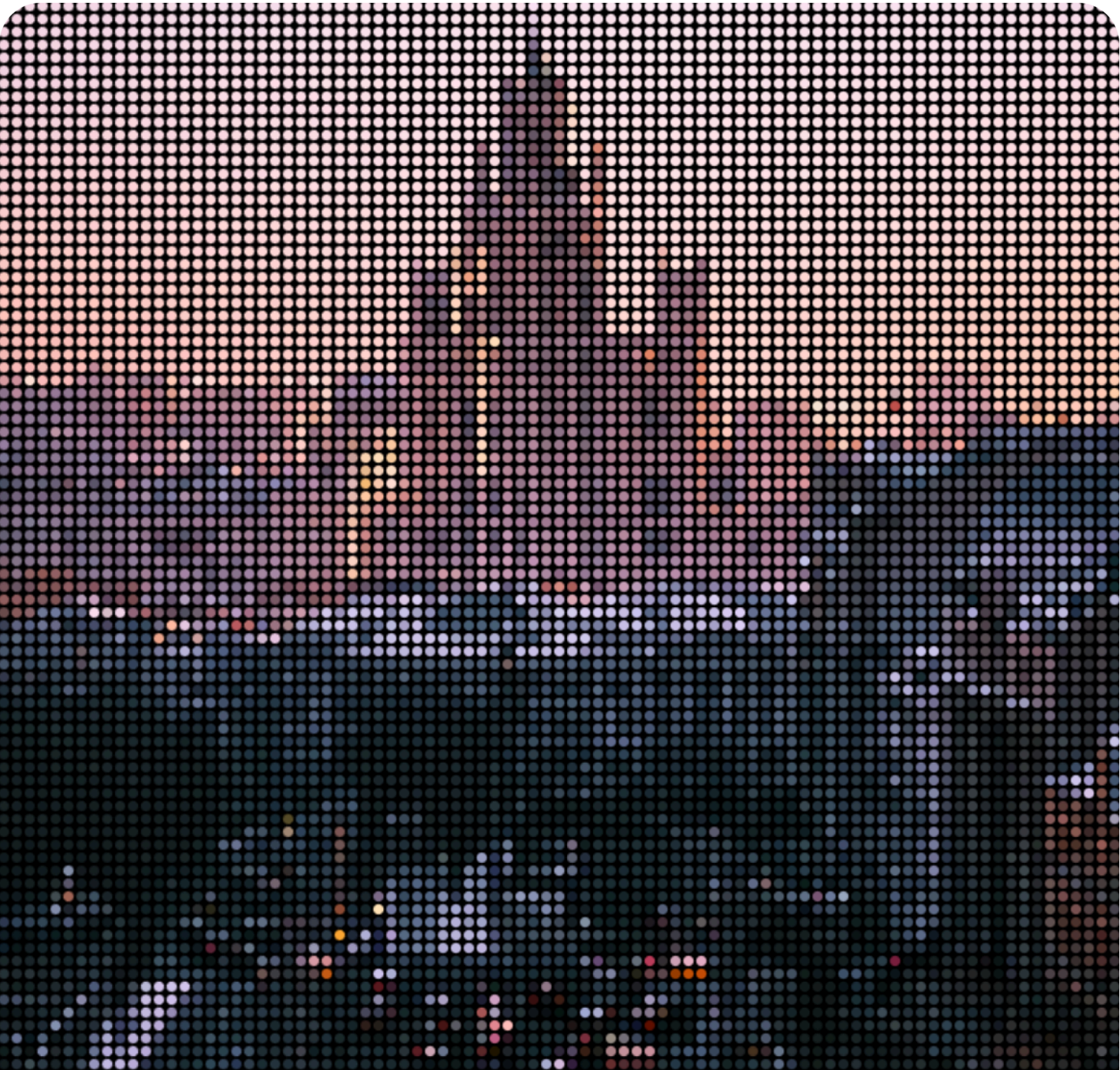
RKS Global

Июнь 2026 · rks.global

Рунет 2025: суверенизация и деградация

Обзор интернет-цензуры в России в 2025-м году



Содержание

1. Рунет 2025. Смена модели интернет-контроля

Работа цензурных ведомств в России в 2025 качественно изменилась. Если раньше Роскомнадзор заносил сайты, технические домены приложений и других сервисов в свой реестр и заставлял интернет-провайдеров их блокировать, то теперь ведомство управляет блокировками на архитектурном уровне.

Акцент цензуры сместился с «противоправного» контента на транспортный и сетевой уровень: протоколы, типы трафика, мобильный доступ и инфраструктурные узлы. А с началом шатдаунов был затронут уровень связанности. Интернет в России уже чаще работает не по принципу «разрешено или запрещено», а по принципу «работает частично, нестабильно или выборочно».

На протяжении предыдущего десятилетия система регулирования строилась вокруг реестров запрещённых сайтов и расширения полномочий регулятора. В реестры добавлялись домены и IP-адреса, блокировались конкретные сервисы, ограничивались отдельные приложения. Законы о блокировках, о «суверенном интернете», о приземлении иностранных IT-компаний создали для этого нормативную базу, а ТСПУ с DPI[1] позволили нарастить технические возможности блокировок. Но в 2024 году ситуация изменилась.

В марте 2024 вступил в силу запрет на «популяризацию» средств обхода блокировок. В 2025 году сайты и отдельные интернет-страницы с информацией о способах обхода блокировок продолжили активно блокировать, а также был принят закон о штрафах за рекламу VPN. К концу года список материалов, заблокированных Роскомнадзором по причине «пропаганды» обхода цензуры, насчитывал около 3000 источников.

[1] ТСПУ — технические средства противодействия угрозам, устройства, которые стоят у интернет-провайдеров и фильтруют интернет-трафик по спускаемым «сверху» инструкциями. DPI — deep packet inspection, технология, которую цензор использует для обнаружения и блокировки VPN и других средств обхода блокировок.

Массовые блокировки популярных VPN-протоколов через ТСПУ (OpenVPN, WireGuard, Shadowsocks) в 2025 году тоже продолжились, но более избирательными методами — в частности, active probing.[2]

То есть, объектом регулирования стали не конкретные сайты, а способы соединения. Не ресурсы, а типы трафика.

Это подтверждают ограничения UDP-трафика (видеостриминги, онлайн-игры) в условиях, когда сами платформы еще оставались доступны, проблемы со звонками в мессенджерах еще до блокировки самих мессенджеров, попытки фильтрации продвинутых VPN-протоколов вроде VLESS с Reality.

В 2025 году в практику вошли региональные шатдауны мобильного интернета. Они стали применяться как рутинная, а не чрезвычайная мера. Официальной причиной называли борьбу с беспилотниками, но отключения мобильного интернета охватывали не только приграничные регионы, но и территории в Сибири и на Дальнем востоке.

Активно тестировалась модель «белых списков», когда стабильно функционировал только ограниченный круг одобренных властями сервисов, а остальные работали нестабильно или не работали вовсе, причем без какого-либо официального запрета. В отдельных случаях это превращалось в «серые списки», когда некоторые не запрещенные сервисы работали как обычно, другие работали с перебоями, третьи не работали.

Одновременно под удар попадал инфраструктурный слой. Это CDN-провайдеры, DNS-сервисы, облачные платформы и системы защиты от DDoS-атак. Воздействие на такие узлы позволяет влиять сразу на тысячи ресурсов, а не осуществлять точечные запреты и блокировки. Резонансный пример такой практики — блокировка Cloudflare, компании, на которой завязана серверная экосистема миллионов сайтов. Тогда у россиян перестали работать не только VPN-сервисы, но и сайты «Ростелекома», «Билайна», Twitch, Miro, SoundCloud, Aviasales и тд — как с блокировкой Telegram в 2018 году. Роскомнадзор отрицал целенаправленное ограничение.

[2]Active probing, или активное зондирование — способ обнаружения VPN-сервисов. Цензор отправляет запрос адресам или серверам, которые считает подозрительными, и смотрит, как те отвечают. У VPN характерный «почерк» ответа, на основании чего этот адрес блокируется.

Теперь, когда власти воспринимают интернет как угрозу собственной безопасности, сопутствующий ущерб их волнует мало.

Ещё одно направление цензуры 2025 года — превращение телекоммуникаций в инструмент контроля доступа через ужесточение верификации SIM-карт, ограничения роуминга, усложнение получения виртуальных номеров. Пристальный контроль за SIM-картами параллельно стал частью и другого процесса — постепенного отъема у россиян права на приватность и анонимность. Но официальной причиной стала борьба с мошенничеством.

В конце 2024 Минцифры внесло изменения в закон «О связи» и обязало иностранных граждан связать свои симки с биометрическими данными. А с 1 июля 2025 года начало отключать связь у не выполнивших требование абонентов.

Для граждан РФ ситуация была не лучше: в апреле 2025 вступил в силу порядок проверки достоверности сведений об абонентах-физлицах, а к ноябрю пользователей обязали завершить процедуру предоставления персональных данных операторам связи и ограничить количество зарегистрированных на одно физлицо SIM-карт двадцатью. Появилась и процедура «охлаждения» SIM-карт после их неиспользования в течение 72 часов или возвращения абонента из-за границы. Официальная причина — борьба с дронами.

Статья КоАП РФ 13.29.1 закрепила наказание абонента за передачу его номера третьему лицу и установила штрафы от 30 до 50 тысяч рублей для физических лиц, до 100 тысяч для ИП и до 200 — для юрлиц.

В 2025 году усилилось давление на глобальные платформы. Как и в 2024 году, российские власти отправляли им запросы на удаление VPN-приложений и приложений независимых СМИ из сторов. Одновременно с этим цензоры успешно блокировали популярные мессенджеры и занимались продвижением импортозамещающих российских аналогов.

Для модели цензуры это значимый поворот: появляется порядок, при котором интернет перестаёт быть постоянно доступным благом и становится опцией, которую можно включать и отключать по решению «сверху».

В 2025 году изменилась не только практика ограничений, но и то, как это преподносится обществу. Чиновники всё реже говорят о запретах и блокировках как

таковых, и всё чаще описывают происходящее как меры защиты: от мошенников, «экстремизма», военных угроз или «опасного контента» для детей.

В частности, блокировки, замедления и региональные шатдауны называются временными ограничениями в связи с обеспечением безопасности. Использование VPN и других инструментов обхода де-факто переводятся в зону подозрительной и даже криминальной активности, а значит, по логике властей, должно строго регулироваться или запрещаться. В дополнение к этому, сбои фильтрующего оборудования тоже вносят свою лепту в общее ощущение деградации интернета в России.

В 2025-м году цензоры перестали искать юридические обоснования блокировок, из которых следует, что ограничения происходят, так как сайты и сервисы якобы нарушают российские законы. Вместо этого власти начали использовать клишированные формулировки о необходимости обеспечения безопасности граждан.

