», «ВымпелКом» (Билайн) и «ЭР-Телеком» (Дом.ру).[29] «Ростелеком», будучи компанией со значительной долей государственного участия, играет особую роль в реализации государственных инфраструктурных проектов (например, программа устранения цифрового неравенства, создание и развитие телекоммуникационной инфраструктуры для нужд государственных органов). Эта компания часто рассматривается как ключевой исполнитель государственной политики в области "суверенизации" Рунета. Управление этими крупными телекоммуникационными компаниями осуществляется их корпоративным менеджментом и советами директоров, однако государство сохраняет значительные рычаги влияния на их стратегические решения, особенно в случае «Ростелекома».

Хотя формально законодательство не поощряет монополизацию, экономические и регуляторные барьеры, такие как высокая стоимость выполнения требований "закона Яровой" и "закона о суверенном Рунете" [25], создают условия, при которых эффективно конкурировать и развиваться могут преимущественно крупные игроки, обладающие значительными финансовыми и административными ресурсами. Это ведет к фактической олигополизации рынка и усилению роли компаний с государственным участием. Усиление позиций крупных, контролируемых или лояльных государству операторов связи, в свою очередь, облегчает реализацию государственной политики по контролю над интернет-трафиком и инфраструктурой. Государственным органам проще взаимодействовать (и, при необходимости, оказывать давление) с ограниченным числом крупных компаний, чем с множеством мелких независимых провайдеров. Это упрощает внедрение централизованных систем управления трафиком (например, ТСПУ) и обеспечение повсеместного соблюдения требований по блокировкам и предоставлению доступа к данным для правоохранительных органов. Таким образом, наблюдаемая олигополизация рынка может быть не только следствием экономических процессов, но и фактором, способствующим

достижению политических целей государства в цифровой сфере.

3.3. Отключения интернета по приказу властей

Федеральный закон № 90-ФЗ от 1 мая 2019 года, широко известный как "закон о суверенном интернете" [13], заложил правовую и техническую основу для централизованного управления российским сегментом сети Интернет. Закон декларирует цели обеспечения целостности, устойчивости и безопасности функционирования Рунета, в том числе в случае внешних угроз. Однако его положения также создают возможность для изоляции российского сегмента от глобальной сети или отключения доступа в интернет в определенных районах страны. Понятие "угроз" в законе трактуется достаточно широко, что оставляет пространство для различных интерпретаций.

Закон предусматривает создание Центра мониторинга и управления сетью связи общего пользования (ЦМУ ССОП), который находится в ведении Роскомнадзора. Операторы связи обязаны устанавливать на своих сетях технические средства противодействия угрозам (ТСПУ), которые позволяют Роскомнадзору осуществлять фильтрацию трафика и, при необходимости, ограничивать доступ к информации или даже отключать сегменты сети. Решения о введении "централизованного управления" сетью принимаются Роскомнадзором на основании правил, утверждаемых Правительством РФ, и в координации с ФСБ и Федеральной службой охраны (ФСО). Причинами для таких действий могут быть названы внешние кибератаки, внутренние угрозы (например, массовые беспорядки, которые могут быть квалифицированы как угроза безопасности), а также проведение учений по обеспечению устойчивости Рунета. Отчет Freedom House за 2022 год упоминает, что российское правительство проводило испытания по отключению Рунета от глобального интернета.[25]

"Закон о суверенном интернете" [13], под предлогом защиты национальной интернет-инфраструктуры от внешних угроз, фактически создает легальный механизм для осуществления внутренних шатдаунов (отключений интернета) или масштабной фильтрации трафика по политическим мотивам. Это представляет серьезную угрозу для свободы информации, свободы выражения мнений и других цифровых прав граждан. Широкая трактовка понятия "угроз" позволяет использовать эти механизмы в различных ситуациях, включая периоды политической нестабильности или для подавления протестной активности.

Требование об обязательной установке ТСПУ на сетях всех операторов связи [25] и

создание централизованной системы управления через ЦМУ ССОП фактически передают государству в лице Роскомнадзора прямой контроль над потоками данных внутри страны. Это не только снижает автономию операторов связи, но и создает инфраструктуру для потенциально тотальной слежки и цензуры, возможности которой выходят далеко за рамки простого отключения доступа к сети. Такая система позволяет осуществлять гранулярный контроль над всем интернет-пространством, включая блокировку конкретных ресурсов, протоколов, замедление трафика к "нежелательным" сайтам и анализ содержания передаваемой информации.

В 2025 году практика отключения интернета по приказу властей перешла от теоретической возможности к массовому применению, затронув десятки регионов. Начиная с мая 2025 года, во время проведения парадов "победы", в более чем 30 городах России был превентивно отключен мобильный интернет под предлогом защиты от атак беспилотников. Эти отключения стали первым случаем скоординированного шатдауна в таком масштабе, продемонстрировав готовность властей использовать созданную инфраструктуру централизованного управления сетями (ТСПУ) для ограничения доступа к связи на обширных территориях.

Ситуация кардинально обострилась летом 2025 года после проведения украинскими силами операции "Паутина", в ходе которой для наведения дронов на аэродромы стратегической авиации в глубине России использовался мобильный интернет. В ответ на это российские власти начали применять практику регулярных и продолжительных отключений мобильного интернета как меру противодействия. По данным независимых наблюдателей, в июне и июле 2025 года число локальных шатдаунов исчислялось сотнями и затрагивало более половины регионов страны, включая те, что находятся в тысячах километров от зоны боевых действий.

Таким образом, "защита от внешних угроз", изначально декларируемая как цель "закона о суверенном интернете", на практике превратилась в легальное основание для массовых и длительных отключений мобильного интернета для гражданского населения. Эти шатдауны, порой продолжающиеся по несколько дней, стали новой реальностью для миллионов россиян, существенно ограничивая их базовые права на доступ к информации, связь и пользование цифровыми сервисами.

3.4. Законодательство о "словах в интернете"

Российское законодательство содержит ряд норм, устанавливающих ответственность граждан и организаций за высказывания и распространение информации в интернете. Ключевой и наиболее резонансной нормой последних лет стала статья 207.3 Уголовного кодекса РФ "Публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий". Эта статья была введена в УК РФ 4 марта 2022 года.[20]

Данная норма предусматривает уголовную ответственность за публичное распространение под видом достоверных сообщений информации, которая, по мнению правоохранительных органов и суда, является заведомо ложной и касается использования Вооруженных Сил РФ или исполнения государственными органами РФ своих полномочий, в том числе за пределами территории России.[21] Определение "заведомой ложности" информации на практике часто основывается на ее несоответствии официальной позиции государственных органов, в частности Министерства обороны РФ. Любая критика официальной версии событий, представление альтернативных данных или независимых оценок может быть истолкована как распространение "фейков". Закон предусматривает суровые наказания, включая крупные денежные штрафы и лишение свободы на срок до 15 лет (в случае наступления тяжких последствий).[25] После введения этой статьи начались многочисленные уголовные и административные преследования граждан, журналистов и общественных активистов за их публикации и комментарии в интернете, в первую очередь касающиеся конфликта в Украине.[25]

Помимо статьи 207.3 УК РФ, существуют и другие законодательные акты, регулирующие высказывания в интернете:

- Законы об ответственности за распространение информации, выражающей "явное неуважение" к обществу, государству, официальным государственным символам, Конституции РФ или органам, осуществляющим государственную власть (так называемый "закон о неуважении к власти").
- Законы об ответственности за публичные призывы к осуществлению экстремистской или террористической деятельности, а также за оправдание терроризма. Понятия "экстремизм" и "оправдание терроризма" могут трактоваться правоприменительными органами достаточно широко.

- Законы об ответственности за клевету.
- Законодательство о запрете реабилитации нацизма.

Введение статьи 207.3 УК РФ ("о фейках об армии") [20] и ее активное правоприменение [25] стали прямым ответом государства на необходимость установления жесткого контроля над информационным полем в условиях вооруженного конфликта. Широкие и расплывчатые формулировки данной статьи, а также суровые санкции, предусмотренные ею, направлены на подавление любой информации и мнений, противоречащих официальной государственной версии событий. Это свидетельствует о целенаправленной политике по установлению государственной монополии на информацию о ключевых событиях, имеющих важное общественно-политическое значение.

Закон "о фейках" и практика его применения создают мощный "охлаждающий эффект" для свободы слова в интернете. Граждане, журналисты и средства массовой информации, опасаясь преследования, все чаще прибегают к самоцензуре.[25] Это приводит к значительному сужению пространства для открытой общественной дискуссии, независимой журналистики и критики действий властей, что негативно сказывается на состоянии гражданского общества и реализации конституционного права на свободу слова и информации. Неопределенность понятия "заведомо ложная информация" и его зависимость от официальной трактовки событий усиливают риски для любого, кто публикует информацию, отличную от распространяемой государственными источниками.

3.5. Законодательство о блокировках в интернете

В Российской Федерации сформирована и постоянно развивается разветвленная система законодательства, позволяющая государственным органам осуществлять блокировку интернет-ресурсов по широкому кругу оснований. Блокировки могут производиться как на основании судебного решения, так и во внесудебном порядке по требованию уполномоченных государственных органов, таких как Роскомнадзор или Генеральная прокуратура. Количество заблокированных интернет-ресурсов неуклонно растет, что свидетельствует об активном использовании этого инструмента государственного контроля.

