Лестница блокировок. Часть вторая: от замедления к изоляции (2025–2026)

Весной 2025 года в первой части "Лестницы блокировок" мы прогнозировали новые этапы российской интернет-цензуры: от блокировок Telegram и VPN до перехода к "белым спискам" и разделения Рунета. Всего за год почти все эти шаги были пройдены в ускоренном темпе.

Вторая часть анализирует события 2025-го и первой половины 2026 года. Веерные отключения мобильного интернета, удушение WhatsApp и Telegram, принудительное внедрение госслужбы MAX, детектирование протоколов обхода и перекладывание цензуры на бизнес сформировали новую архитектуру контроля. Цензура перешла от принципа "запретить лишнее" к принципу "разрешить только нужное". Это фиксация уже произошедших фактов с проверяемыми источниками. Первая часть доступна здесь: https://ozi-ru.net/art1.html

Дисклеймер: Настоящий документ составлен на основе данных из указанных источников, поиск и обобщение которых выполнялись с помощью нескольких больших языковых моделей (LLM). Итоговый текст прошел обязательную ручную редактуру и проверку человеком.

Оглавление

Глава 1. Введение: год, в котором прогноз стал хроникой

Первая часть этого исследования заканчивалась весной 2025 года прогнозом.[1] Опираясь на логику эскалации, мы перечислили вероятные следующие ступени "лестницы блокировок": полную блокировку Telegram, внедрение статистических методов выявления VPN, переход к блокировке крупных блоков IP-адресов, тактику "серых списков" и намеренного ухудшения качества связи, переход от "черных списков" к "белым" и, наконец, полную изоляцию Рунета. Часть этих шагов мы относили к ближайшей перспективе, часть — к отдаленной. Переход к "белым спискам", например, описывался как технически сложный сценарий "в более отдаленной перспективе".

Прошел год и за это время почти все перечисленные ступени оказались пройдены — а некоторые в темпе, которого не предполагал даже пессимистичный прогноз. Telegram заблокирован. VPN-протоколы нового поколения детектируются по поведенческим признакам. Блоки IP-адресов крупных хостеров и CDN уходят в реестр пачками. "Белые списки" из теоретической конструкции

[1] Лестница блокировок. Часть первая // Общество защиты интернета URL: https://ozi-ru.net/art1.html

превратились в работающий механизм, развернутый в большинстве регионов страны. А движение к разделению трафика на внутренний и международный из метафоры "цифрового железного занавеса" стало предметом конкретных совещаний в Минцифры с конкретными цифрами лимитов.

Более того, период 2025–2026 годов добавил к "лестнице" то, чего прежний анализ не предусматривал как центральные инструменты: веерные отключения мобильного интернета (шатдауны), ставшие повседневностью по всей стране, и принуждение десятков миллионов пользователей к государственному мессенджеру. Если предыдущий этап цензуры можно описать формулой "запретить доступ к лишнему", то новый этап точнее описывается формулой "разрешить доступ только к нужному". Это качественный сдвиг: от точечной фильтрации к управлению самой возможностью соединения.

Цель этой части — проследить события 2025 года и первой половины 2026 года, показать, как отдельные меры складываются в единую архитектуру контроля, и зафиксировать фактуру с проверяемыми источниками. Прогноза в этой части нет: мы фиксируем то, что уже произошло.