Все эти процессы позволяют говорить о новой стадии цензуры в России. Её теперь определяют не количество блокировок, а изменение характера вмешательства:

- на смену полной блокировке всё чаще приходит управляемая деградация (ухудшение качества передачи данных);
- фильтрация распространяется на типы трафика и протоколы, а не только конкретные интернет-ресурсы;
- доступ к интернету перестал быть одинаковым по всей стране и стал зависеть от региона и текущего «режима» на сетях операторов: одни и те же сервисы и функции могут работать в одном субъекте РФ и одновременно быть недоступными в другом;
- доступ пользователя к связи теперь может ограничиваться и на телекоммуникационном уровне (через SIM-карты).
- В 2024 году эксперты RKS Global делали прогнозы относительно того, как будет развиваться цензура в России. Среди вероятных сценариев были:
- применение статистических методов блокировок,
- запрет популярных международных сервисов и продвижение отечественных аналогов,
- введение «белых списков»,
- обход блокировок в условиях ужесточающейся цензуры будет возможен благодаря инструментам, которые умеют маскироваться под безобидные сервисы и ускользать от DPI.

2025 год оправдал худшие ожидания экспертов RKS Global. WhatsApp и Telegram были заблокированы на фоне навязывания национального мессенджера MAX, в регионах начался переход к «белым спискам», а VPN-сервисы без функций маскировки трафика под HTTPS и раздельного туннелирования почти перестали работать. Но, несмотря на ужесточение цензурного законодательства и применения новых методов блокировок (как статистические методы, когда трафик объявляется подозрительным, если в большом объеме направляется на неизвестный ресурс), VPN-сервисы с функцией маскировки всё ещё показывали себя хорошо.

2. ТСПУ и DPI

К 2025 году технологическая инфраструктура цензуры в РФ окончательно превратилась в самостоятельный контур управления связностью.

Как это работает

Главный компонент этой инфраструктуры — система ТСПУ, позволяющая властям полностью контролировать интернет внутри страны. Эта система представляет собой специализированный программно-аппаратный комплекс, который все провайдеры интернета обязаны установить на своих сетях.

ТСПУ не завязаны на реестре Роскомнадзора: независимо от них они блокируют отдельные интернет-ресурсы, неподконтрольные властям хостинги, протоколы VPN и др. Интернет-провайдеры и операторы связи не могут влиять на работу ТСПУ.

Система умеет также замедлять трафик или полностью отключать интернет в отдельных регионах. К тому же, при желании это можно выдать за технические проблемы, а не полноценное решение о запрете.

Инфраструктура ТСПУ к 2025 году была уже сформирована. Эксперты говорят о почти полном покрытии ключевых узлов связи, включая узлы широкополосного доступа (инфраструктурные точки, через которые абоненты подключаются к сети оператора), мобильной сети, трансграничные узлы, вплоть до спутниковых операторов. Нормативная база была обеспечена годом ранее.

В январе 2026 года стало известно, что подведомственный Роскомнадзору орган, ГРЧЦ, имеет KPI к 2030 году фильтровать 98% российского интернет-трафика и блокировать 92% VPN-соединений. После публикации новостей об этом в СМИ, документы исчезли с сайта Роскомнадзора.

По информации источников издания РБК, в декабре 2025 года Роскомнадзор обновил настройки ТСПУ, что привело к существенным нарушениям в работе VPN-сервисов. В частности, начались блокировки трёх протоколов: SOCKS5, VLESS и L2TP. Протокол VLESS оставляет минимум технических следов, и ранее цензор не мог его обнаружить. Но в декабре стало очевидно, что ТСПУ научились выявлять его по косвенным признакам.

Ответственность операторов связи

В конце 2025 года были приняты поправки в КоАП РФ, ужесточающие ответственность для операторов связи. Они касаются правил работы в интернете, проверки данных абонентов и взаимодействия с контролирующими органами. Большинство из нововведений вступило в силу 1 января 2026 года, и уже через несколько дней Роскомнадзор заявил, что обнаружил 35 случаев нарушений установки ТСПУ.

Так, в декабре 2025 года Центр мониторинга и управления сетью связи общего пользования провел мониторинг прохождения трафика через ТСПУ сети «Тинко». Провайдер не обеспечил пропуск трафика на присоединённую сеть связи через ТСПУ, и у него был доступен YouTube. На провайдера составили протокол об административном правонарушении и назначили штраф в 250 тыс. рублей.

В апреле 2026 года стало известно об иных штрафах операторам связи, которые нарушили правила установки и использования ТСПУ. По сообщениям СМИ, суды назначили штрафы на общую сумму 4 млн рублей по 15 фактам нарушений, а ещё по пяти — вынесли предупреждения.

Технологическая инфраструктура цензуры в 2025 объединяет два контура:

1. Инфраструктура DPI/ТСПУ даёт возможность блокировать сайты и сервисы не только по списку запрещённых адресов, но и вмешиваться в само соединение: фильтровать, замедлять или обрывать трафик по его признакам и поведению. Из-за этого ограничения выглядят как нестабильность или деградация отдельных функций, а не как формальная блокировка.

2. Воздействие на один слой инфраструктуры масштабируется сразу на тысячи ресурсов за счет воздействия на крупнейшие узлы экосистемы (как Cloudflare).

3. Реестровые блокировки

Несмотря на эволюцию ТСПУ, государство продолжает наращивать и реестровые блокировки. Уполномоченные ведомства и суды выносят постановление о признании информации запрещенной, Роскомнадзор добавляет сайт или страницу в специальный реестр, согласно которому интернет-провайдеры должны запретить к нему доступ.

Черный список Роскомнадзора

Роскомнадзор отчитался об ограничении доступа к 1 289 000 материалам в 2025 году — это на 59% больше, чем в 2024. Речь именно о единицах контента, а не отдельных сайтах и доменах. Блокировки материалов, связанных с VPN, выросли до 93 000 (рост на 1235%), «ЛГБТ-контент» — 170,3 тыс. (рост на 269%).

В рамках «противодействия угрозам устойчивости, безопасности и целостности Рунета» в 2025 году также заблокировали 252 анонимных почтовых сервиса (на 20% больше, чем годом ранее), 173 приложения (+28%), 410 центров распространения вредоносного программного обеспечения, более 1,2 млн ресурсов (+50%) и 119 тыс. фишинговых сайтов (+441%).

Почти 13 лет вплоть до октября 2025 года работал сервис общественного мониторинга реестра запрещённых сайтов «Роскомсвободы», который также включал в себя реестр блогеров и организаторов распространения информации. После приостановки деятельности организации, появился новый реестр, агрегирующий данные по блокировкам - blockedin.org.

На основе данных двух проектов, эксперты посчитали, что за 2025 год в реестр Роскомнадзора было внесено 570 439 страниц и сайтов (из них разблокировано около 46 тысяч). Общее количество блокировок за всё время наблюдения - 1,7 млн.

Блокировки по мотивам военной цензуры

«Роскомсвобода» фиксировала, что уже в августе 2025 по мотивам военной цензуры (блокировок, инициатором которых выступал «неуказанный госорган», под именем которого, вероятно, теперь и скрывается Генпрокуратура) в реестре оказалось около 25 тыс. записей. По данным экспертов, изучающих реестр запрещенных сайтов, к весне 2026 года число сайтов и ссылок, заблокированных под предлогом борьбы с «дискредитацией» и «фейками» об армии перевалило за 30 тысяч.

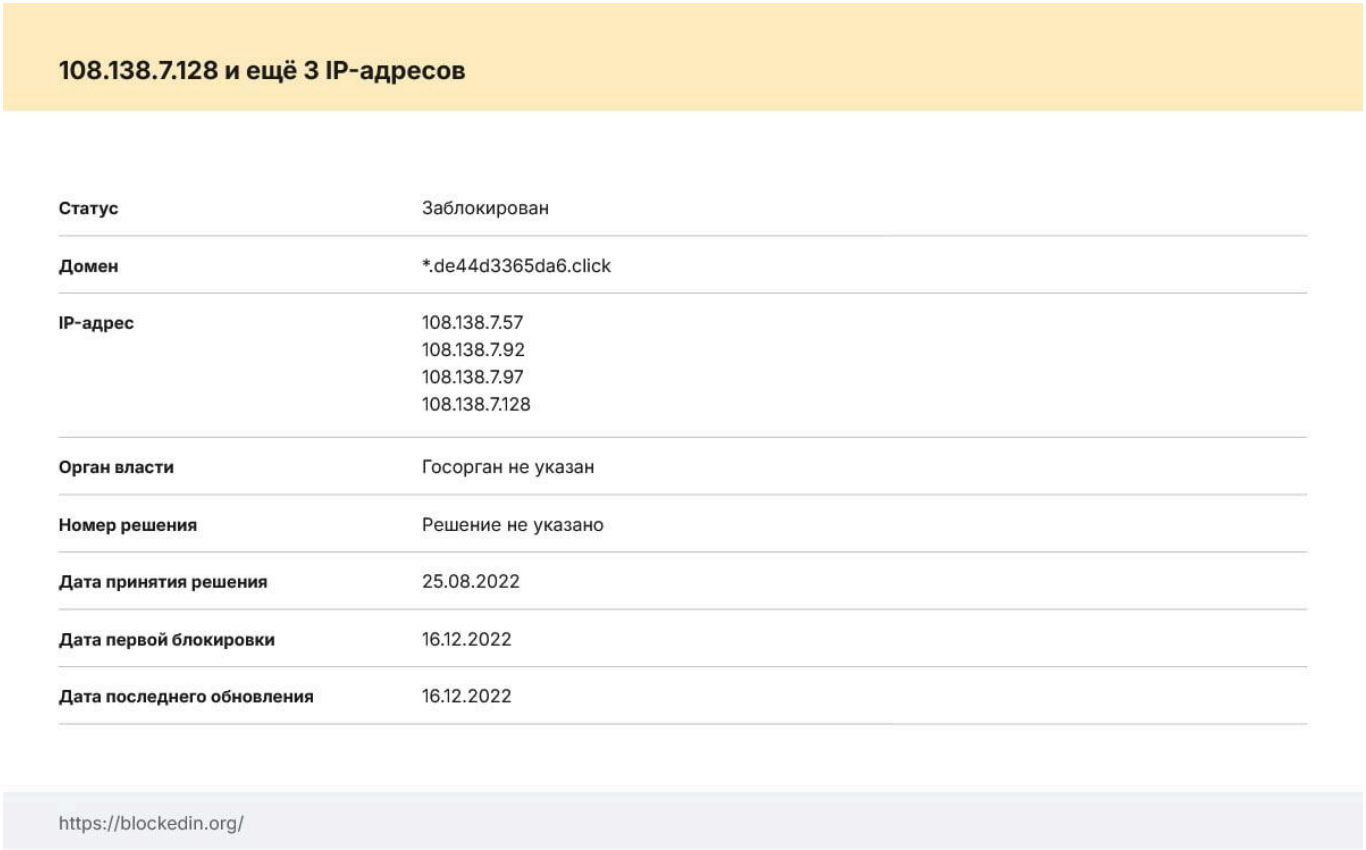
Военная цензура в России началась с 24 февраля 2022 года. Уже в первые дни Генеральная прокуратура начала выносить решения о блокировках, которые сразу приобрели массовый характер. За короткий период под запрет попали Facebook и его мессенджер, Instagram, Twitter, BBC, «Голос Америки», DW, студенческий журнал DOXA, расследовательский Bellingcat, «Кавказский узел», TJ, масса украинских изданий — УНИАН, ТСН, «Зеркало недели», «24 канал», «Громадське»,

— а также государственные сайты Украины, в том числе Министерства здравоохранения и антикоррупционного бюро НАБУ.