3.5.1. Законодательство

Да, в России существует обширное законодательство, регулирующее порядок и

основания для блокировки интернет-ресурсов. Ключевыми нормативно-правовыми актами в этой сфере являются:

- **Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации"**: Этот закон является основополагающим и содержит общие положения о порядке ограничения доступа к информации, распространение которой в Российской Федерации запрещено. Он определяет категории запрещенной информации и процедуры ее блокировки.
- **"Закон Лугового" (поправки в ФЗ № 149-ФЗ)**: Предоставляет Генеральной прокуратуре РФ и ее заместителям право требовать от Роскомнадзора немедленной внесудебной блокировки сайтов, содержащих призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в несанкционированных публичных мероприятиях, а также распространяющих недостоверную общественно значимую информацию под видом достоверных сообщений ("фейки") и информацию, выражающую явное неуважение к органам государственной власти.
- **Законодательство о защите детей от информации, причиняющей вред их здоровью и развитию (ФЗ № 436-ФЗ)**: Устанавливает основания для блокировки ресурсов, содержащих детскую порнографию, информацию о способах совершения самоубийства, информацию о способах изготовления и использования наркотических средств и т.д.
- **Законодательство об авторских и смежных правах ("антипиратское законодательство")**: Предусматривает возможность блокировки ресурсов, незаконно распространяющих объекты авторского права, по решению суда.
- **Законодательство о противодействии экстремистской деятельности и терроризму**: Является основанием для блокировки материалов и ресурсов, признанных экстремистскими или террористическими.
- **Федеральный закон № 90-ФЗ ("о суверенном интернете")**: Хотя и не является прямым законом о блокировках, он создает техническую инфраструктуру (в частности, ТСПУ), которая используется для реализации блокировок, инициированных на основании других законов.[25]

Human Rights Watch в своих отчетах анализировала российское законодательство, принятое с 2017 года, отмечая, что оно в совокупности предоставляет властям широкие возможности по контролю интернет-инфраструктуры и цифровой активности граждан.[48]

3.5.2. Процедуры блокировок

Процедуры блокировки интернет-ресурсов в России можно разделить на два основных типа: судебные и внесудебные.

- **Судебный порядок**: Ограничение доступа к информации или интернет-ресурсу осуществляется на основании вступившего в законную силу решения суда. Иск о признании информации запрещенной к распространению и о блокировке ресурса может быть подан уполномоченным государственным органом (например, прокуратурой, Роскомнадзором по определенным категориям дел) или правообладателем (в случае нарушения авторских прав).
- **Внесудебный порядок**: Предусматривает блокировку ресурсов по решению уполномоченных государственных органов без предварительного судебного разбирательства. Наиболее часто такой механизм используется:
    - **Генеральной прокуратурой РФ и ее заместителями**: На основании "закона Лугового" для блокировки сайтов с призывами к массовым беспорядкам, экстремизму, участию в несанкционированных акциях, распространению "фейков" о социально значимых событиях или деятельности госорганов, а также информации, содержащей неуважение к власти.
    - **Роскомнадзором**: По обращениям других федеральных органов исполнительной власти (например, Федеральной налоговой службы – в отношении сайтов с нелегальными азартными играми; Федеральной службы по регулированию алкогольного рынка – в отношении сайтов, незаконно торгующих алкоголем; МВД – по вопросам детской порнографии, распространения наркотиков, информации о способах совершения самоубийства).
    - **Роскомнадзором самостоятельно**: В отношении ресурсов, содержащих детскую порнографию, информацию о способах изготовления и употребления наркотических средств, психотропных веществ и их прекурсоров, информацию о способах совершения самоубийства, а также призывы к совершению самоубийства.

После принятия решения (судебного или внесудебного) информация о ресурсе (доменное имя, URL-адрес страницы, сетевой адрес) вносится в Единый автоматизированный информационный систему "Единый реестр доменных имён, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию,

распространение которой в Российской Федерации запрещено" (ЕАИС "Единый реестр"). Операторы связи, действующие на территории России, обязаны в течение установленного законом срока (обычно 24 часа) ограничить доступ к ресурсам, внесенным в данный реестр. Блокировка может осуществляться различными техническими способами, включая блокировку по IP-адресу, по URL-адресу, по доменному имени, а также с использованием технических средств противодействия угрозам (ТСПУ), которые позволяют осуществлять глубокую проверку пакетов (DPI) и более таргетированную фильтрацию трафика.

Отчет Freedom House отмечает, что процедуры блокировки, осуществляемые Роскомнадзором, часто остаются непрозрачными, и ограничения доступа могут производиться с нарушением процессуальных норм, включая блокировку сайтов без предварительного уведомления их владельцев.[25]

3.5.3. Реестры заблокированных интернет-ресурсов

Да, в Российской Федерации существует официальный централизованный реестр интернет-ресурсов, содержащих информацию, распространение которой запрещено. Этот реестр известен как **Единый автоматизированный информационная система "Единый реестр доменных имён, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено"** (сокращенно ЕАИС "Единый реестр" или просто "Реестр запрещенных сайтов"). Ведение данного реестра возложено на Роскомнадзор.[49]

Доступ к полной базе данных этого реестра для широкой общественности **ограничен**. Обычные пользователи не могут просмотреть весь список заблокированных ресурсов. Однако Роскомнадзор предоставляет публичный сервис на своем официальном сайте (eais.rkn.gov.ru), который позволяет проверить, находится ли конкретный URL-адрес, доменное имя или IP-адрес в реестре.[49] Операторы связи, имеющие лицензию на оказание услуг связи на территории РФ, получают от Роскомнадзора регулярные выгрузки из реестра для осуществления технических мер по ограничению доступа к запрещенным ресурсам.

Помимо официального реестра, существуют неофициальные проекты и инициативы, которые пытаются агрегировать данные о блокировках и предоставлять их в более открытом виде. Одним из наиболее известных таких

проектов является реестр, который ведет общественная организация "Роскомсвобода".[50] Эти неофициальные реестры часто собирают информацию из различных источников, включая данные, доступные операторам связи, сообщения пользователей, собственные технические измерения и анализ публичных решений судов и госорганов.

Существуют как официальные, так и неофициальные ресурсы, предоставляющие информацию о заблокированных сайтах в России:

1. **Официальный сервис проверки наличия ресурса в Едином реестре Роскомнадзора**:
   - **Ссылка**: http://eais.rkn.gov.ru/ [49]
   - **Описание**: Данный сервис, предоставляемый Роскомнадзором, позволяет любому пользователю проверить, внесен ли конкретный домен, URL-адрес страницы или IP-адрес в Единый реестр запрещенных сайтов. Сервис не предоставляет полного списка заблокированных ресурсов, а лишь отвечает на конкретный запрос о статусе указанного ресурса. Через официальный сайт Роскомнадзора (rkn.gov.ru) также можно направить сообщение о наличии в сети Интернет противоправной информации.[52]
2. **Реестр заблокированных сайтов проекта "Роскомсвобода"**:
   - **Ссылка**: https://reestr.rublacklist.net/ [50]
   - **Описание**: Это общественный проект, который с 2012 года собирает и систематизирует информацию о блокировках интернет-ресурсов в России. "Роскомсвобода" агрегирует данные из различных источников, включая официальные выгрузки (когда они были доступны), данные от операторов связи, сообщения пользователей и собственные технические исследования. Ресурс предоставляет статистику по блокировкам, возможность поиска по своей базе данных, а также API для автоматизированного получения информации. Он стремится обеспечить большую прозрачность в вопросе интернет-цензуры в стране.

Помимо этих двух основных ресурсов, существуют и другие проекты и инструменты, которые могут отслеживать блокировки, например, Censor Tracker (расширение от "Роскомсвободы") [50], а также международные проекты, такие как OONI (Open Observatory of Network Interference), которые собирают данные о сетевых аномалиях, указывающих на цензуру.

3.5.4. Развитие блокировок

Open Observatory of Network Interference (OONI) является международным проектом, который занимается сбором и анализом данных о цензуре в интернете по всему миру, используя для этого специализированное программное обеспечение OONI Probe. Отчеты и данные OONI предоставляют ценную информацию о масштабах и методах блокировок в различных странах, включая Российскую Федерацию.