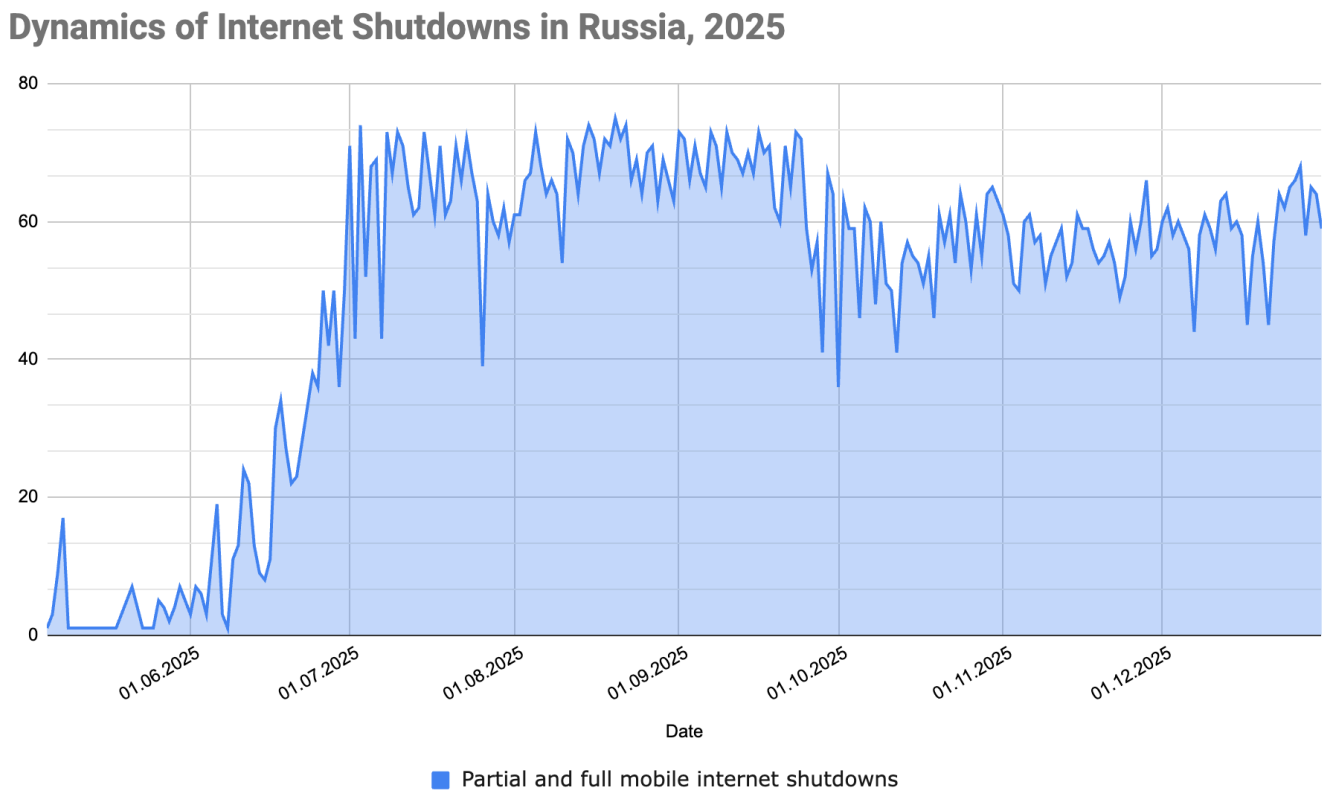
Оговорка о терминах. На протяжении всего описываемого периода государство почти нигде не использует слово "блокировка" применительно к крупнейшим сервисам. Официальные формулировки — "замедление", "частичное ограничение", "меры понуждения". Как и в случае с YouTube летом 2024 года, фактический результат (невозможность пользоваться сервисом) достигается техническими средствами без формального объявления. Мы будем разделять официальную риторику и фактическое положение дел везде, где они расходятся.

Глава 2. Год отключения

Главным новшеством 2025 года стали массовые отключения мобильного интернета — практика, которая за несколько месяцев прошла путь от единичных эпизодов к общенациональной норме. Масштаб виден по годовой статистике проекта "На Связи" (сотрудничающего с Обществом защиты интернета), которая ведёт счёт случаям отключений помесячно. В мае 2025 года наблюдатели зафиксировали всего 68 случаев за месяц. Уже в июне их число выросло почти в десять раз — до 652. Пик пришёлся на разгар лета: 1967 случаев в июле и 2099 в августе — больше, чем зафиксировано во всём мире за весь 2024 год (по данным Access Now — 296 отключений в 54 странах). К осени интенсивность стабилизировалась на высоком уровне: 1725 случаев в октябре, 1693 в ноябре и 1823 в декабре. Всего за 2025 год зафиксировано 12 024 инцидента.[2]