В последующие дни и недели список пополнялся лавинообразно: «Медуза», «Медиазона», «Эхо Москвы» и телеканал «Дождь», Republic, The Village, «Бумага», «Радио Свобода», Colta.ru, Amnesty International, «Голос», «7×7», Instagram, «Евроньюс», The New Times, независимая белорусская телестанция «Белсат» и многие другие.

Некоторые решения ведомства постепенно расширялись, так что если в конце февраля-начале марта они насчитывали десятки, то к апрелю счёт по одному только решению мог идти на несколько сотен сайтов.

Формальная законодательная основа для военной цензуры была создана уже после. Законы о «дискредитации» армии и о «фейках» о ней наделили Генпрокуратуру расширенными полномочиями блокировать ресурсы без суда. Позднее инициатором всё большего числа блокировок стал так называемый «неуказанный госорган». Именно этот «неуказанный госорган» сегодня является главным цензором материалов, где отражена информация отличная от официальной позиции российских властей о «специальной военной операции».



Блокировка одного из зеркал True Story

Напомним, что в июле 2022 года количество сайтов и ссылок, подвергшихся военной цензуре, превысило 5 000, в феврале 2023 их стало 10 000, в ноябре того же года - больше 15 000, летом 2024 года - 20 000, летом 2025 года - 25 000.

На конец 2025 - начало 2026 года количество блокировок по мотивам военной цензуры насчитывает более 30 000.

Так в 2025 году по мотивам военной цензуры был заблокирован официальный сайт футбольного клуба «Динамо» (Киев). Среди прочего блокируются песни Noize MC и певицы Монеточки. Причём зачастую из-за блокировок по HTTPS доступ теряется не к одной странице с «запрещенным контентом», а ко всему сайту целиком. Так произошло с блокировкой материала испанского спортивного издания Marca, где разоблачался фейк о Владимире Путине.

Блокировка информации об обходе цензуры

По данным экспертов количество материалов в реестре, заблокированных за информацию об обходе блокировок к началу 2026 года приблизилось к 3000. Это не только ресурсы самих VPN-сервисов, но и инструкции, зеркала, страницы документации, обзоры и любые материалы об обходе цензуры.

С марта 2024 года Роскомнадзор может самостоятельно, без решения суда блокировать любые ресурсы с информацией о способах обхода интернет-цензуры. Возможно, одним из поводов для принятия такого закона стал массовый рост использования VPN, прокси-сервисов и других антицензурных инструментов после волны блокировок 2022 года, когда россияне оказались отрезаны от Facebook, Instagram, Twitter, десятков независимых СМИ, и быстро освоили инструменты для восстановления доступа к заблокированному контенту.

Уже с первых дней действия закона Роскомнадзор начал массово вносить ресурсы с информацией об обходе блокировок в реестр. В промежуток с 1 по 6 марта 2024 года было заблокировано 1700 сайтов и ссылок. Характерная черта этих блокировок — использование так называемых «резиновых» решений: на основании одного и того же решения Роскомнадзора, принятого ещё в марте 2024 года, в реестр продолжают добавлять всё новые ссылки.

В первую очередь под удар попадают сайты VPN-сервисов и их зеркала. В реестре оказались Express VPN, Tesla VPN, Pingle VPN, Gen VPN, Happ VPN, «Дед VPN»,

Octohide VPN, PaperVPN, Amnezia VPN. Блокируются не только сами VPN-сервисы, но и любые упоминания о них.

В 2025 под запрет попал сайт «Гильдии VPN». В числе заблокированных оказался сайт по продаже роутера Deeper Connect со встроенным VPN. Под запрет попал и сервис «Юбуст» для ускорения YouTube, причём охота долгое время велась за всеми вариациями написания его домена. Заблокирована страница на игровой платформе Fandom с информацией об обходе блокировок. Заблокировано зеркало AdGuard VPN (и не только его) на серверах Amazonaws. Попали под блокировку ссылки с информацией о протоколе VLESS и ядре XRay.

Блокируются также сервисы, которые лишь косвенно связаны с темой: например, ссылки с инструкциями по восстановлению доступа к Facebook и Instagram, опубликованные на совершенно посторонних сайтах. Развлекательный портал Pikabu регулярно вынужден удалять контент о средствах обхода цензуры, чтобы самому не оказаться в реестре. За 2025 год сервис получил почти 30 запросов от властей на удаление «инструкций по обходу блокировок».

4. От IP-блокировок к протокольному контролю

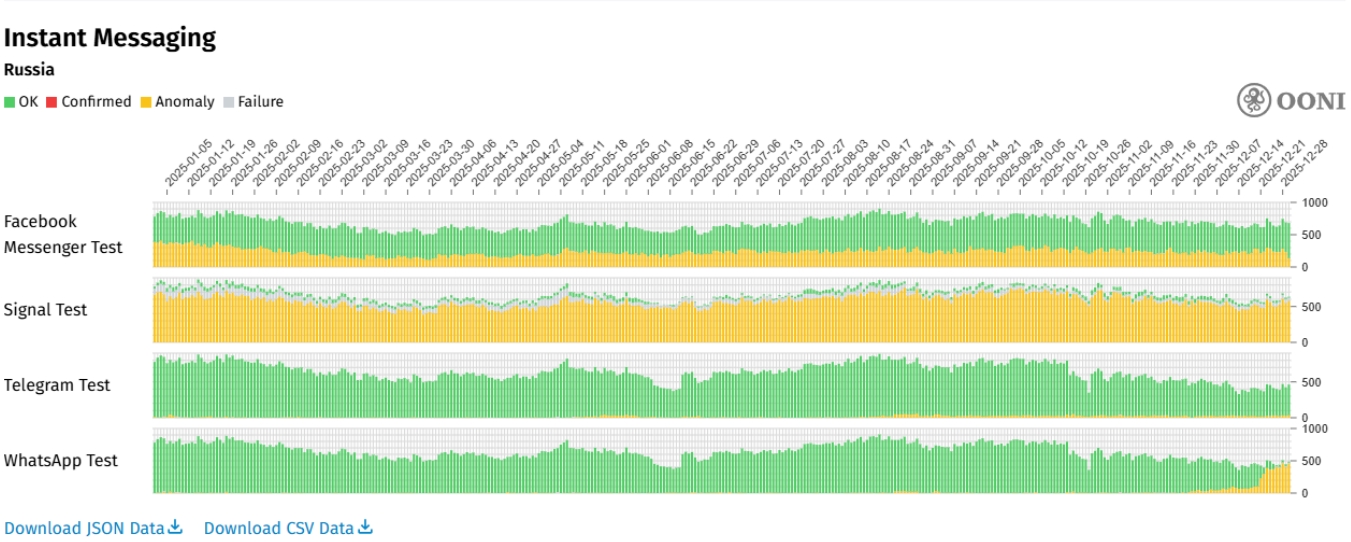
Кроме блокировки конкретных IP-адресов и доменов, стали чаще блокироваться протоколы и определенные типы трафика. То есть, цензурное вмешательство затрагивает сам способ соединения. Для пользователя это проявляется не как недоступность конкретного сайта, а как нестабильная работа определённых функций. Например, голосовых звонков в мессенджерах, некоторых VPN-сервисов и сервисов, использующих протокол передачи данных под названием User Datagram Protocol (UDP).

В течение года фиксировались многочисленные сообщения о сбоях VPN на базе WireGuard-подобных протоколов, проблемах с игровыми сервисами и VoIP-звонками. Такие ошибки возникают, когда цензор довольно грубым образом фильтрует или ограничивает UDP, но TCP (Transmission Control Protocol) при этом сохраняет работоспособность. UDP в целом чувствительнее TCP: он используется

для передачи медиаданных в режиме прямого времени, и властям нетрудно нарушить плотный ровный медиапоток.

Характерным примером протокольного вмешательства стала деградация VoIP и звонков в мессенджерах. Пользователи сообщали о сбоях при голосовых вызовах в Telegram и WhatsApp, хотя текстовые сообщения доходили.

В августе 2025 Роскомнадзор официально подтвердил «частичное ограничение» звонков в Telegram и WhatsApp, при этом в публичной формулировке подчёркивалось, что «никаких иных ограничений функциональности» не вводится. Вскоре последовали сообщения о проблемах и в других VoIP-сервисах, устроенных похожим образом (видеоконференции и звонки). «Роскомсвобода» фиксировала жалобы на сбои Google Meet в России при отсутствии глобального сбоя у Google, а Роскомнадзор публично отрицал, что принимал ограничительные меры.



Тестирование доступности мессенджеров в 2025 году. Данные ooni.org.

5. Блокировки глобальных сервисов и продвижение локальных аналогов

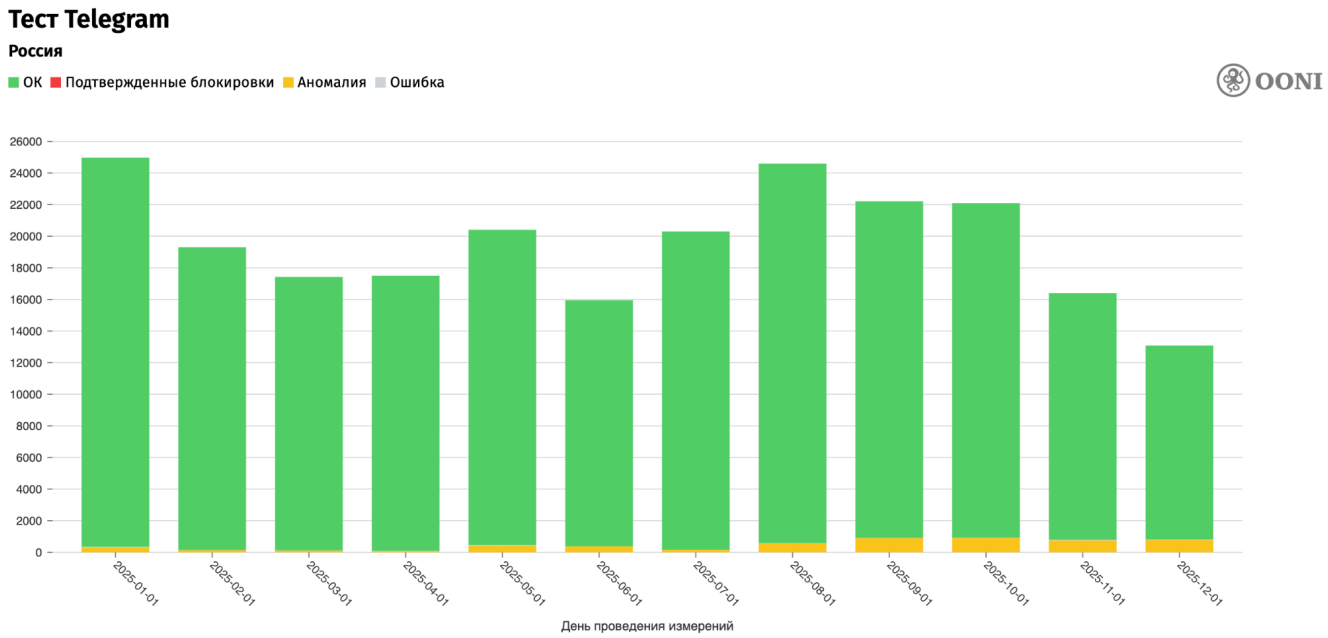
Динамику 2025 года в блокировках глобальных сервисов лучше всего видно на примере войны с популярными мессенджерами и сервисами общения. Если в 2024 году под блокировки попали ограниченно распространенные сервисы, такие как Viber, Discord, Signal, Session, SimpleX Chat, то в 2025 году власти взялись за самые востребованные. На фоне давления на глобальные сервисы импортозамещение перестало быть только громким лозунгом и превратилось в реальную ограничительную меру.