Анализ данных OONI, особенно за период после февраля 2022 года, показывает значительное усиление интернет-цензуры в России:

- **Массовая блокировка новостных ресурсов**: Практически сразу после начала конфликта в Украине российские интернет-провайдеры начали блокировать доступ к большому числу как иностранных (например, BBC, Deutsche Welle), так и независимых российских новостных веб-сайтов (таких как "Медуза", "Новая Газета", The New Times).[53]
- **Рост числа заблокированных доменов**: По данным OONI, если в 2023 году было подтверждено блокирование 139 новостных доменов в России, то к сентябрю 2024 года это число увеличилось как минимум до 279 доменов. Это свидетельствует о продолжающемся и расширяющемся подавлении независимых источников информации.[53]
- **Технические методы блокировок**:
    - **TLS-интерференция**: Большинство блокировок новостных сайтов в России, по данным OONI, реализуются посредством вмешательства в процесс установления TLS-соединения (TLS interference). Это часто проявляется в виде тайм-аута TLS-сессии или инъекции RST-пакета (сброса соединения) после отправки сообщения ClientHello во время TLS-рукопожатия. Такие методы указывают на использование систем глубокой проверки пакетов (DPI), которые анализируют поле Server Name Indication (SNI) в ClientHello для принятия решения о блокировке.[53]
    - **DNS-блокировки**: Также продолжают применяться блокировки на уровне DNS, когда при запросе IP-адреса заблокированного домена возвращается ложный или нулевой ответ. Эти блокировки, по-видимому, реализуются провайдерами децентрализованно и могли существовать еще до массового внедрения ТСПУ.[53]
- **Централизованное управление блокировками**: Несмотря на то, что технические средства противодействия угрозам (ТСПУ), оснащенные DPI, устанавливаются каждым оператором связи на своей сети

(децентрализованное развертывание), сами решения о блокировках и списки блокируемых ресурсов, вероятно, управляются централизованно Роскомнадзором. Об этом свидетельствует одновременность блокировок одних и тех же ресурсов на сетях разных провайдеров, а также корреляция блокировок с датами внесения ресурсов в реестр Роскомнадзора.[53]

- **"Война цензуры" с ЕС**: В ответ на блокировку российских государственных СМИ (таких как Sputnik и RT) в странах Европейского Союза, российские власти приняли ответные меры, заблокировав доступ к ряду европейских новостных изданий на территории РФ. OONI зафиксировала такие блокировки с августа 2024 года.[53]
- **Непрозрачность блокировок**: OONI отмечает, что реализация интернет-цензуры становится все менее прозрачной. Если раньше пользователи часто видели страницу-заглушку, информирующую о блокировке, то сейчас блокировки могут маскироваться под технические сбои.[54]

Вывод по развитию блокировок: Данные OONI и других наблюдателей [25] подтверждают, что в России происходит систематическое и постоянно расширяющееся применение интернет-блокировок, особенно в отношении новостных ресурсов, независимых СМИ и контента, который власти считают нежелательным или "фейковым". Технические методы блокировок становятся все более изощренными, с активным использованием систем DPI, управляемых централизованно. Эта практика серьезно ограничивает право граждан на доступ к информации и свободу выражения мнений. Эволюция законодательства и практики блокировок в России демонстрирует явный переход от точечных ограничений (например, по узким категориям запрещенной информации, таким как детская порнография или пропаганда наркотиков) к широкомасштабной политической и новостной цензуре, особенно усилившейся после февраля 2022 года.

Непрозрачность процедур блокировки [25] и ограниченный публичный доступ к полному официальному реестру заблокированных сайтов [49] создают атмосферу правовой неопределенности. Это затрудняет для владельцев ресурсов и пользователей понимание точных причин блокировки и возможность ее эффективного оспаривания, что усиливает риски произвола со стороны регулирующих органов и ограничивает право на доступ к информации и справедливое судебное разбирательство. Использование современных технологий блокировки, таких как DPI для анализа SNI и вмешательства в

TLS-соединения [53], свидетельствует о значительном технологическом потенциале государства в области контроля интернета. Это делает традиционные методы обхода блокировок менее эффективными и требует от пользователей поиска более сложных и технологически продвинутых решений для сохранения доступа к информации.

Логическим развитием и ужесточением политики блокировок стало внедрение в России с августа-сентября 2025 года механизма так называемых "белых списков". Эта технология применяется во время массовых отключений мобильного интернета и представляет собой фундаментальный сдвиг в подходе к цензуре: вместо блокировки отдельных "запрещенных" ресурсов (черный список) доступ в сеть полностью перекрывается, за исключением ограниченного перечня предварительно одобренных сайтов и сервисов. Таким образом реализуется принцип "запрещено всё, что не разрешено".

Первые эксперименты по применению "белых списков" были зафиксированы в сентябре 2025 года в ряде регионов, включая Дагестан, Татарстан, Ростовскую и Волгоградскую области. Согласно разъяснениям Минцифры, в перечень разрешенных ресурсов вошли "наиболее востребованные и социально значимые" российские сервисы: портал "Госуслуг", сайты госорганов, социальные сети "ВКонтакте" и "Одноклассники", сервисы "Яндекса", маркетплейсы Ozon и Wildberries, а также личные кабинеты операторов связи. При этом список является динамическим и может обновляться еженедельно на основе анализа популярности ресурсов.

Внедрение "белых списков" является наиболее радикальным на сегодняшний день шагом по ограничению доступа к информации и построению изолированной цифровой экосистемы. Данный механизм, работающий пока только в мобильных сетях, позволяет властям в любой момент отрезать пользователей от глобального интернета, оставляя им лишь доступ к одобренным государством сервисам. Это не только качественно новый технологический уровень цензуры, но и серьезный удар по цифровым правам граждан, создающий условия для полного контроля над информационным полем во время шатдаунов.

4. Нарушения прав человека в интернете

Многочисленные отчеты как российских, так и международных правозащитных организаций, включая Freedom House [25], Human Rights Watch [48], и "Роскомсвободу" [25], а также сообщения независимых средств массовой информации, свидетельствуют о систематических и широкомасштабных нарушениях прав человека в российском сегменте интернета. Эти нарушения охватывают широкий спектр прав, включая свободу выражения мнений, право на доступ к информации, право на неприкосновенность частной жизни и право на справедливое судебное разбирательство.

Ситуация особенно усугубилась после февраля 2022 года, что отразилось в резком падении позиций России в международных рейтингах свободы интернета.[25] Ключевые проявления нарушений цифровых прав включают: произвольные и массовые блокировки интернет-ресурсов, в том числе независимых СМИ и социальных сетей; уголовное и административное преследование граждан за их высказывания в интернете, особенно по новым статьям о "фейках" и "дискредитации армии"; усиление давления на независимые медиа-проекты и неправительственные организации, работающие в цифровой сфере; расширение практик государственной слежки и требований по хранению пользовательских данных, что подрывает право на приватность.

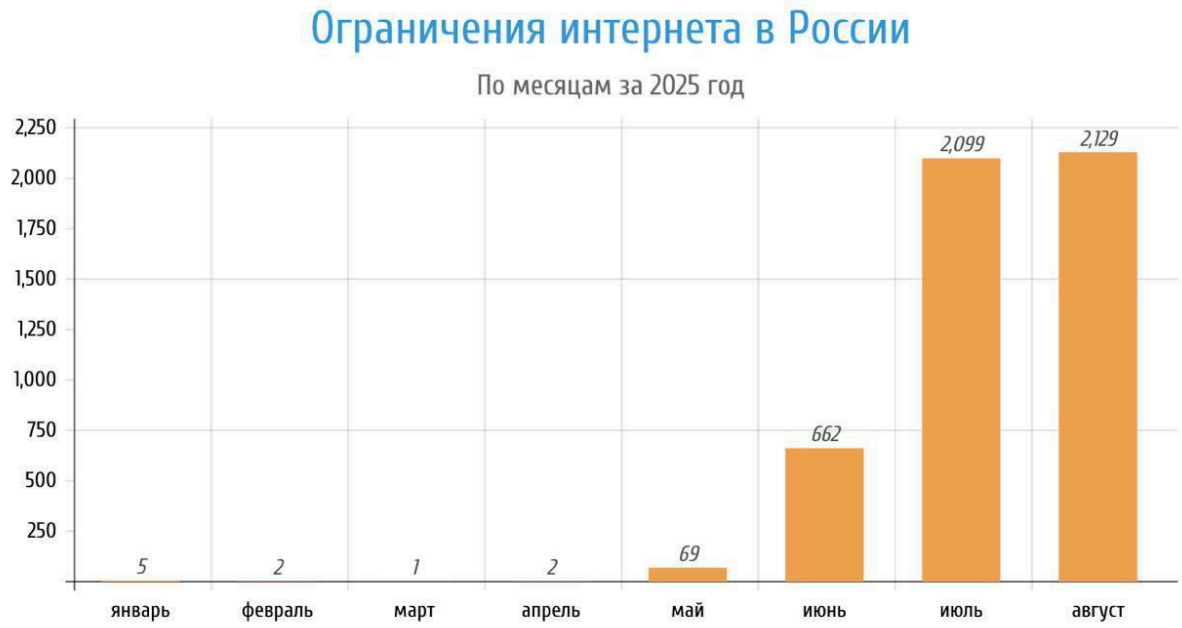
4.1. Отключение интернета по приказу властей

"Закон о суверенном интернете" создал техническую и правовую базу, которая в 2025 году была использована для массового ограничения доступа к связи. Если ранее отключения интернета российскими властями фиксировались преимущественно за пределами РФ, в частности на территории Украины, то начиная с мая 2025 года эта практика стала активно и масштабно применяться внутри самой России.