[2] Помесячная статистика веерных отключений мобильного интернета за 2025 год — проект "На Связи" (в сотрудничестве с Обществом защиты интернета); сводные данные также в статье Википедии "Отключения интернета в России". URL: https://ru.wikipedia.org/wiki/Отключения_интернета_в_России

График 1. Динамика отключений мобильного интернета в России, 2025



На графике — динамика веерных отключений мобильного интернета в России за 2025 год: по вертикальной оси отложено число регионов, где в течение суток фиксировались частичные или полные отключения, по горизонтальной — даты с мая по декабрь. Более ранних данных на графике нет: до так называемых "парадов победы" закреплённой практики отключения мобильного интернета в России не было. Кривая наглядно распадается на три фазы. До начала июня значения держатся у нуля с редкими одиночными всплесками до 15–19 регионов. С первых чисел июня линия почти вертикально идёт вверх и за три-четыре недели поднимается с единиц до 70 с лишним регионов. С июля по сентябрь держится высокое плато в коридоре 55–75 регионов с сильными суточными колебаниями. Осенью, после короткого провала на рубеже сентября и октября, кривая не идёт на спад, а закрепляется в диапазоне 45–68 регионов до конца года — отключения превращаются из разового события в постоянный фон.

1. Парад как точка отсчета (май 2025)

Первое массовое отключение, привлекшее всеобщее внимание, произошло в дни "празднования 80-летия Победы". С 7 по 9 мая 2025 года мобильную связь и интернет ограничивали в Москве и

более чем тридцати регионах.[3] Официального объяснения по существу не дали: пресс-секретарь президента Дмитрий Песков заявил, что ограничения вводятся "по понятным причинам", а все, что связано с обеспечением безопасности граждан, "оправдано".[4] Логика была прозрачна: мобильный интернет используется для управления беспилотниками, поэтому на время массовых мероприятий его проще отключить, чем прикрывать небо над самими мероприятиями средствами ПВО.

2. "Паутина" и перелом (июнь 2025)

Переломным моментом стала украинская операция "Паутина" (Spiderweb) 1 июня 2025 года, когда дроны, заранее скрытно доставленные вглубь России в специальных контейнерах на грузовиках с дистанционно вскрывающейся крышей и запущенные уже рядом с аэродромами, атаковали стратегическую авиацию сразу на нескольких базах. Управление частью аппаратов, по ряду сообщений (но не доказано), велось в том числе через российские сотовые сети. После этого отключения мобильного интернета перестали быть привязаны к праздникам и превратились в рутинную реакцию на любую угрозу или ее ожидание.[5]

Именно операция "Паутина" объясняет июньский скачок: до неё счёт отключений шёл на десятки случаев в месяц, сразу после — на сотни. 8 июля 2025 года был поставлен антирекорд по охвату: мобильный интернет в той или иной форме отключали в 77 из 89 субъектов федерации.[6] На графике этот перелом виден как почти отвесный подъём кривой в первых числах июня, а антирекорд 8 июля ложится на верхнюю границу — около 75 регионов в сутки.

Методология подсчета у независимых наблюдателей консервативна: учитываются жалобы пользователей, подтвержденные технической проверкой минимум по двум операторам, а также официальные сообщения властей.[7] Это означает, что реальный масштаб, скорее всего, выше зафиксированного.