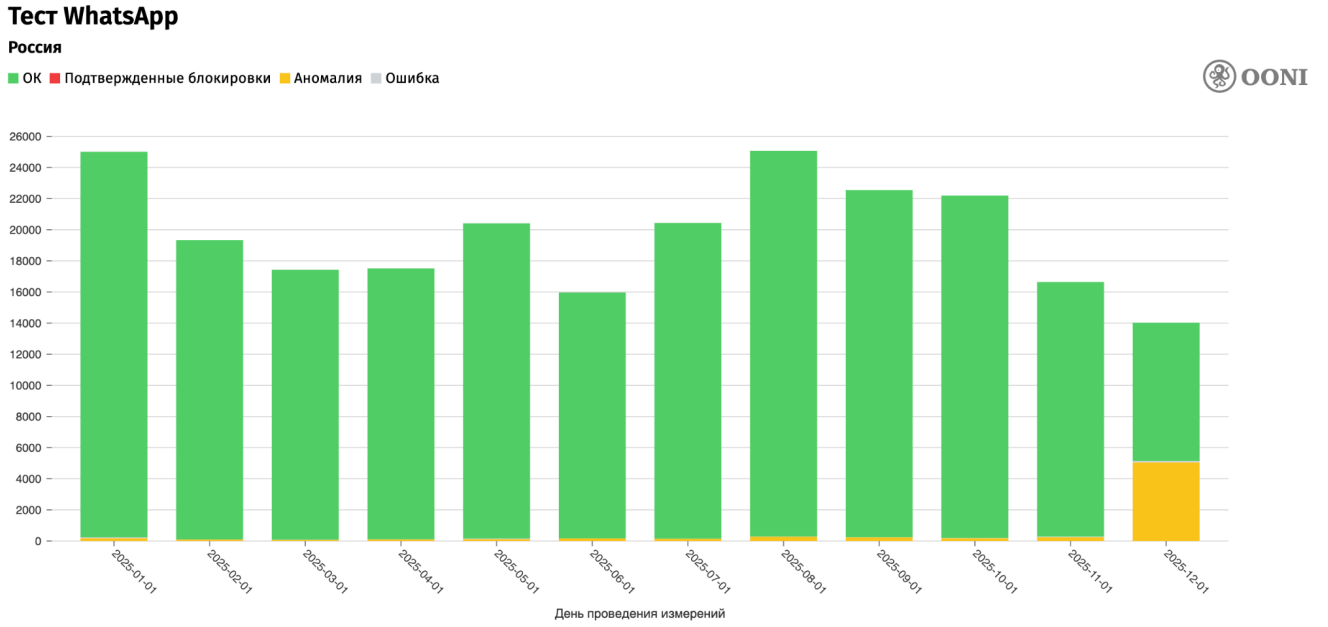
Контроль общения

В августе 2025 года Роскомнадзор объявил, что будет вводить «постепенные ограничения для сервисов, которые систематически игнорируют российское законодательство, с возможностью их снятия в случае устранения нарушений». Речь шла о требованиях по размещению серверов на территории России, обеспечению защиты персональных данных, защите граждан от мошенничества и созданию условий для пресечения экстремизма и терроризма. Требования по защите от мошенничества и созданию условий для пресечения экстремизма не имеют количественного измерения: РКН сам решает, насколько хорошо сервисы с этим справляются.

С того же августа власти начали ограничивать голосовые и видеозвонки в двух самых популярных в России мессенджерах — WhatsApp и Telegram. Роскомнадзор заявлял, что ограничения были наложены «в целях противодействия преступникам». Telegram якобы «системно создавал» инфраструктуру «пробива» личных данных россиян, хотя на самом деле мессенджер регулярно удалял боты пробива.

По сведениям некоторых СМИ, еще весной 2025 года российские операторы связи выступали с инициативой заблокировать звонки в зарубежных мессенджерах. Компании открыто объяснили это тем, что им нужны дополнительные доходы для поддержания инфраструктуры.





Измерения работы Telegram и WhatsApp в России в 2025 году (наличие аномалий свидетельствует о потенциальных блокировках, когда нет точных сигналов, таких как страница блокировки)

Давление на геймеров

Параллельно с мессенджерами внимание цензоров привлекли глобальные игровые платформы. Весной 2025 на фоне проблем с доступом к ресурсам за Cloudflare поступали жалобы на работу игровых сервисов и разработчиков игр (Steam, Ubisoft, EpicGames), стримингговой платформы Twitch, игры Genshin Impact и платформы для общения геймеров Discord.

Пострадала и UGC-платформа (то есть — с контентом, который создают сами пользователи) для детей и подростков — Roblox. 3 декабря 2025 Роскомнадзор ограничил к ней доступ, а 17 декабря опубликовал официальное сообщение о контакте с руководством платформы уже «после ограничения её работы в России» и о готовности Roblox поэтапно привести работу в соответствие требованиям российского законодательства.

Тема защиты детей от опасного или противоправного контента в интернете всегда более общественно одобряемая, чем меры борьбы с абстрактными мошенниками и террористами, поэтому общественная реакция ожидаемо менее острая. В целом же на любых платформах с пользовательским контентом всегда можно найти спорные материалы, поэтому недостатка аргументов для блокировок не будет.

Пропаганда национальных сервисов

В марте 2025 года компания VK заявила о выпуске бета-версии российского супераппа MAX, а к середине августа 2025 пресс-служба MAX отчиталась о 18 млн пользователей. Даже если это и было правдой, такая цифра и близко не доходила до показателей WhatsApp и Telegram. В разгар блокировок голосовой связи в этих мессенджерах, на фоне административного давления и агрессивного медиапродвижения MAX, среднесуточный охват нацмессенджера составил 5,7% населения. Telegram и WhatsApp охватывали 55,2% и 66,7% соответственно.

Такие невысокие цифры использования MAX могут быть связаны не только с проблемами с приватностью — просто мессенджер действительно выглядит недоработанным и менее удобным, чем привычные иностранные аналоги. Но российский суперапп предустанавливается на новые телефоны, которые продаются в России, а сотрудников бюджетных учреждений, родителей школьников и детсадовцев заставляют использовать его под угрозой проблем на работе или у ребенка. Так или иначе, его аудитория растет.

В сентябре 2025 года эксперты RKS Global протестировали MAX на предмет непрерывной слежки за пользователями и опровергли гипотезу, что он ведет себя как шпионское программное обеспечение. Однако уже через несколько месяцев результаты новых тестов показали, что в приложении появился функционал расширенной слежки. Оно может просить больше доступов или пытаться получить их самостоятельно, может передавать больше информации, чем ему было разрешено получить и др. Поведение мессенджера, аффилированного с государством, может измениться в любой момент. А россиянампрактически не остается выбора, кроме как пользоваться подконтрольными государству сервисами.

6. Давление на магазины приложений, медиа-площадки и цензура на платформах с медиаконтентом

В 2025 Роскомнадзор продолжил наступление на площадки размещения различных типов контента. Под прицелом оказались все каналы получения информации и нужных инструментов.

Притеснение магазинов приложений

В 2025 году деплатформинг — выдавливание инструментов обхода блокировок из точек их распространения — принял массовый характер. В марте 2025 года Роскомнадзор направил к компании Google 47 обращений об удалении VPN-приложений, хотя до этого такие запросы были единичными.

Согласно данным проекта App Censorship, который занимается изучением интернет-цензуры, за период с 12 марта по 1 апреля 2025 года Россия направила 214 запросов на удаление приложений из Google Play, затронув 212 VPN и аналогичных сервисов — более 90% от всех обращений к Google в тот период. Кроме приложений, Роскомнадзор требовал удалить более 80 тысяч URL-адресов из поиска Google в рамках закона о запрете информации про обход блокировок, но компания запросы проигнорировала.

Apple быстрее и успешнее договаривается с российскими властями. Ещё в сентябре 2024 года было известно о 98 VPN, недоступных в российском AppStore, и это помимо приложений независимых медиа и подкастов. На призывы к открытости и соблюдению прав человека корпорация предпочитала и по-прежнему предпочитает не реагировать.

В начале 2025 года компания Apple заблокировала российским разработчикам доступ к программе Apple Developer Enterprise Program (ADEP). Ранее инструмент активно использовался крупными компаниями и разработчиками для корпоративных бизнес-приложений, чат-ботов, CRM-системы и логистических решений без необходимости публикации в App Store.

Представители компании объясняли свои действия тем, что игнорирование законов помешает работать в России. Правда, как показывает 2026 год, позиция «nothing personal, just business» не защищает этот самый бизнес от последующих претензий со стороны государства.

Удаление приложений VPN из магазинов усложняет пользовательский путь. Некоторые отказываются от установки проверенных сервисов только потому, что они недоступны в AppStore. Разработчики VPN и эксперты публикуют гайды, чтобы помочь пользователям установить сервис, однако проблема остается острой. В 2025 году Apple продолжила скрывать от россиян приложения VPN.

Уже весной 2026 стало известно о том, что Apple удалила из своего стора ряд proxy/V2Ray-клиентов, среди которых Streisand, V2Box, v2RayTun, Happ Proxy Utility. Эти приложения часто использовались для доступа к независимым медиа и Telegram при DPI-блокировках.

Давление на соцсети и контент-мейкеров

В ноябре 2024 года начал действовать закон о регистрации блогеров в реестре соцсетей РКН. Все блогеры с более чем 10 тыс. подписчиков в любой соцсети должны были подать заявление на портале Госуслуг и предоставить персональные данные, иначе им запрещалось размещать рекламу и предложения о финансировании, а пользователи не смогли бы делать репосты.

Весной 2025 власти добавили в Telegram бот Trustchannelbot, чтобы сверять номер заявления на Госуслугах и данные владельца канала, и маркировать подтвержденные каналы знаком A+. Для этого блогерам нужно было добавить бота к себе в канал. Соответственно, ему становились доступны управление каналом и его содержимое. Trustchannelbot видел публикации, историю правок и удалений постов, мог менять название, описание и username, добавлять и удалять участников.

Такая практика создавала реальные риски массового сбора данных об аудитории в случае взломов или утечек, а ранние версии механизма допускали связывание пользователей с номером телефона и профилем на Госуслугах.

Требование Роскомнадзора пройти верификацию Telegram-каналов через специального бота превратило бюрократическую маркировку в технический рычаг.

Цензура контент-платформ

В 2025 году новая волна цензуры накрыла цифровые платформы с контентом. Музыка, фильмы, книги начали исчезать не только по факту блокировки по реестру

запрещенных сайтов, но и через системные удаления со стриминговых сервисов и онлайн-библиотек.