Ситуация кардинально изменилась летом 2025 года, когда после серии атак беспилотников на военные объекты в глубине страны, власти начали применять тотальные отключения мобильного интернета как меру противодействия. Эта практика быстро превратилась из единичных случаев в массовое явление, затронувшее десятки регионов. Мониторинг и подсчет случаев отключений

мобильного интернета ведет, в частности, проект **"НаСвязи"**, фиксирующий географию и продолжительность шатдаунов.

График 8: Динамика сообщений об отключениях интернета в регионах РФ за 2025 год



Таким образом, к концу 2025 года произошел качественный сдвиг в политике контроля над интернетом. Если ранее основной акцент делался на фильтрации и блокировке контента, то теперь к этому добавился инструмент полного отключения доступа к мобильному интернету на обширных территориях. Массовые шатдауны стали новой реальностью и одним из ключевых элементов контроля над информационным пространством в России.

4.2. Криминализация высказываний в интернете

В Российской Федерации наблюдается устойчивая тенденция к криминализации высказываний в интернете, особенно тех, которые касаются общественно-политических тем, деятельности государственных органов и Вооруженных Сил. Это приводит к многочисленным случаям как уголовного (лишение свободы, условные сроки), так и административного (штрафы, аресты) преследования граждан за их публикации, комментарии, лайки или репосты в

социальных сетях и на других интернет-платформах.

Наиболее резонансным инструментом такого преследования в последние годы стала статья 207.3 Уголовного кодекса РФ ("о фейках об армии"), введенная в марте 2022 года.[20] Эта статья активно применяется для подавления информации о конфликте в Украине, отличающейся от официальной позиции российских властей.

Примеры наиболее упоминаемых случаев преследования:

- **Дело Марии Пономаренко**: Журналистка из Барнаула Мария Пономаренко была приговорена в апреле 2023 года к шести годам колонии общего режима по статье о "военных фейках" (п. "д" ч. 2 ст. 207.3 УК РФ) за пост в Telegram-канале об авиаударе по драмтеатру в Мариуполе.[56] Позднее, уже находясь в колонии, против нее было возбуждено еще одно уголовное дело за предполагаемое нападение на сотрудников ФСИН, по которому ей добавили срок.[56] Дело Пономаренко получило широкий общественный резонанс, сообщалось о серьезных проблемах с ее психологическим состоянием в заключении.
- **Дело Ильи Яшина**: Оппозиционный политик Илья Яшин был приговорен в декабре 2022 года Мещанским судом Москвы к 8 годам и 6 месяцам колонии общего режима по делу о распространении "фейков" о российской армии по мотивам политической ненависти (п. "д" ч. 2 ст. 207.3 УК РФ).[58] Поводом для уголовного преследования стал его прямой эфир на YouTube-канале от 7 апреля 2022 года, в котором он рассказывал о событиях в украинском городе Буча, в том числе ссылаясь на международные источники и репортажи СМИ. Обвинение утверждало, что Яшин "утвердительно сообщил под видом достоверных сведений", что российские военные убивали жителей Бучи. Яшин вину не признал, настаивая на том, что представлял различные точки зрения и выполнял свой гражданский долг, критически оценивая информацию.[58]

Помимо этих громких дел, существует множество других случаев привлечения к ответственности по статье 207.3 УК РФ, а также по другим статьям, таким как "дискредитация использования Вооруженных Сил РФ" (ст. 280.3 УК РФ и ст. 20.3.3 КоАП РФ), статьи об экстремизме, оправдании терроризма, неуважении к власти и клевете. Отчет Freedom House за 2022 год указывает, что после принятия закона о "фейках" россиянам стали еще чаще выписывать штрафы и возбуждать дела за публикации и комментарии в соцсетях, а 8 июля 2022 года был вынесен

первый уголовный приговор по новой статье.[25] По крайней мере, в 53 странах мира (включая Россию, согласно контексту отчета) пользователи столкнулись с юридическими последствиями за самовыражение в интернете, вплоть до длительных тюремных сроков.[25]

Такая правоприменительная практика создает атмосферу страха и способствует самоцензуре среди интернет-пользователей, опасающихся преследования за выражение своего мнения, даже если оно основано на открытых источниках или является оценочным суждением.

4.3. Преследование СМИ и НКО

Средства массовой информации и негосударственные организации (НКО) в России, особенно те, которые занимают независимую позицию или критикуют действия властей, подвергаются значительному давлению, в том числе за их деятельность и публикации в интернете. Это давление проявляется в различных формах:

- **Блокировки интернет-ресурсов**: После 24 февраля 2022 года российские власти резко активизировали усилия по блокированию доступа к веб-сайтам независимых СМИ и платформ социальных сетей. Были заблокированы Facebook, Instagram и Twitter. По подсчетам "Роскомсвободы", к концу мая 2022 года было заблокировано более 5000 веб-сайтов по соображениям "военной цензуры", включая российские независимые СМИ (например, DOXA, "Медуза", "Медиазона", "7x7"), зарубежные медиа (BBC, "Голос Америки", Deutsche Welle, Bellingcat), а также сайты правозащитных организаций (Amnesty International, Human Rights Watch, "Голос").[25]
- **Законодательство об "иностранных агентах" и "нежелательных организациях"**: Широко применяется законодательство об "иностранных агентах", которое накладывает на СМИ и НКО, а также на физических лиц, получающих иностранное финансирование (даже косвенное) и занимающихся "политической деятельностью" (трактуемой очень широко), обременительные требования по отчетности, маркировке материалов и аудиту. Многие независимые СМИ и НКО были внесены в реестры "иностранных агентов", что существенно затрудняет их работу, приводит к потере рекламодателей, доверия аудитории и создает риски преследования. Деятельность организаций, признанных "нежелательными" на территории РФ, полностью запрещена, а сотрудничество с ними влечет уголовную ответственность. Закон об "иностранных агентах" был значительно

расширен.[25]

- **Штрафы и административное давление**: СМИ и НКО, а также их руководители и сотрудники, регулярно подвергаются крупным штрафам за несоблюдение требований законодательства (например, за отсутствие маркировки "иностранного агента", за отказ удалять "запрещенный контент" по требованию Роскомнадзора). Роскомнадзор многократно штрафовал онлайн-платформы за отказ удалять контент и локализовать пользовательские данные.[25]
- **Уголовное преследование журналистов и сотрудников НКО**: Журналисты и сотрудники НКО могут подвергаться уголовному преследованию по различным статьям, включая "фейки об армии", "дискредитацию армии", "экстремизм", "клевету".
- **Вынужденное прекращение деятельности или релокация**: Из-за накладываемых штрафов, блокировок доступа к сайтам, а также преследований отдельных журналистов, некоторые СМИ были вынуждены прекратить свою деятельность в России или перевести свои редакции за рубеж, чтобы не подвергать еще большей опасности своих сотрудников.[25]
- **Признание Meta экстремистской организацией**: Решение российского суда о признании компании Meta (владеющей Facebook и Instagram) экстремистской организацией и запрете ее деятельности в РФ создало дополнительные риски для пользователей этих платформ и для бизнеса, использовавшего их для продвижения.[25]

Отчет Human Rights Watch за 2020 год анализировал совокупность законов, принятых с 2017 года (включая "пакет Яровой"), которые предоставили российским властям широкие возможности по контролю интернет-инфраструктуры и цифровой активности, что напрямую затрагивает деятельность СМИ и НКО.[48] Доклад Госдепартамента США о практиках в области прав человека в России за 2022 год также освещает проблемы, связанные с произвольным или незаконным вмешательством в частную жизнь, что актуально для деятельности онлайн-СМИ и НКО.[60]

Эти меры приводят к значительному сокращению пространства для независимой журналистики и деятельности гражданского общества в России, ограничению доступа граждан к альтернативным источникам информации и усилению государственной пропаганды.

5. Гражданское общество в области управления интернетом

Гражданское общество в Российской Федерации, занимающееся вопросами управления интернетом и защиты цифровых прав, действует в сложных условиях. С одной стороны, существует ряд организаций и активистов, которые стремятся отстаивать принципы свободы информации, приватности и открытости сети. С другой стороны, их деятельность сталкивается с усиливающимся давлением со стороны государства, законодательными ограничениями и сужением пространства для публичной дискуссии и влияния на принятие решений.

Несмотря на это, организации гражданского общества продолжают играть важную роль в мониторинге нарушений цифровых прав, оказании правовой помощи пострадавшим, просвещении пользователей по вопросам кибербезопасности и обхода блокировок, а также в попытках участвовать в обсуждении законодательных инициатив, касающихся интернета. Они также способствуют повышению осведомленности общества о проблемах интернет-цензуры и необходимости защиты цифровых свобод.

5.1. Организации

В России существует несколько организаций, которые активно занимаются защитой прав граждан в интернете, мониторингом законодательства и правоприменительной практики, а также просветительской деятельностью. Среди них можно выделить:

- **"Роскомсвобода"**:
    - **Описание**: "Роскомсвобода" – одна из ведущих российских общественных организаций, специализирующаяся на защите цифровых прав и продвижении идей свободы информации, приватности и анонимности в интернете. Организация была создана в 2012 году в ответ на введение Единого реестра запрещенных сайтов. "Роскомсвобода" ведет мониторинг блокировок интернет-ресурсов (проект reestr.rublacklist.net), анализирует законодательные инициативы в сфере регулирования интернета, оказывает юридическую помощь гражданам и организациям, чьи цифровые права были нарушены, проводит общественные кампании и образовательные мероприятия.[50] Техническая

команда "Роскомсвободы" также разрабатывает инструменты для обхода цензуры и повышения цифровой безопасности, такие как расширение Censor Tracker и маркетплейс VPN-сервисов VPNlove.me.[50]
    - **Интернет-ресурс**: https://roskomsvoboda.org/ [61]
- **Международная правозащитная группа "Агора"**:
    - **Описание**: "Агора" – это объединение юристов и адвокатов, оказывающих правовую помощь по делам, связанным с нарушением прав человека в России, включая дела о свободе слова, свободе собраний и преследовании активистов, журналистов и блогеров за их высказывания в интернете. "Агора" была основана в 2005 году и вела множество резонансных дел, защищая граждан от незаконных действий государственных чиновников.[62] Хотя основной фокус "Агоры" шире, чем только цифровые права, значительная часть их работы связана именно с защитой прав в онлайн-пространстве. В 2014 году организация была удостоена международной правозащитной премии Рафто. Впоследствии российские власти признали Ассоциацию "Агора" "иностранным агентом", а в 2016 году она была ликвидирована по решению суда. Международная правозащитная группа "Агора" продолжила свою деятельность, но в июне 2023 года Генеральная прокуратура РФ признала ее деятельность "нежелательной" на территории России.[62]
    - **Интернет-ресурс**: agora.legal (основной сайт международной группы), openinform.ru (упоминается как сайт в Википедии для ранее существовавшей организации).[62]
- **Общество Защиты Интернета (ОЗИ)**:
    - **Описание**: российская общественная организация, основанная в 2016 году, которая занимается исследованием свободы и связности интернета в России. Организация проводит мониторинг и анализ законодательных инициатив, направленных на регулирование сети, отслеживает случаи блокировок и отключений, а также ведет проекты по измерению уровня интернет-проникновения и связности регионов. ОЗИ регулярно публикует отчеты, исследования и комментарии по ключевым вопросам развития Рунета, выступая за сохранение его открытости и доступности.
    - **Интернет-ресурс**: https://ozi-ru.net/

Помимо этих организаций, существуют и другие группы, юристы и активисты, которые вносят свой вклад в защиту цифровых прав в России, однако их деятельность часто менее формализована или освещена в предоставленных

материалах.

5.2. VPN и средства обхода блокировок

Использование VPN (Virtual Private Network) и других средств обхода блокировок получило широкое распространение в России, особенно на фоне ужесточения интернет-цензуры и блокировки популярных зарубежных социальных сетей, новостных ресурсов и других веб-сайтов. VPN-сервисы позволяют пользователям получать доступ к заблокированному контенту, а также повышать уровень своей анонимности и приватности в сети.

Российские власти предпринимают активные шаги по ограничению доступа к самим VPN-сервисам и протоколам, которые они используют, а также к информации о способах обхода блокировок. Это создает своего рода "гонку вооружений" между регуляторами, стремящимися полностью контролировать информационное пространство, и пользователями, ищущими пути сохранения доступа к глобальной сети.

5.2.1. Статус VPN-услуг

Формально использование VPN-сервисов гражданами для личных целей в России **не запрещено**.[64] Однако с 2017 года действует законодательство (поправки в Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации"), которое обязывает владельцев VPN-сервисов и анонимайзеров подключаться к Федеральной государственной информационной системе (ФГИС), содержащей реестр заблокированных сайтов, и фильтровать трафик своих пользователей, не допуская их к запрещенным ресурсам.[65] VPN-сервисы, которые отказываются выполнять эти требования, могут быть заблокированы Роскомнадзором.

С 1 марта 2024 года вступил в силу приказ Роскомнадзора, который вводит критерии для блокировки сайтов, содержащих информацию о способах обхода блокировок, установленных в России. Это включает запрет на популяризацию VPN-сервисов, которые не исполняют требования российского законодательства (т.е. не фильтруют трафик).[66] Запрещено публиковать информацию о VPN, если она описывает, как с его помощью обойти блокировки ресурсов.[64] С 30 ноября 2024 года ограничения также должны были распространиться на научную, научно-техническую и статистическую информацию о способах обхода

блокировок.[66]

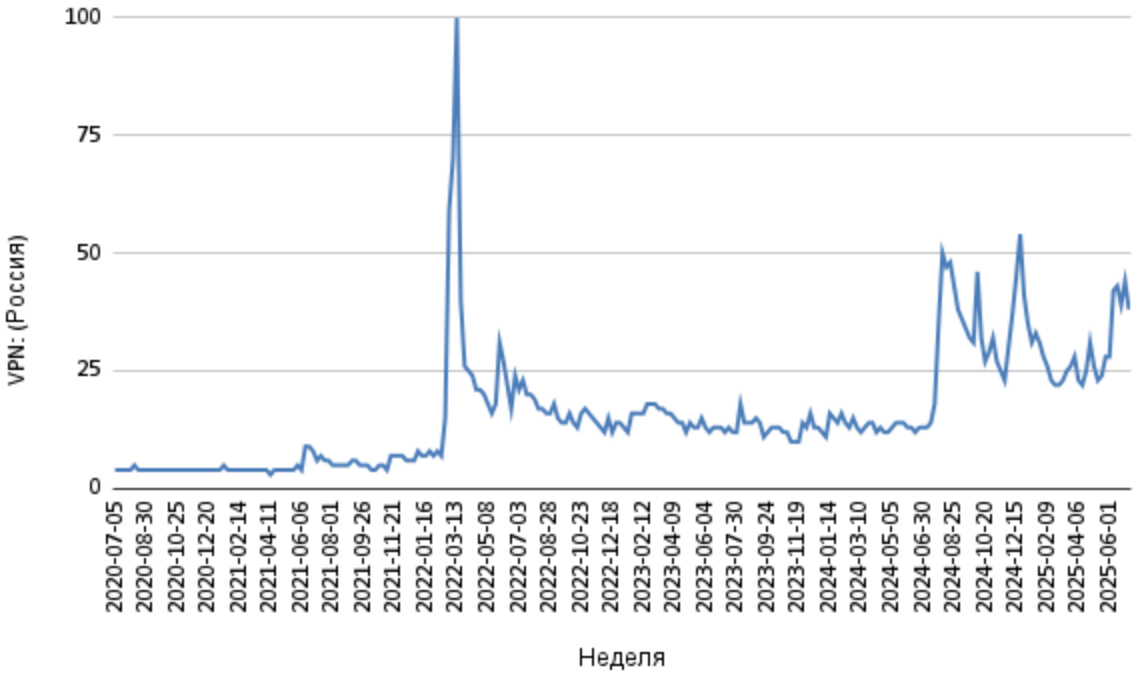
Основные законы, регулирующие эту сферу:

- **Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации"** (в редакции Федерального закона от 29.07.2017 № 276-ФЗ, который ввел положения о VPN и анонимайзерах).[65]
- **Приказы Роскомнадзора**, устанавливающие порядок блокировки VPN-сервисов и информации о них.

5.2.2. Количество пользователей VPN

Точные данные о количестве пользователей VPN в России по годам собрать сложно, так как многие исследования опираются на опросы или косвенные оценки. Тем не менее, имеющиеся данные указывают на значительный рост популярности VPN-сервисов, особенно после февраля 2022 года.

График 9: Динамика поисковых запросов про VPN в Российской Федерации (2020-2025)



Источник: trends.google.com

Анализ динамики поисковых запросов по теме "VPN" в России демонстрирует кардинальное изменение роли данной технологии для пользователей и напрямую коррелирует с этапами усиления государственной интернет-цензуры.

График четко разделяется на три периода. До начала 2022 года интерес к VPN находился на стабильно низком, фоновом уровне, что говорит о его использовании преимущественно технически подкованной, нишевой аудиторией. С марта 2022 года ситуация радикально меняется: VPN трансформируется в массовый инструмент, необходимый для доступа к базовым информационным ресурсам. Это подтверждается как пиковыми значениями, так и установлением нового, значительно более высокого базового уровня интереса к технологии на всем последующем временном отрезке.

Пики поисковой активности являются прямым индикатором реакции населения на действия регулятора (Роскомнадзора) и служат точным маркером введения новых ограничений.

Абсолютный пик (март 2022 года): Максимальное значение (100) было достигнуто в период с конца февраля по середину марта 2022 года. Этот взрывной рост интереса однозначно связан с началом полномасштабных боевых действий в Украине и последовавшими за этим беспрецедентными по своему масштабу блокировками. В этот короткий промежуток времени в России были заблокированы ключевые социальные сети (Facebook, Instagram, Twitter) и множество независимых новостных изданий. Данный пик представляет собой единовременную, "шоковую" реакцию миллионов пользователей, впервые столкнувшихся с невозможностью доступа к привычным платформам.