Так, «Яндекс.Музыка» за период IV квартал 2024 и I квартал 2025 по требованиям госорганов удалила 1576 единиц контента (песни, клипы, подкасты) и получила десятки запросов на удаление по конкретным ссылкам. В том числе это был контент, «направленный на дестабилизацию общественно-политической обстановки» в России» (позже такая категория в Transparency Report от «Яндекс.Музыки» уже выделяется). За II-IV квартал 2025 было удалено 2068 единиц контента.

Источник: Transparency Report «Яндекс Музыка» .

Онлайн-кинотеатр «Кинопоиск» (принадлежит компании «Яндекс») в 2025 году удалил девять фильмов и сериалов по требованию Роскомнадзора. Причинами удалений стали: «пропаганда нетрадиционных отношений» (пять проектов), сцены самоубийства (четыре проекта). Директор компании подчеркнул, что запросов на удаление контента от иных государственных органов сервис не получал.

По сообщениям СМИ, в августе 2025 года Таганский суд Москвы принял решение о взыскании с «Кинопоиска» штрафа в 3 млн рублей за демонстрацию контента, признанного «пропагандой нетрадиционных сексуальных отношений». В 2024 году «Кинопоиск» уже был оштрафован на 10 млн рублей по похожей статье.

Другие российские онлайн кинотеатры и стриминговые платформы, такие как «Okko», «Иви», «Билайн» также подверглись штрафам и санкциям за публикацию запрещённого контента. В частности, стриминги сняли с показа испанский сериал «Галгос», в котором нашли признаки ЛГБТ-пропаганды. Компания Apple была оштрафована на 7,5 млн рублей связи с распространением на стриминговом сервисе сериала со сценами «пропаганды нетрадиционных сексуальных отношений».

Наряду с прямой цензурой сверху развивается самоцензура. Популярные стриминги массово вырезают опасные сцены (в частности, ЛГБТ-сюжеты) и в ряде случаев, когда удалять приходится слишком много, сервис блокирует просмотр отдельных серий. Также из фильмов вырезают сцены с эротикой, курением, алкоголем, нецензурной лексикой и др. Пользователи жаловались, что стриминги никак не отмечают контент, из которого вымарана часть эпизодов, выдавая исправленные версии за оригинал. В начале 2026 года появились сообщения, что соответствующие маркировки появились у некоторых сервисов.

С 1 марта 2026 года в России вступил в силу закон, который запрещает прокат и распространение фильмов, дискредитирующих традиционные российские духовно-нравственные ценности или пропагандирующих их отрицание. Закон был подписан президентом Владимиром Путиным 31 июля 2025 года.

В книжном сегменте помимо выборочного давления на издателей и книготорговцев к концу года логика опережающей зачистки дошла до больших онлайн-каталогов: исчезновение контента происходит не только по прямому запрету, но и из-за страха правовых последствий у площадки и правообладателей. «Литрес», крупнейший сервис электронных книг и аудиокниг в России и странах СНГ, сообщил, что снял с продажи около 4,5 тысячи книг из-за риска подпасть под санкции за «пропаганду наркотиков». Всего было удалено порядка 0,5% от общего количества книг на платформе.

Издательские дома в России весь год спешно отзывали из магазинов книги, которые могут быть опасными с точки зрения цензоров. Так как никаких официальных списков запрещенных книг нет, то бремя отбора ложится на самих книготорговцев. В опалу попадают не только книги с ЛГБТ-тематикой, но и те, в которых затрагиваются темы наркотиков, феминизма, религии и пр.

14 мая 2025 года сотрудников издательств «Popcorn Books» и «Individuum» (входящих в группу «Эксмо-АСТ») обвинили в экстремизме. По заявлениям Следственного комитета издательства занимались пропагандой ЛГБТ, в том числе, среди несовершеннолетних. После начала дела все книги издательств «Popcorn Books» и «Individuum» были изъяты с продажи и уничтожены, а сами издательства

прекратили свою деятельность. Весной 2026 года в офисе издательства «Эксмо» прошли обыски с изъятием техники и документов.

Деградация YouTube

Троттлинг (замедление скорости соединения интернет-провайдером) YouTube имеет свою долгую историю. Пользователи по-прежнему видят торможение и частичную недоступность сервиса, но такую, что использование его без VPN становится просто невозможно. Вместо прямого запрета власти ухудшают качество связи до полной потери производительности. Такой подход позволяет сократить аудиторию сервиса без официального запрета, а значит, снизить риски негативной социальной реакции.

В 2024 году в начале замедления YouTube власти России списывали проблемы на деградацию оборудования Google, затем появились заявления официальных лиц о том, что это намеренные действия властей. В 2025 года в Госдуме назвали условия при которых YouTube сможет снова работать в России. Компания Google должна, по мнению депутатов, оплатить штрафы и восстановить доступ к заблокированным без решения суда аккаунтам российских СМИ, а также «разобраться со своим заброшенным оборудованием».

В декабре 2025 года компания Google уведомила российских провайдеров, что планирует забрать свое оборудование Google Global Cache (GGC), как вышедшее из обращения. В частности речь идет о кэширующих серверах модели Dell R720. А в начале 2026 года стало известно, что доменное имя www.youtube.com было удалено РКН из национальной системы доменных имён (НСДИ).

7. Телекоммуникации как инструмент контроля

Нововведение 2025 года — тотальный контроль использования SIM-карт. Государство стало решать, кто имеет право подключаться, на каких условиях и когда именно у пользователя появится мобильный интернет.

С 1 января 2025 года иностранцам стало сложнее покупать SIM-карты. Для того, чтобы получить телефонный номер, иностранным гражданам и лицам без гражданства теперь был нужен СНИЛС, учётная запись на Госуслугах и подтверждение личности по биометрии. Также, появилась обязанность

регистрировать уникальный номер устройства — IMEI. Власти объяснили ужесточение процедуры «мерами, направленными на борьбу с мошенниками и «серыми» сим-картами».

Новый порядок использования SIM-карт вводил ограничения и для россиян. Российским гражданам можно было зарегистрировать максимум 20 SIM-карт на один паспорт (иностранцам — 10). Операторы связи проверяли, сколько телефонных номеров зарегистрировано на абонентов и отключали тех, кто не соответствовал новым требованиям. Из-за этого за год было заблокировано 14 млн телефонных номеров.

В 2025 году в обиход вошел новый термин — «охлаждение» SIM-карт.
После возвращения из-за границы абонент сотовой сети получал SMS о том, что услуги сети для него недоступны, и ему необходимо пройти верификацию или ждать 24 часа, пока связь вернётся. То же самое происходило, если сим-карта была неактивна более 72 часов. После прохождения верификации (через звонок на горячую линию, через приложение оператора связи и пр.), функции мобильного интернета и SMS-сообщений разблокировались.

По заявлениям властей, «охлаждение» должно было отключать от сети SIM-карты, которые использовались в украинских беспилотниках. В таком случае, дроны теряли бы управление. В Кремле заявили, что гражданам «процедура охлаждения SIM-карт никакого дискомфорта не доставляет».

Важным нововведением стала ответственность, которую возложили на абонентов за передачу личных SIM-карт третьим лицам. Статья 13.29.1 КоАП РФ вводила штрафы за предоставление третьим лицам возможности пользоваться мобильным номером — до 50 тыс рублей для граждан и до 200 тыс — для организаций. Эта мера тоже была обоснована борьбой с мошенниками.

Таким образом, власть вновь легитимизировала отключение мобильного интернета в своих интересах уже не как разовую меру безопасности, а формализованную процедуру с восстановлением доступа после проверки личности.

8. Региональные шатдауны в России

В большинстве регионов ограничения влияли не только на работу мессенджеров и соцсетей, но и на сервисы, которые давно упрощали повседневную жизнь: банковские приложения, онлайн-платёжные системы, службы такси и доставки.

В 2025 году отключения мобильного интернета регистрировались почти по всех регионах России. Первые крупные сбои были зафиксированы в мае: накануне празднования Дня Победы мобильный интернет пропал у всех основных операторов в десятках регионов страны. Власти официально связали это с мерами безопасности на массовых мероприятиях и призвали граждан «с пониманием» относиться к ограничению мобильного интернета ввиду «опасного соседства». В тот момент это преподносилось как исключительная мера, но позднее подобные отключения стали повторяться регулярно.

В Москве в мае 2025 года сбои длились несколько дней и охватили как минимум центр города, где проходили сначала репетиции парада, а затем праздничные мероприятия. Уже в марте 2026 года мобильный шатдаун в Москве длился почти две недели, нанеся экономике города серьезный урон. По словам властей, такие отключения могут длиться «столько, сколько необходимо, чтобы обеспечивать безопасность граждан».

С июня 2025 частота интернет-отключений резко возросла: по данным проекта «На связи», количество дней с перебоями интернета (фиксирование сбоев на сетях как минимум двух операторов), выросло с 69 случаев в мае до 662 в июне, а в июле достигло 2099.

Шатдауны мобильного интернета распространились далеко за пределы приграничных зон. Нестабильность связи регистрировалась в центральных, южных, сибирских и дальневосточных регионах, включая крупные города и области предельно далеко от зоны боевых действий, где вероятность ударов или непосредственной угрозы со стороны беспилотников была на тот момент минимальна.

Власти объясняли введение ограничений необходимостью обеспечения безопасности граждан и защиты критической инфраструктуры. В официальных комментариях и региональных пресс-релизах упоминались угрозы, связанные с использованием беспилотников: эти формулировки повторялись в заявлениях

профильных министерств, МЧС и Роскомнадзора и закрепляли интерпретацию шатдаунов как временных превентивных мер в интересах населения, а не как инструмента ограничения доступа. При этом корреляция между между отключениями интернета и эффективностью борьбы с БПЛА у экспертов остаётся под вопросом.

На деле практика шатдаунов была разнообразной: в одних местах интернет пропадал полностью на несколько часов или несколько дней, в других — работал только Wi-Fi, в третьих доступ сохранялся только к одобренным государством сервисам (российским банкам, маркетплейсам и тд) по так называемым «белым спискам». Логика в выборе интернет-ограничений отсутствовала. Сложно утверждать, насколько технические возможности операторов связи координировались с указаниями федеральных властей и желанием местной администрации снизить ущерб от шатдаунов (если таковое было).

В Нижегородской области перебои мобильного интернета фиксировались настолько регулярно, что в отдельных муниципалитетах доступ к мобильным данным на протяжении длительных периодов вообще почти не появлялся. Регион неоднократно упоминался в медиа и мониторинговых сводках как пример того, как мобильный интернет перестаёт быть гарантированной услугой.

Северный Кавказ стал одним из пионеров в практике шатдаунов ещё в конце 2024. Тогда масштабное отключение доступа к «недружественному» сегменту интернета были зафиксированы в Дагестане, Чечне и Ингушетии и продолжались по меньшей мере сутки и уже были описаны в обзоре RKS Global за 2024 год. В течение 2025 года нестабильность соединения в регионе сохранилась под предлогом противодействия терроризму и интересов национальной безопасности.

Источник: https://monitor-ru.net/stat.

Статистика и свидетельства пользователей подтверждают, что к концу года практика локальных шатдаунов перестала быть эпизодической: в 80% российских регионов фиксировались регулярные ограничения мобильного интернета, а по данным экспертов, к концу декабря число зафиксированных региональных отключений исчислялось тысячами случаев по всей стране.

«На связи» приводит множество свидетельств нарушения связности в регионах. Среди них хутор Красиво Белгородской области, куда не был проведен проводной интернет, и поэтому во время шатдаунов жители оказывались изолированными от мира; Ижевск, где шатдауны не спасли от атак беспилотников, но при этом не позволили населению получить экстренные оповещения и укрыться; или Ульяновская область, где вместо временных ограничений связи собирались вводить постоянные.

Источник: Meduza.io, данные: проект «На связи».

Уже в начале 2026 Федеральная служба безопасности России (ФСБ) получила право блокировать связь, даже вне ситуаций угрозы безопасности, что упрощает процесс принятия решений о шатдаунах в интернете. Условия для таких блокировок будут устанавливаться исключительно президентом. Новый закон создал правовую основу для массовых и немедленных отключений любых услуг связи, включая мобильный и проводной интернет, телефонные звонки, электронную почту и т.д. Закон также освободил операторов связи от ответственности за убытки, понесённые абонентами из-за отключений.

По данным экспертов, Россия заняла первое место среди всех стран по отключениям интернета в 2025 году. За год интернет в России был недоступен суммарно 37 166 часов, что обошлось экономике почти в 12 млрд долларов, поскольку современный бизнес сильно завязан на интернет-инфраструктуре. Это самый большой экономический ущерб из-за интернет-шатдаунов в мире, и Россия третий раз лидирует по этому показателю.

9. «Белые» и «серые» списки

Если региональные шатдауны стали самым заметным интернет-явлением 2025 года, то «белые списки» ухудшают ситуацию ещё сильнее. При запуске «белых списков» доступ сохраняется только к заранее согласованным сервисам, тогда как остальной трафик не проходит. Логика «черных списков» — «блокируется только запрещённое»; логика «белых списков» — «работает только разрешённое».

Режим «белого списка» технически похож на инверсию привычной модели блокировок. В обычной реестровой схеме трафик пропускается по умолчанию, а соединения к конкретным IP/доменам режутся через DPI или ACL (access control list). В allowlist-модели по умолчанию блокируется весь внешний трафик, за исключением заранее определённых доменных имён, IP-подсетей или ASN.

Такая схема не требует индивидуального внесения каждого запрещённого ресурса в реестр. Оператору достаточно получить перечень разрешённых адресов и применить политику отклонения всего трафика вне списка исключений. С точки инженерной точки зрения это стандартный механизм сегментации трафика, используемый, например, в корпоративных сетях или при аварийных режимах. Разница в том, что в теперь чрезвычайный режим начал применяться к массовым пользователям

Идею «белых списков» публично впервые анонсировал министр цифрового развития связи и массовых коммуникаций Максут Шадаев в августе 2025 года. Он пообещал, что в список попадут «все ресурсы, нужные для жизни».

Первую версию «белого списка» Минцифры опубликовало 5 сентября. В него вошли сервисы Госуслуг, цифровых пратформ «Яндекс», «ВКонтакте», «Одноклассники», «Дзен», Rutube, Mail.ru, мессенджер Max, маркетплейсы Ozon, Wildberries и Avito, сайт платежной системы Мир, сайты правительства, администрации президента и платформа дистанционного электронного голосования (ДЭГ), операторы связи Билайн, МегаФон, МТС, Ростелеком, Т2.

После этого СМИ и каналы публиковали свои версии белых списков, но официальный белый список сайтов, работающих при шатдаунах, так и не был опубликован. Из-за отсутствия четких правил в «список» не могут попасть социально-значимые сервисы, а для коммерческих, особенно небольших, недоступность во время отключений интернета может привести к разорению.

В марте 2026 года «белые списки» появились в Москве, Санкт-Петербурге и областях. Отмечалась потеря связи по районам с ограничением ко всем сайтам, кроме разрешенных.

Предугадать, какие именно ресурсы кроме информационных понадобятся жителям при шатдауне, достаточно сложно. Так, компания, обслуживающая общественные туалеты в Москве, попросила включить их платежную систему в «белые списки», так как пользователи столкнулись с проблемами во время шатдаунов. В Петербурге городской транспорт временно стал бесплатным, потому что система оплаты проезда закономерно не работала при отключениях интернета.

Параллельно с «белыми списками» в 2025 году в российском интернете появились «серые списки». Так называются ограничения интернета, когда формальных жестких блокировок нет, но сервисы работают нестабильно: соединения обрываются, отдельные функции (например, звонки) пропадают, скорость сильно снижается. Подобные ситуации фиксировались в отношении мессенджеров и видеохостингов и обсуждались как пример управляемой деградации без официального запрета.

Для аналитических инструментов «серые списки» выглядят как селективная фильтрация или ограничение определённых типов трафика, а не как полная блокировка домена.

Именно сочетание этих двух механизмов — узко ограниченной связности через «белые списки» и деградации через «серые» — постепенно формирует своеобразную модель российской интернет-цензуры, отличную от моделей Китая и Ирана.

Ранее прогнозы возможности перехода к модели «работает только то, что одобрено» звучал как крайний сценарий развития инфраструктуры ТСПУ. В 2025 году этот сценарий начал реализовываться на практике, прежде всего в мобильных сетях во время региональных ограничений. Российский интернет идёт по наихудшему сценарию, превращаясь в контролируемую среду со строгими режимами доступа к контенту и самой связи.

10. РКН vs. VPN: игра в «кошки-мышки»

Официальный запрет на распространение информации об обходе блокировок не сработал: спрос на VPN растёт пропорционально ограничениям. В свою очередь, ограничения только ужесточаются. Представители власти периодически уверяют граждан в том, что «введение штрафов за использование VPN не планируется и даже не обсуждается». Однако, эксперты считают, что это довольно реальный вариант развития событий.

Изменение рынка антицензурных решений

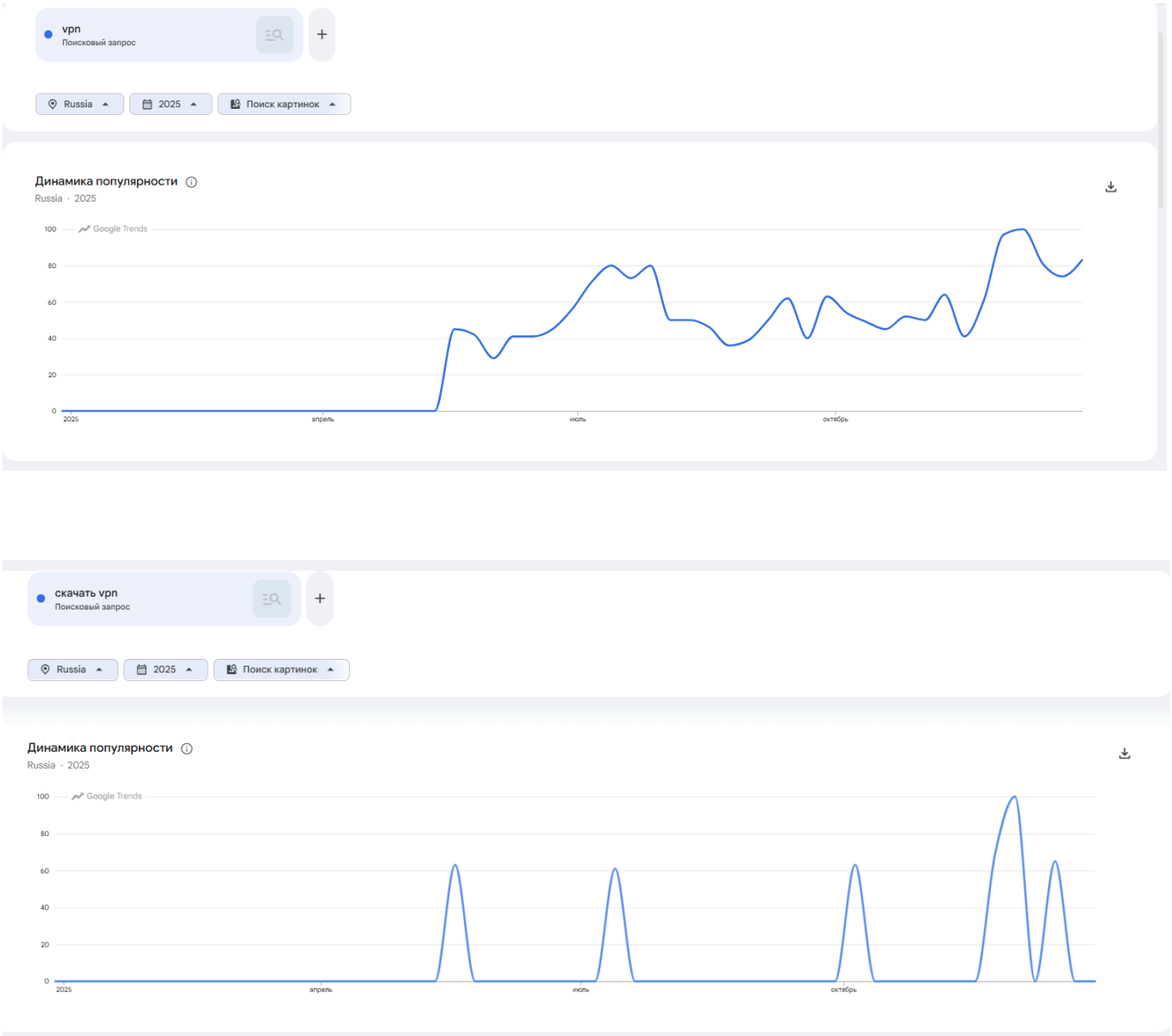
VPN-сервисы стали главным инструментом восстановления доступа к популярным ресурсам и мессенджерам, заблокированным властями России. Рынок средств обхода цензуры стремительно рос на протяжении всего 2025 года. По приблизительным оценкам экспертов, до половины интернет-юзеров в России пользуются VPN, причем большинство из них — платными версиями. Опросы показывают схожую картину — двое из пяти человек активно пользуются VPN-сервисами, а осведомленность россиян о технологиях обхода блокировок с 2024 по 2026 год выросла до 74%.

Согласно результатам опроса аналитического центра Левада за март 2025 года, наиболее активными пользователями VPN были молодые люди, более образованные и обеспеченные опрошенные, а также оппозиционно настроенные граждане. Издание «Коммерсант» приводит статистику Sensor Tower, согласно которой в конце 2025 года активная база пользователей топ-5 VPN в России составила 7,3 млн человек, а за 12 месяцев (с марта 2025 года по март 2026 года) совокупные установки VPN-сервисов достигли 35,7 млн - по данным Digital Budget.

BlancVPN сообщил, что за 2025 год через серверы компании прошло больше 50 петабайт трафика: это примерно 10 миллиардов фотографий в высоком разрешении или 13 миллионов фильмов в качестве 4K.

Частота пользовательских запросов в Google тоже росла в течение всего года. Популярность запроса «vpn» начала расти в первых числах мая 2025 — именно тогда в стране произошли первые локальные шатдауны, приуроченные к Дню

Победы. Также, запросы «скачать vpn» и тд. набирали популярность в периоды, когда происходили блокировки мессенджеров и другие ограничения.