Серия пиков (с августа 2024 года): Вторая волна высокой активности, начавшаяся в августе 2024 года, связана с применением новой тактики ограничения — так называемым "замедлением" трафика к видеохостингу YouTube. В отличие от полной блокировки, троттлинг делает использование сервиса практически невозможным из-за постоянной буферизации видео и низкой скорости загрузки. В этой ситуации VPN становится для пользователей ключевым инструментом не столько для обхода блокировки, сколько для восстановления базовой работоспособности и приемлемой скорости доступа к критически важному видеоконтенту.
Волнообразный характер спроса в этот период объясняется тем, что пользователи ищут не просто любой VPN, а тот, который эффективно справляется

с обходом троттлинга. Это указывает на новый, более сложный этап противостояния, когда регулятор пытается ограничивать доступ к отдельным сервисам, не блокируя их полностью, а пользователи вынуждены постоянно искать и тестировать новые технологические решения для сохранения качества доступа в Интернет.

По данным Forbes на декабрь 2023 года, основной возраст пользователей VPN – 35–44 года (63% от использующих VPN в этой группе). При этом доля пользователей в возрасте 25–34 лет выросла на 10 п.п. по сравнению с 2022 годом.[69] Среди молодежи в возрасте 18–24 лет VPN пользуются более половины – 62% опрошенных (данные "Левада-Центра" на март 2023).[68]

Блокировки VPN-сервисов и протоколов:
Роскомнадзор активно блокирует VPN-сервисы, которые не сотрудничают с властями и позволяют обходить блокировки. Блокировки осуществляются как путем внесения IP-адресов и доменов самих VPN-сервисов в реестр запрещенных сайтов, так и путем блокировки VPN-протоколов с использованием ТСПУ (DPI).

Хронология блокировок протоколов [66]:

- **Сентябрь 2021 г.**: Начало блокировок VPN-сервисов (VyprVPN, Opera VPN).
- **2022 г.**: Попытки блокировать сервисы через API-хосты, IP-адреса; сообщения о блокировке IPsec и IKEv2 в некоторых регионах.
- **Начало 2023 г.**: Блокировки протоколов OpenVPN и IKEv2.
- **Май, Август, Сентябрь 2023 г.**: Волны частичных и временных блокировок OpenVPN, IKEv2, IPSec, WireGuard. К концу сентября WireGuard перестал работать примерно у 20% пользователей.
- **2024 г.**:
  - С 1 августа 2024 г. – блокировка WireGuard во многих регионах.
  - С 15 октября 2024 г. – блокировка Shadowsocks на мобильном интернете.
  - Активнее блокируется OpenVPN.
  - Сообщается о блокировках Outline (клиента для VPN).
  - Блокировки часто носят не массовый и не долгосрочный характер, протоколы могут становиться доступными и снова недоступными.[66]
- **Удаление из магазинов приложений**: В июле 2024 года Apple по запросу Роскомнадзора начала удалять VPN-приложения из российского AppStore.[66]

Методы блокировки включают: внесение сайтов VPN в реестр, блокировку IP-адресов серверов, блокировку протоколов с помощью ТСПУ (DPI), удаление приложений из магазинов, запрет на популяризацию VPN.[66]

5.2.3. Случаи преследования за использование VPN

В предоставленных материалах **отсутствует информация** о случаях уголовного или административного преследования **рядовых пользователей** исключительно за сам факт использования VPN-сервисов для личных целей. Действующее законодательство не предусматривает прямой ответственности для граждан за использование VPN для доступа к заблокированным ресурсам.

Однако, следует учитывать несколько аспектов:

1. **Ответственность за распространение информации**: Если пользователь с помощью VPN получает доступ к запрещенной информации и затем распространяет ее (например, делает репост), он может быть привлечен к ответственности за само распространение этой информации (например, по статьям о "фейках", экстремизме и т.д.), независимо от того, использовался ли VPN для доступа к первоисточнику.
2. **Ответственность для владельцев VPN-сервисов**: Законодательство предусматривает ответственность для владельцев VPN-сервисов и анонимайзеров за отказ от сотрудничества с властями (неподключение к ФГИС, нефильтрация трафика).
3. **Деанонимизация**: Использование VPN не гарантирует полной анонимности, и в случае совершения противоправных действий с использованием VPN, правоохранительные органы могут предпринимать попытки установить личность пользователя.

Информация о преследовании **организаций, предоставляющих услуги VPN**, в предоставленных материалах сводится к их блокировкам Роскомнадзором и требованиям о подключении к ФГИС. Прямых данных об уголовных делах против владельцев VPN-сервисов именно за предоставление услуг VPN (а не за сопутствующие правонарушения) в этих материалах нет.

5.2.4. Мониторинг блокировок

Мониторингом блокировок интернет-ресурсов в России занимаются несколько организаций и проектов:

1. **"Роскомсвобода"**:
    - Ведет общедоступный реестр заблокированных сайтов (reestr.rublacklist.net).[50]
    - Публикует новости и аналитику по теме блокировок и интернет-цензуры.
    - Разрабатывает инструменты для мониторинга и обхода блокировок (например, Censor Tracker).[50]
    - **Дайджест сообщений (на основе предоставленных материалов)**:
        - **Декабрь 2022 г.**: "Роскомсвобода" сообщила о блокировке 14.8 тысяч сайтов за неделю (5-11 декабря), что было значительно выше среднего показателя (4.9 тысяч сайтов в неделю в 2022 г.). Отмечалось, что таких массовых блокировок не наблюдалось с 2018 и 2021 годов. Большинство блокировок (60%) проводились по судебным решениям, 14% - по решениям неназванного ведомства (предположительно, Генпрокуратуры).[51]
        - **Общая деятельность**: "Роскомсвобода" с момента своего основания в 2012 году отслеживает законодательную деятельность и правоприменение в области регулирования интернета, освещает резонансные случаи блокировок, ужесточения законов и преследования граждан.[61]
2. **OONI (Open Observatory of Network Interference)**:
    - Международный проект, собирающий данные о цензуре в интернете по всему миру с помощью тестов OONI Probe.[54]
    - Публикует отчеты и данные о блокировках в России.
    - **Дайджест сообщений (на основе предоставленных материалов)**:
        - **Отчет "Censorship Chronicles: The systematic suppression of independent media in Russia" (опубликован в 2024 г., охватывает период с сентября 2023 по сентябрь 2024 г.)**: Подтверждена блокировка как минимум 279 новостных доменов (рост со 139 в предыдущем исследовании 2023 г.). Большинство блокировок реализуются через TLS-интерференцию (с использованием DPI/ТСКУ), также применяются DNS-блокировки. Блокировки, вероятно, централизованно управляются Роскомнадзором. Отмечена "война цензуры" с ЕС.[53]
        - **Общие данные (февраль 2025 г.)**: OONI собрала более двух миллиардов сетевых измерений в более чем 200 странах. OONI Explorer является одной из крупнейших открытых баз данных по интернет-цензуре. В своих последних сообщениях OONI указывала на

блокировку Discord в России.[54]

3. **Другие проекты**: Могут существовать и другие локальные или международные инициативы, отслеживающие доступность интернет-ресурсов в России, но они не были подробно освещены в предоставленных материалах.

Мониторинг блокировок показывает, что интернет-цензура в России является динамичным и постоянно развивающимся процессом. Власти не только расширяют список оснований для блокировок и количество блокируемых ресурсов, но и совершенствуют технические методы их реализации, стремясь сделать обход ограничений более сложным для пользователей.

6. Вывод

Анализ состояния цифровых прав и интернета в Российской Федерации за период с 2019 по 2025 год выявляет сложную и противоречивую картину. С одной стороны, Россия демонстрирует высокий уровень проникновения интернета, развитие цифровых сервисов и наличие современной телекоммуникационной инфраструктуры в крупных городах. С другой стороны, этот период характеризуется последовательным и значительным усилением государственного контроля над интернет-пространством, что приводит к существенным ограничениям цифровых прав и свобод граждан.

Соблюдение прав человека в области доступа к информации:

Право на доступ к информации в России подвергается серьезным ограничениям. Это проявляется через:

1. **Масштабные блокировки интернет-ресурсов**: Государство активно использует механизм блокировок для ограничения доступа к широкому спектру информации, включая независимые СМИ, оппозиционные сайты, контент правозащитных организаций и зарубежные социальные сети. Особенно интенсивно блокировки применяются в отношении информации, касающейся общественно-политической ситуации в стране и за рубежом, а также критики действий властей. Использование современных технологий DPI (ТСКУ) делает эти блокировки все более эффективными.
2. **Законодательство о "фейках" и "дискредитации"**: Введенные нормы, особенно статья 207.3 УК РФ, создали правовую основу для уголовного преследования за распространение информации, не соответствующей

официальной позиции государства. Это привело к многочисленным уголовным делам, тюремным срокам и штрафам для журналистов, активистов и обычных граждан, что оказывает сильный "охлаждающий эффект" на свободу слова.

3. **Давление на СМИ и НКО**: Независимые медиа и неправительственные организации сталкиваются с беспрецедентным давлением, включая блокировки, присвоение статусов "иностранного агента" и "нежелательной организации", штрафы и преследование сотрудников. Это приводит к сокращению числа независимых источников информации и сужению пространства для общественной дискуссии.
4. **Контроль над инфраструктурой**: "Закон о суверенном интернете" создал предпосылки для централизованного управления Рунетом, включая возможность его изоляции.
5. **Ограничение использования средств обхода блокировок**: Государство предпринимает усилия по блокировке VPN-сервисов и информации о способах обхода цензуры, стремясь ограничить доступ граждан к заблокированным ресурсам.