Популярность поисковых запросов «vpn» и «скачать vpn» в Google за 2025 год в России

Небезопасные VPN

На фоне беспрецедентного спроса на VPN в 2025 года стало появляться множество скамерских сервисов, которые выдавали себя за известные VPN, и сервисов-однодневок. С одной стороны, в ответ на блокировки Роскомнадзором очередного VPN-сервиса или протокола достаточно быстро появляются новые сервисы, но с другой, о качестве этих продуктов можно только догадываться.

При этом блокировки в России настолько жесткие, что любой сервис — от самостоятельно поднятого VPN-сервера для небольшого сообщества до крупного коммерческого продукта — может оказаться неработоспособным в любой момент. Люди скачивают и устанавливают себе по нескольку VPN, и иногда среди них оказываются непроверенные, но временно работающие сервисы.

Бесплатные VPN представляют повышенный риск. Разработку и поддержание программы нужно окупать, и его создатели могут продавать данные пользователей рекламодателям. А иногда под оберткой бесплатного VPN распространяется мошенническая или шпионская программа.

В середине 2025 года стало известно, что в Иране, ещё одной стране с жесткой интернет-цензурой, под видом VPN распространялась программа, которая собирала переписки, контакты, местоположение и другие данные пользователей и сливала их Министерству разведки и безопасности. В России о таких случаях пока не известно, но есть сведения, что две страны обмениваются друг с другом практиками цензуры и слежки.

В июле 2025 года представители власти предложили создать «государственный» VPN. По их словам, «ГосVPN» позволит посещать зарубежные ресурсы, которые сами ограничили россиянам доступ, не будучи заблокированными (в пример привели иностранные медицинские журналы). Также к ним относится Microsoft, Booking и др., хотя в целом популярных сервисов, которые добровольно ушли из России, меньше, чем запрещенных. Кроме этого, едва ли стоит ожидать, что государственный VPN станет шифровать пользовательский трафик от самого себя, а значит все действия юзера будут ему видны.

В ходе исследования, проходившего в октябре — декабре 2025 года, эксперты RKS Global выяснили, что почти 20% самых скачиваемых в России бесплатных VPN-приложений связаны с российской интернет-инфраструктурой. 16 приложений из 87 использовали Яндекс.Метрику, причем один сервис даже отправлял данные на собственные серверы в России. Все данные, которые передаются в Россию, согласно «закону Яровой» будут предоставлены силовикам по запросу в любой момент.

Постоянные сбои VPN, выход из строя сервисов, необходимость искать замену, снова платить за доступ или скачивать на свой страх и риск бесплатные альтернативы — всё это ведет к негативному пользовательскому опыту. Что играет на руку властям, которые стремятся дискредитировать VPN как технологию.

VPN как отягчающее

Закон, согласно которому, использование VPN-сервисов при совершении преступлений становится к отягчающим обстоятельствам, был подписан в конце июля 2025 года и вступил в силу с 1 сентября. Также, в ст. 63 УК РФ был добавлен пункт об ужесточении наказания за преступления, совершённые с применением «программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен (VPN-сервисов)». При этом власти уточняли, что использование VPN в личных целях не криминализуется.

Как оказалось, это не совсем так. В декабре 2025 года в Тульской области был вынесен первый приговор, где использование VPN фигурировало как отягчающее обстоятельство. «Используя программно-аппаратное средство доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, зашел в сеть «Интернет», где на сайте обнаружил в наличии смесь (препарат), содержащую наркотическое средство», — сказано в решении.

Тогда же в июле был подписан закон о штрафах за рекламу средств обхода блокировок (вступил в силу 1 сентября 2025 года). В соответствии с документом, за рекламу VPN-сервисов граждан могут оштрафовать на сумму от 50 тыс. до 80 тыс. рублей, должностных лиц — от 80 тыс. до 150 тыс. рублей, а юрлиц — от 200 тыс. до 500 тыс. рублей.

Но привлекать к ответственности за рекламу VPN-сервиса начали ещё до принятия закона. В январе 2025 года Федеральная антимонопольная служба России признала рекламу VPN-сервиса в Telegram-канале «ненадлежащей» по причине того, что его владелец разместил в нем ссылки на онлайн-сервисы.

В июле 2025 российские власти обязали владельцев VPN-сервисов сотрудничать с РКН и завели очередной реестр для исполнительных VPN-провайдеров. Сотрудничество в том числе подразумевало, что сервисы должны ограничивать доступ к запрещенным в России ресурсам, что делало VPN по сути бессмысленными (они все еще помогали бы с приватностью, но этот сценарий использования менее актуален для россиян, чем обход блокировок). За отказ владельца VPN-сервисов ждал штраф и последующая блокировка уже его продукта.

Единственные VPN, которым такой реестр мог бы пригодиться — корпоративные, для удаленного доступа сотрудников. Если они выполняют требования регулятора, то могут быть относительно спокойны насчёт блокировок. Когда Роскомнадзор блокирует VPN по протоколам, страдают все сервисы, потому что они работают по одному принципу, — но лояльные корпоративные сервисы, как правило, не затрагиваются.

Ранее на сайте Роскомнадзора появилась рекомендация для «владельцев VPN российских частных виртуальных сетей» отказаться от иностранных протоколов шифрования, «используемых, в том числе, приложениями, предоставляющими доступ к запрещённой информации». Или, если отказаться невозможно, передавать IP-адреса используемых VPN-серверов, чтобы их внесли в специальный список исключений. Наталья Касперская, президент ГК InfoWatch — компании, тесно связанной с государством — заметила, что передача IP-адресов Роскомнадзору означает, что эти адреса скорее всего будут взломаны или утекут. А значит, зарубежные сервисы (GitHub и проч., нужные для программистов) их увидят и просто заблокируют доступ.

Блокировка VPN-протоколов

Представители VPN-сервисов говорят о том, что им приходится работать в ситуации постоянного давления. Предугадать, с какими трудностями разработчики и пользователи VPN столкнутся завтра, невозможно: ситуация меняется очень быстро.

Логика протокольных блокировок описана в главе 4.

По данным DPI Detector, в течение всего 2025 года года популярные протоколы Shadowsocks, Wireguard и OpenVPN массово блокировались на мобильном и частично домашнем интернете почти во всех регионах страны. Время от времени фиксировались трудности у Cloak.

С мая 2025 года ряде регионов у разных операторов фиксировались попытки блокировок XRay (REALITY) и SOCKS5 на домашнем интернете. Пик блокировок пришелся на 4–16 июня, когда на домашнем интернете было заблокировано большинство протоколов, что частично совпадает с началом блокировок хостингов в России. В августе большой сбой фиксировался на протоколах OpenVPN, Shadowsocks, AnyConnect и Cloak также на домашнем интернете в Санкт-Петербурге, Ленинградской и Псковской областях.

С осени 2025 года работа большинства VPN-протоколов в России затруднена из-за активного внедрения «белых списков». Популярные ещё в начале года Shadowsocks, Wireguard и OpenVPN не работали или работали с перебоями. Эксперты отмечают, что ранее в случаях перебоев с другими протоколами помогало подключение через Xray (VLESS+Reality), но с ноября и он подвергся частичной блокировке.

Особенность протокола VLESS+Reality в том, что он скрывает сам факт использования VPN, маскируя VPN-трафик под обычный HTTPS-трафик. VPN Guild опубликовала заявление, в котором призвала пользователей VPN и СМИ не паниковать относительно блокировки VLESS, так как «цензоры могут осложнить доступ для определенных групп пользователей, но они не могут полностью контролировать эти технологии». К началу декабря работоспособность XRay постепенно восстановилась.

В июле 2025 года команда Amnezia выпустила новую версию своего собственного протокола AmneziaWG, созданного специально для работы в самых сложных с точки зрения цензуры регионах. В версия AmneziaWG 1.5 трафик стал маскироваться под наиболее распространённые UDP-протоколы (QUIC, DNS и др.). Однако, по словам самих разработчиков, «маскировка спасает не всегда»: системы DPI научились распознавать даже обфусцированные протоколы на основе статистики и поведенческих паттернов. В начале 2026 года вышла версия AmneziaWG 2.0, в которой трафик стал ещё менее детектируемым за счёт постоянно меняющихся заголовков и размеров пакетов данных.

Технологическая гонка требует ресурсов, которых у цензурных ведомств несоизмеримо больше. Издержки этого противостояния не готовы нести даже крупные провайдеры типа Nordvpn или Surf Shark. Но и расходы госорганов тоже растут. По подсчетам The Moscow Times, с 2022 года Минцифры, Роскомнадзор и другие госструктуры заключили контракты на на ограничение распространения информации и блокировки на 35 млрд рублей, из них 12 млрд — в 2025 году.

Помимо описанной выше блокировки VPN-протоколов, российские цензоры применяют и другие методы блокировки. VPN блокируют по сигнатурам (когда система ТСПУ ищет любые узнаваемые признаки VPN — шаблоны трафика, заголовки, особенности шифрования, типичные пакеты и другие «отпечатки»), статистическими методами (например, если через один сервер проходит слишком много трафика, цензоры предполагают, что он используется для VPN и через некоторое время такие IP-адреса блокируют). Также проводятся «контрольные закупки» у конкретных VPN-сервисов, после чего изучается их устройство и начинается блокировка серверов.

11. Альтернативные средства обхода блокировок

VPN — самый распространенный инструмент борьбы с цензурой, но эта популярность делает его и главной мишенью надзорных ведомств. Между тем, существуют и другие способы выхода в свободный интернет, и многие из них не требуют особой технической подкованности.

Большинство СМИ ещё до блокировки Telegram запустили почтовые рассылки. Специалисты советуют завести дополнительные почты на Google, а также на Proton или Tuta, потому что российские почтовые клиенты типа «Яндекс.Почты» и Mail.ru могут блокировать нежелательных отправителей, и письмо не дойдет даже до папки «спам».

Поскольку в рассылку сложно включить полноценные статьи, некоторые медиа стали вспоминать про ленту RSS. Это файл, напоминающий текстовый, но с разметкой веб-сайта. Как только материал публикуется на сайте, он автоматически попадает в RSS. Пользователь получает файл на почту, или устанавливает программу RSS-ридер, где подписывается на RSS-ленты различных СМИ.

Перемещение на незапрещённые альтернативы является более краткосрочным решением — Роскомнадзору ничего не стоит заблокировать очередной мессенджер или сервис видеозвонков, как было с Google Meet или FaceTime. И вряд ли французский, корейский или американский сервис станет прикладывать усилия, чтобы вновь стать доступным в стране, где у него сравнительно небольшая аудитория, или если в нем изначально нет встроенных функций противодействия блокировкам. К тому же, далеко не все эти сервисы соответствуют критериям безопасности.

Например, Delta Chat, мессенджер, который работает на протоколах электронной почты, устойчив к блокировкам и прошёл аудиты безопасности, хоть и у некоторых пользователей в России были проблемы со скоростью доставки сообщений. Также работает децентрализованный Matrix, у которого вместо единственного центрального сервера, на котором все держится, развернута инфраструктура из множества серверов. А вот ставший популярным imo специалисты не рекомендуют для приватного общения.