В совокупности эти факторы свидетельствуют о системном характере нарушений права на свободный доступ к информации. Государственная политика направлена на формирование контролируемого информационного пространства, где доминирует официальная точка зрения.

Прогноз развития событий:

- **Нейтральный сценарий (стагнация с элементами дальнейшего ужесточения)**:
    - Сохранение текущего уровня государственного контроля над интернетом с периодическими "закручиваниями гаек" в ответ на внутри- или внешнеполитические события.
    - Продолжение блокировок "нежелательных" ресурсов и VPN-сервисов, но без тотального отключения от глобальной сети.
    - Дальнейшее развитие национальной цифровой инфраструктуры (НСУД, ТСПУ) для повышения эффективности фильтрации и контроля трафика.
    - Продолжение правоприменительной практики по статьям о "фейках" и "дискредитации", но без резкого увеличения масштабов репрессий, если не будет значимых дестабилизирующих факторов.
    - Постепенное "выдавливание" иностранных цифровых платформ и сервисов с российского рынка и их замена национальными аналогами,

находящимися под более плотным контролем государства.
    - Сохранение высокого уровня самоцензуры среди пользователей и СМИ.
- **Положительный сценарий (ослабление регулирования, либерализация)**:
    - Этот сценарий представляется **маловероятным** в текущих политических и геополитических условиях.
    - Теоретически, он мог бы включать:
        - Смягчение или отмену наиболее репрессивных законов (о "фейках", о "неуважении к власти", об "иностранных агентах" в их текущем виде).
        - Сокращение практики внесудебных блокировок, повышение прозрачности процедур ограничения доступа к информации.
        - Прекращение преследования за мирные высказывания в интернете.
        - Снижение давления на независимые СМИ и НКО.
        - Отказ от планов по изоляции Рунета и более открытое взаимодействие с глобальным интернет-сообществом.
    - Для реализации такого сценария необходимы глубокие политические изменения в стране.
- **Отрицательный сценарий (усиление цензуры, "цифровой железный занавес")**:
    - Дальнейшее ужесточение законодательства, расширение оснований для блокировок и уголовного преследования за онлайн-активность.
    - Усиление технических мер по блокировке VPN и других средств обхода цензуры, вплоть до попыток блокировки по протоколам на национальном уровне.
    - Более активное использование технологий искусственного интеллекта для мониторинга и выявления "нежелательного" контента и пользователей.
    - Постепенное или резкое (в случае кризисной ситуации) ограничение доступа к глобальным интернет-сервисам и платформам, вплоть до полной изоляции российского сегмента интернета ("китайский вариант" с национальным файрволом).
    - Усиление требований к идентификации пользователей и сбору данных о их онлайн-активности.
    - Полное подавление независимых онлайн-СМИ и превращение интернета преимущественно в канал распространения государственной пропаганды.
    - Этот сценарий может быть реализован в случае эскалации внутриполитической напряженности, усиления внешнего давления или

принятия стратегического решения о построении полностью автаркичной цифровой экосистемы.

Учитывая текущие тенденции, наиболее вероятным представляется развитие событий по сценарию, близкому к нейтральному, с постоянным риском смещения в сторону отрицательного сценария при изменении внешних или внутренних условий. Состояние цифровых прав в России будет оставаться предметом серьезной озабоченности как для граждан страны, так и для международного сообщества.

Источники

1. Russian Federation | Data, дата последнего обращения: июня 13, 2025, https://data.worldbank.org/country/russian-federation
2. Digital in The Russian Federation — DataReportal – Global Digital ..., дата последнего обращения: июня 13, 2025, https://datareportal.com/digital-in-the-russian-federation
3. Digital 2024: The Russian Federation - DataReportal, дата последнего обращения: июня 13, 2025, https://datareportal.com/reports/digital-2024-russian-federation
4. Digital 2025: The Russian Federation — DataReportal – Global ..., дата последнего обращения: июня 13, 2025, https://datareportal.com/reports/digital-2025-russian-federation
5. Численность населения, дата последнего обращения: июня 13, 2025, https://rosstat.gov.ru/bgd/regl/b11_13/IssWWW.exe/Stg/d1/04-02.htm
6. ВВП России - TAdviser, дата последнего обращения: июня 13, 2025, https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%92%D0%92%D0%9F_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
7. Russia GDP - Trading Economics, дата последнего обращения: июня 13, 2025, https://tradingeconomics.com/russia/gdp
8. Экономика России - Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D0%BA%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
9. Валовой внутренний продукт России — Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%92%D0%B0%D0%BB%D0%BE%D0%B2%D0%BE%D0%B9_%D0%B2%D0%BD%D1%83%D1%82%D1%80%D0%B5%D0%BD%D0%BD%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
10. Архив курсов валют ЦБ РФ, посмотреть курсы валют ... - Myfin.by, дата

последнего обращения: июня 13, 2025, https://myfin.by/currency/cb-rf-archive
11. World Bank confirms forecast for Russia's GDP growth at 1.6% in 2025, 1.1% in 2026, дата последнего обращения: июня 13, 2025, https://interfax.com/newsroom/top-stories/109215/
12. Архив курсов доллара ЦБ РФ, посмотреть курс доллара Центробанка России на выбранную дату - Myfin.by, дата последнего обращения: июня 13, 2025, https://myfin.by/currency/cb-rf-archive/usd
13. ФОРМИРОВАНИЕ ИНСТИТУТА «СУВЕРЕННОГО ИНТЕРНЕТА» В РОССИЙСКОЙ ФЕДЕРАЦИИ Текст научной статьи по специальности «Политологические науки» - КиберЛенинка, дата последнего обращения: июня 13, 2025, https://cyberleninka.ru/article/n/formirovanie-instituta-suverennogo-interneta-v-rossiyskoy-federatsii
14. Закон о «суверенном интернете - Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD_%D0%BE_%C2%AB%D1%81%D1%83%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%BD%D0%BE%D0%BC_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5%C2%BB
15. АКТУАЛЬНЫЕ ПРОБЛЕМЫ РОССИЙСКОЙ ЭКОНОМИКИ - Современная Европа, дата последнего обращения: июня 13, 2025, http://www.sov-europe.ru/images/pdf/2015/3/Kudrov_3-2015.pdf
16. Структурные проблемы экономического роста Российской Федерации Текст научной статьи по специальности «Экономика и бизнес - КиберЛенинка, дата последнего обращения: июня 13, 2025, https://cyberleninka.ru/article/n/strukturnye-problemy-ekonomicheskogo-rosta-rossiyskoy-federatsii
17. Государственный строй России — Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%93%D0%BE%D1%81%D1%83%D0%B4%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D1%81%D1%82%D1%80%D0%BE%D0%B9_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
18. Административно-территориальное деление России - IS MUNI, дата последнего обращения: июня 13, 2025, https://is.muni.cz/el/phil/jaro2017/RJ_67/administrativnoe_delenie_RF.pdf
19. Территориальное деление России - Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D1%80%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
20. 207.3: «Фейки» об армии - Tilda, дата последнего обращения: июня 13, 2025, http://longreads.mr7.tilda.ws/statia_2073

21. Что теперь нельзя писать о Вооруженных Силах РФ и работе госорганов за рубежом?, дата последнего обращения: июня 13, 2025, https://mmdc.ru/blog/2022/03/04/chto-teper-nelzya-pisat-o-vooruzhennyh-silah-rf/
22. .ru — Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/.ru
23. О Координационном центре доменов .RU/.РФ, дата последнего обращения: июня 13, 2025, https://cctld.ru/about/
24. Роскомнадзор - Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D0%BA%D0%BE%D0%BC%D0%BD%D0%B0%D0%B4%D0%B7%D0%BE%D1%80
25. Freedom on the Net 2022: Россия заняла 65 место из 70 в ..., дата последнего обращения: июня 13, 2025, https://roskomsvoboda.org/post/freedom-on-the-net-2022/
26. Успеть за 6 суток : обзор аудитории интернета, дата последнего обращения: июня 13, 2025, https://mediascope.net/upload/iblock/9da/f39jd547adzptf0mu2j1tlmw44pjgt5d/Mediascope_%D0%9D%D0%A0%D0%A4_6%20%D1%81%D1%83%D1%82%D0%BE%D0%BA.pdf
27. Mediascope: месячная аудитория интернета в РФ составляет ..., дата последнего обращения: июня 13, 2025, https://habr.com/ru/news/858782/
28. Internet users for the Russian Federation (ITNETUSERP2RUS) | FRED | St. Louis Fed, дата последнего обращения: июня 13, 2025, https://fred.stlouisfed.org/series/ITNETUSERP2RUS
29. Объем российского рынка ШПД в b2c-сегменте достиг 42,2 млрд рублей в 2 квартале 2024 года | Кабельщик, дата последнего обращения: июня 13, 2025, https://www.cableman.ru/content/obem-rossiiskogo-rynka-shpd-v-b2c-segmente-dostig-422-mlrd-rublei-v-2-kvartale-2024-goda
30. Интернет-доступ (рынок России) - TAdviser, дата последнего обращения: июня 13, 2025, https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF_%28%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8%29
31. Российский телеком-рынок растет благодаря нетелекоммуникационным услугам. Обзор: Телеком 2024 - CNews, дата последнего обращения: июня 13, 2025, https://www.cnews.ru/reviews/telekom_2024/articles/rossijskij_telekom-rynok_rastet
32. Связь в России — Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D1%8F%D0%B7%D1%8C_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8