Из соцсетей остались незаблокированными только наименее популярные в России типа Reddit или Mastodon, причем Reddit сам иногда банит российских пользователей. Mastodon — децентрализованная соцсеть, где вместо страниц и профилей — серверы. Серверы отличаются тематически (технологии, активизм, региональная повестка), и пользователь с учетной записью на одном сервере подписывается на пользователей с других серверов и видит их посты. Можно создать сервер на Mastodon, а можно на собственной инфраструктуре. Роскомнадзор не сможет заблокировать всю соцсеть (как и мессенджер Element, упоминавшийся выше) — ему понадобится блокировать каждый сервер отдельно.

Ещё один способ обойти блокировки — купить физическую или электронную зарубежную SIM-карту и включить роуминг. Когда пользователь выходит в сеть с карточкой из Германии, Сербии и тп, его устройство регистрируется в сети через международный роуминг и направляет трафик через домашнего (родного для карточки) оператора. Способ работает не всегда — некоторые иностранные SIM-карты всё равно подключаются к российским сетям. Прежде чем приобретать карточку, понадобится изучить информацию об услугах оператора и о том, каким образом он обрабатывает трафик.

С 2025 года почти перестали работать некоторые известные утилиты обхода блокировок, в частности, бесплатные GoodbyeDPI и Zapret. В отличие от VPN, который создаёт туннель от устройства до своего сервера и затем до нужного сайта, и скрывает местоположение юзера, GoodbyeDPI и Zapret просто модифицировали пакеты трафика. То есть, меняли форму некоторых заголовков, подмешивали ложные запросы, дробили пакеты, чтобы ТСПУ запутался. Но в отличие от того же VPN, эти инструменты не шифровали трафик, так что цензурное оборудование всё равно могло вычислить, на какой именно ресурс отправлялся запрос.

Параллельно Роскомнадзор применяет «резиновые» блокировки: на основании одного решения о запрете ресурса блокируются новые ссылки, зеркала и страницы, так что реестр пополняется пакетами без необходимости каждый раз оформлять новую процедуру. И всё же зеркала позволяют получать информацию хотя бы ограниченное время.

В современном мире Роскомнадзору очень сложно окончательно обрубить все возможности для связи. При необходимости люди находят самые нестандартные способы коммуникации — после блокировки WhatsApp и Telegram они общались в чатах приложений для тренировок, мобильных игр, в комментариях фотографиям Apple,в «Яндекс.Пробках» и «Google Таблицах».

12. Расширение запретительного законодательства

Законодатели перешли от ограничения публикаций и санкций за распространение «нежелательной» информации к наказанию за её поиск и потребление. В ситуации возрастающих рисков от слежки в сети за действиями пользователя VPN возвращается к своему базовому назначению — не только обходить блокировки, но и скрывать содержимое сетевой активности от провайдера и государства.

Запрет поиска экстремистских материалов в интернете

В КоАП была введена статья 13.53, согласно которой умышленный поиск заведомо экстремистских материалов и получение доступа к ним, в том числе через средства обхода блокировок, наказывается штрафом от 3 000 до 5 000 рублей. Таким образом, рискует уже не только автор, распространитель или владелец площадки, но и пользователь, который ищет или открывает запрещённый материал. Вычислить такого пользователя можно через проверку устройств, историю браузера и поисковых запросов, а также через операторов связи, если пользователь посещает незащищенные шифрованием сайты (HTTP, а не HTTPS).

Эксперты, опрошенные «Роскомсвободой», отмечали, что операторы могут видеть, какие приложения запускает пользователь и на какие сайты он заходит (например, через DNS). По мнению экспертов, эти поправки напоминают белорусский сценарий — криминализацию потребления запрещённого контента и софта.

В ноябре 2025 года стало известно о первом административном деле за преднамеренный поиск экстремистских материалов в интернете. Его завели против жителя Свердловской области, которому суд назначил штраф около 3 000 рублей. По одной из версий, информацию о правонарушении в ФСБ передал неназванный оператор связи.

Запрет рекламы у «нежелательных» и «экстремистских» организаций

С 1 сентября 2025 к запретам на рекламу у «иноагентов», рекламу обхода блокировок и распространение научно-технической и статистической информации о VPN добавился запрет на рекламу на ресурсах, признанных «нежелательными» или «экстремистскими», а также вообще на всех заблокированных ресурсах. Закон затрагивает рекламу в Instagram и Facebook, так как эти ресурсы принадлежат корпорации Meta, признанной российскими властями «экстремистской организацией» и запрещенной в России. Причём наказание предусматривается как за публикацию новой рекламы, так и за неудаление старой.

В случае нарушения применяется общий состав по ч. 1 ст. 14.3 КоАП: до 2 500 рублей для граждан, до 20 000 рублей для должностных лиц и до 500 000 рублей для юрлиц.

Уже через пару месяцев депутаты предложили увеличить штрафы, так как им стало «очевидно, что штраф в 2500 рублей никого не останавливает — рекламу в запрещенных соцсетях блогеры по-прежнему размещают». В октябре стало известно о первом штрафе за рекламу в Instagram: некое «третье лицо» пожаловалось на блогера за материал, размещенный до вступления в силу закона.

В 2026 году эта логика распространилась на крупные платформы, которые не имеют экстремистских или нежелательных статусов, а просто находятся под блокировкой. Telegram и YouTube стали предметом отдельного контроля. ФАС разъясняла, что по фактам размещения рекламы в Telegram и YouTube анализируются содержание рекламы, дата договора, дата публикации и дата введения ограничений на работу платформы; затем ведомство объявило переходный период до конца 2026 года, в течение которого меры ответственности за рекламу на этих двух площадках применяться не будут.

Рекламная инфраструктура всё сильнее привязывается к реестрам, статусам площадок и решениям регуляторов, превращая маркетинговые бизнес-процессы в ещё один механизм давления на независимые медиа, блогеров и сервисы обхода блокировок.

13. На пути к изоляции Рунета: преодоление зависимости от мировой инфраструктуры и технологий

Цензоры в 2025 году практикуют в Рунете не тотальную изоляцию, а селективную доступность: где-то троттлинг, где-то деградация функций, где-то доступ, разрешенный по списку исключений, как при шатдаунах.

Селективная доступность стала устойчивым режимом функционирования рунета: цензурные ведомства нарушали работу сервисов так, что ими становилось неудобно пользоваться. Так, в начале блокировок мессенджеры могли работать без VPN, но сообщения и медиа-файлы доставлялись с задержкой, а VoIP-вызовы не проходили, либо качество связи резко падало.

Тем не менее, полная изоляция остаётся сложной даже при расширении имеющихся инструментов в распоряжении цензоров. Россия всё ещё зависит от мировой инфраструктуры доставки контента (CDN), облаков и трансграничной связности, поэтому любое давление на инфраструктурных посредников быстро превращается в побочный ущерб для огромного массива несвязанных ресурсов.

Например, при региональных шатдаунах мобильного интернета наблюдалась частичная связность по спискам, но даже в таком режиме стабильность работы даже непредсказуемой: списки расширялись, менялись, формально обозначенное, как разрешённое, могло работать не всегда.

14. Заключение и прогнозы

Все описанные выше наблюдения имеют своей целью фиксацию этапов развития цифровой цензуры в России в 2025 году. Ретроспективный обзор цензурных практик, применяющихся в России, может быть полезным исследователям, журналистам, цифровым активистам, разработчикам антицензурных инструментов, а также просто пользователям интернета в России, которые смогут самостоятельно спрогнозировать дальнейший ход событий и подготовиться.

Спустя год после публикации первого обзора за 2024 год, ситуация с интернетом в России стала ещё менее предсказуемой, чем раньше. Учитывая всё описанное выше, эксперты предполагают, что возможно следующее развитие событий:

1. Технологическая война, которую ведет Роскомнадзор против свободного интернета в России зависит от развития военного конфликта между Россией и Украиной.
   Здесь важен экономический аспект - как будет распределяться и перераспределяться бюджет РФ в условиях дефицита, сколько будет выделено денег на цензуру и насколько эффективно они будут освоены.
   Важно и то, станут ли в какой-то момент объекты инфраструктуры связи (дата-центры, точки обмена трафиком, ретрансляторы и пр.) целью для военных атак, какой урон они понесут и как быстро смогут восстановиться.

2. По всей видимости, будет продолжаться деградация физической инфраструктуры российского интернета. С одной стороны это связано с нехваткой инвестиций и собственных производственных мощностей, с другой - с последствиями санкций и слишком высокой цены параллельного импорта. Импорт из Китая скорее всего не будет закрывать все потребности.
   Так ситуация с замедлениями и деградацией глобальных сервисов станет ещё более непрозрачной. Не всегда теперь ясно, то ли дело в банальном износе оборудования, то ли в намеренных действиях Роскомнадзора.

3. Деградация инфраструктуры ведет к тому, что новые нагрузки на нее в виде блокировок, замедлений, нарушения связности могут иметь непредсказуемые эффекты. Так в марте 2026 года, когда началась новая большая волна блокировки Telegram, ТСПУ на нескольких узлах ушло в bypass, и заблокированные ресурсы (включая YouTube и WhatsApp) временно стали доступны. Такие инциденты могут повторяться и учащаться.

4. В связи с усложнением ситуации с бюджетом и инфраструктурой, государство постарается перекладывать часть цензурных обязательств на бизнес. Так в апреле 2026 года российские IT-компании уже были вынуждены подчиниться требованию наладить слежку за VPN на устройствах пользователей.

5. Отключения интернета в разных регионах будут повторяться. Это продолжение движения в сторону деградации связанности, начатое в полном объеме России в 2025 году.

6. Цензоры будут продолжать охоту за VPN, атакуя в первую очередь наиболее большие и популярные сервисы. Цель - нанести как можно больший урон и отключить разом как можно большее количество пользователей. Будут продолжаться блокировки серверов VPN, статистические блокировки, а также

удаления приложений из сторов (в первую очередь из AppStore). Пользовательский опыт будет ухудшаться.

7. В связи с тем, что каждый VPN-сервис будет рано или поздно атакован и потеряет работоспособность на какое-то время, распространенной пользовательской практикой становится подключение и использование нескольких VPN и других антицензурных инструментов одновременно. Это позволяет не потерять доступ в свободный интернет.
Однако эксперты настаивают на том, что критически важно изучать информацию о VPN до их установки, особенно аккуратно относиться к решениям, которые распространяются бесплатно. Для выбора надежных решений можно пользоваться информацией на сайтах: vpnlove.org, vpnguild.org, vpnpay.io, vpn-ru.net. Также можно опираться на советы privacyguides.org и руководство от Electronic Frontier Foundation.

8. Риски ужесточения законодательства за рекламу и распространение антицензурных инструментов, а также введение наказания за пользование ими по прежнему очень актуальны.

9. Следуя логике развития импортозамещения и контроля над сервисами в Рунете, вероятно мы увидим реализацию идеи «государственного VPN», который получит преференции будет позиционироваться, как легальная альтернатива другим сервисам, как мы видели это в истории с мессенджером MAX.

Обзор создан на основе открытой информации, сообщений СМИ, собственных исследований команды RKS Global, а также в результате сбора мнений экспертов в сфере цифровых прав. В документ включены данные тестирования блокировок VPN-протоколов проекта DPIDetector, полученные благодаря помощи волонтеров-держателей нод.

Обзор не мог бы состояться без опоры на материалы коллег из команд Роскомсвободы, Tech Talk, На связи, OONI, VPN Guild, Amnezia VPN. Выражаем им большую признательность за их труд и борьбу.