33. Speedtest Global Index – Internet Speed around the world ..., дата последнего обращения: июня 13, 2025, https://www.speedtest.net/global-index
34. Интернет в России: что говорит статистика? | Эксперты объясняют от Роскачества, дата последнего обращения: июня 13, 2025, https://rskrf.ru/tips/eksperty-obyasnyayut/internet-stats/
35. России обещан рост скорости интернета в 100 раз - CNews, дата последнего обращения: июня 13, 2025, https://www.cnews.ru/news/top/2024-03-06_rossii_predrekli_100-kratnyj
36. Ookla обновила рейтинг по скорости мобильного и широкополосного интернета, дата последнего обращения: июня 13, 2025, https://timeweb.com/ru/community/articles/ookla-obnovili-reyting-po-skorosti-mobilnogo-i-shirokopolosnogo-interneta
37. Focus on Russia - RIPE NCC Statistics and Data, дата последнего обращения: июня 13, 2025, https://labs.ripe.net/author/fergalc/focus-on-russia-ripe-ncc-statistics-and-data/
38. дата последнего обращения: января 1, 1970, https://stat.ripe.net/country/RU#tabId=routing
39. IPv6 Adoption - Google, дата последнего обращения: июня 13, 2025, https://www.google.com/intl/en/ipv6/
40. Почему IPv6 быстрее и как его внедрить. Кейс X-COM - VAS Experts, дата последнего обращения: июня 13, 2025, https://vasexperts.ru/blog/ipv4-i-ipv6/pochemu-ipv6-bystree-i-kak-ego-vnedrit-kejs-x-com/
41. IPv6 Adoption Statistics: a Comparison of Different Metrics - RIPE Labs, дата последнего обращения: июня 13, 2025, https://labs.ripe.net/author/wilhelm/ipv6-adoption-statistics-a-comparison-of-different-metrics/
42. IPv6 Users by Country - APNIC Labs, дата последнего обращения: июня 13, 2025, https://labs.apnic.net/dists/v6dcc.html
43. IPv6 Capability Metrics - APNIC Labs Measurements, дата последнего обращения: июня 13, 2025, https://stats.labs.apnic.net/ipv6/RU
44. Russia surpasses the USA in IPv6 adoption (60% vs. 48%) - Reddit, дата последнего обращения: июня 13, 2025, https://www.reddit.com/r/ipv6/comments/1ggash9/russia_surpasses_the_usa_in_ipv6_adoption_60_vs_48/
45. Управление интернетом - Координационный центр доменов, дата последнего обращения: июня 13, 2025, https://cctld.ru/help/wiki/upravlenie-internetom/
46. Липов, Андрей Юрьевич - Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%9B%D0%B8%D0%BF%D0%BE%D0%B2,_%D0%90%D0%BD%D0%B4%D1%80%D0%B5%D0%B9_%D0%AE%D1%80%D1%8C%D0%B5%D0%B2%D0%B8%D1%87

47. Структура - Роскомнадзор, дата последнего обращения: июня 13, 2025, https://rkn.gov.ru/about/structure/
48. Россия: Нарастающая изоляция, контроль и цензура в интернете | Human Rights Watch, дата последнего обращения: июня 13, 2025, https://www.hrw.org/ru/news/2020/06/18/russia-growing-internet-isolation-control-censorship
49. Единый реестр запрещённых сайтов — Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%95%D0%B4%D0%B8%D0%BD%D1%8B%D0%B9_%D1%80%D0%B5%D0%B5%D1%81%D1%82%D1%80_%D0%B7%D0%B0%D0%BF%D1%80%D0%B5%D1%89%D1%91%D0%BD%D0%BD%D1%8B%D1%85_%D1%81%D0%B0%D0%B9%D1%82%D0%BE%D0%B2
50. Роскомсвобода - Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D0%BA%D0%BE%D0%BC%D1%81%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0
51. «Роскомсвобода»: в реестр заблокированных сайтов за неделю внесли почти 15 тысяч ресурсов — Meduza, дата последнего обращения: июня 13, 2025, https://meduza.io/news/2022/12/12/roskomsvoboda-v-reestr-zablokirovannyh-saytov-za-nedelyu-vnesli-pochti-15-tysyach-resursov
52. Роскомнадзор | Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммун.. 2025 | ВКонтакте, дата последнего обращения: июня 13, 2025, https://vk.com/rkn
53. Censorship Chronicles: The systematic suppression of independent ..., дата последнего обращения: июня 13, 2025, https://ooni.org/post/2024-russia-report/
54. OONI | Open Observatory of Network Interference | Censorship | Internet | Websites | Apps - Digital Rights Community, дата последнего обращения: июня 13, 2025, https://www.digitalrights.community/blog/community-series-ooni
55. Свобода слова в России. Совместный доклад для 4 цикла Универсального периодического обзора ООН | ОВД-Инфо, дата последнего обращения: июня 13, 2025, https://reports.ovd.info/svoboda-slova-v-rossii
56. Журналистку Марию Пономаренко осудили на год и 10 месяцев колонии, дата последнего обращения: июня 13, 2025, https://www.svoboda.org/a/zhurnalistku-mariyu-ponomarenko-osudili-na-god-i-10-mesyatsev-kolonii/33361563.html
57. Журналистке Пономаренко из Барнаула увеличили срок за нападение на сотрудника ФСИН - Интерфакс, дата последнего обращения: июня 13, 2025, https://www.interfax.ru/russia/1016904
58. Илью Яшина приговорили к 8,5 годам по делу о "военных фейках ..., дата последнего обращения: июня 13, 2025, https://www.bbc.com/russian/news-63864402
59. Суд признал Яшина виновным по делу о «фейках» про армию | Forbes.ru, дата последнего обращения: июня 13, 2025,

https://www.forbes.ru/society/482143-sud-priznal-asina-vinovnym-po-delu-o-fejkah-pro-armiu
60. 2022 Country Reports on Human Rights Practices: Russia - State Department, дата последнего обращения: июня 13, 2025, https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/russia/
61. Роскомсвобода, дата последнего обращения: июня 13, 2025, https://roskomsvoboda.org/about/
62. Agora (organization) - Wikipedia, дата последнего обращения: июня 13, 2025, https://en.wikipedia.org/wiki/Agora_(organization)
63. Агора (организация) - Википедия, дата последнего обращения: июня 13, 2025, https://ru.wikipedia.org/wiki/%D0%90%D0%B3%D0%BE%D1%80%D0%B0_(%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F)
64. Запрет на использование и рекламу VPN: миф или реальность? - FirstVDS, дата последнего обращения: июня 13, 2025, https://firstvds.ru/blog/zapret-na-ispolzovanie-i-reklamu-vpn-mif-ili-realnost
65. Запрет VPN в России: законы и их практическое применение | Блог АдминВПС, дата последнего обращения: июня 13, 2025, https://adminvps.ru/blog/vpn-v-rossii-zaprety-i-ih-prakticheskoe-primenenie/
66. Хронология блокировок VPN в России 2019-2024. Куда мы ... - Habr, дата последнего обращения: июня 13, 2025, https://habr.com/ru/companies/amnezia/articles/861198/
67. Использующим VPN компаниям советуют отказаться от иностранных протоколов шифрования - Интерфакс, дата последнего обращения: июня 13, 2025, https://www.interfax.ru/russia/1020310
68. После замедления YouTube число пользователей VPN в России достигло 36%, дата последнего обращения: июня 13, 2025, https://www.agents.media/posle-zamedleniya-youtube-chislo-polzovatelej-vpn-v-rossii-dostiglo-36/
69. Количество пользователей VPN в России выросло почти на 40 ..., дата последнего обращения: июня 13, 2025, https://www.forbes.ru/tekhnologii/501873-kolicestvo-pol-zovatelej-vpn-v-rossii-vyroslo-pocti-na-40-v-2023-godu
70. ЧИСЛЕННОСТЬ НАСЕЛЕНИЯ, дата последнего обращения: июня 13, 2025, https://rosstat.gov.ru/bgd/regl/b05_13/IssWWW.exe/Stg/04-02.htm
71. World Development Indicators | DataBank, дата последнего обращения: июня 13, 2025, https://databank.worldbank.org/data/reports.aspx?source=2&country=RUS
72. Государственный строй России: структура, органы власти - Российское общество Знание, дата последнего обращения: июня 13, 2025, https://znanierussia.ru/articles/%D0%93%D0%BE%D1%81%D1%83%D0%B4%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D

0%B9_%D1%81%D1%82%D1%80%D0%BE%D0%B9_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
73. Правительство России официальный сайт, дата последнего обращения: июня 13, 2025, http://government.ru/