3. Москва и вопрос об эффективности (2025–2026)

К весне 2026 года отключения дошли до столицы в новом качестве. С 6 марта 2026 года мобильный интернет в центре Москвы отключали более недели подряд — по сведениям отраслевых источников,

---

[3] Шатдауны в России: что происходит с мобильным интернетом // Forbes Россия URL: https://www.forbes.ru/tekhnologii/542902
[4] Песков объяснил отключения мобильного интернета перед парадом // Forbes Россия URL: https://www.forbes.ru/tekhnologii/542902
[5] Карта шатдаунов: как в России отключают мобильный интернет // Meduza URL: https://meduza.io/feature/2025/07/07/karta-shatdaunov
[6] Отключения мобильного интернета в России // Рувики URL: https://ru.ruwiki.ru/wiki/Отключения_мобильного_интернета_в_России
[7] Как умирает интернет: карта шатдаунов // Meduza URL: https://meduza.io/feature/2025/10/16/kak-umiraet-internet-karta-shatdaunov

это было связано с финальным тестированием режима "белых списков" в столице.[8] Для москвичей это стало неожиданностью: отключения на территории Москвы случались и раньше, но никогда не были такими масштабными и продолжительными. Столица, привыкшая жить в особом режиме, на собственном опыте выяснила, что находится в России.

При этом эффективность шатдаунов как меры противодействия беспилотникам вызывает все больше вопросов. Дата-журналисты "Новой газеты Европа" в марте 2026 года, сопоставив географию отключений с сообщениями о реальных атаках, пришли к выводу, что около 85% случаев отключений приходились на дни, когда в соответствующих регионах не сообщалось о прилетах. В регионах, находящихся глубоко в тылу, вне досягаемости украинских дровнов, интернет отключали более чем в 98% дней наблюдения.[9] Это подтверждает и форма графика: осенью кривая не снижается, а держится высоко до конца года. Мобильные шатдауны из ситуативной меры безопасности превратились в постоянный режим работы, который сам по себе становится инструментом ограничения связи.

4. Цена

Экономические оценки расходятся в зависимости от методики, но все указывают на колоссальный масштаб ущерба. Общество защиты интернета, используя методику Брукингского института, оценивало один час полного шатдауна примерно в 46 млрд рублей по стране (только для Москвы — около 9,6 млрд рублей в час).[10] Международный сервис Top10VPN по итогам года назвал Россию мировым лидером 2025 года по продолжительности интернет-ограничений: 37 166 часов, около 146 млн затронутых пользователей и ущерб в 11,9 млрд долларов — более 60% общемирового ущерба от шатдаунов.[11]

Реакция рынка оказалась показательной: спрос сместился в сторону проводного доступа и спутникового интернета. "Коммерсантъ" со ссылкой на данные "Триколора" сообщал, что продажи услуги "Триколор Интернет" во втором квартале 2025 года выросли в 2,4 раза год к году.[12] Невозможность полагаться на мобильную связь стала не временным неудобством, а фактором, перестраивающим потребительское поведение.

---

[8] "Белые списки" сайтов в России // Википедия URL: https://ru.wikipedia.org/wiki/%C2%AB%D0%91%D0%B5%D0%BB%D1%8B%D0%B5_%D1%81%D0%BF%D0%B8%D1%81%D0%BA%D0%B8%C2%BB_%D1%81%D0%B0%D0%B9%D1%82%D0%BE%D0%B2_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8

[9] Ни ответа, ни прилета // Новая газета Европа URL: https://novayagazeta.eu/articles/2026/03/26/ni-otveta-ni-prileta

[10] Отключения продолжаются: как жить в эпоху интернет-шатдауна // Ямал-Медиа URL: https://yamal-media.ru/narrative/otkljuchenija-prodolzhajutsja-kak-zhit-v-epohu-internet-shatdauna

[11] The Global Cost of Internet Shutdowns // Top10VPN URL: https://www.top10vpn.com/research/cost-of-internet-shutdowns/

[12] Спрос на спутниковый и проводной интернет вырос на фоне отключений // Коммерсантъ URL: https://www.kommersant.ru/doc/7908736

5. Административная логика отключений

Чтобы понять, почему отключения стали именно такими — хаотичными и повсеместными, — нужно смотреть не на технику, а на бюрократию. За веерными шатдаунами стоит не единая государственная стратегия, а логика ведомственной отчётности.

Публичное обоснование неизменно: власти разных уровней многократно повторяли, что отключают мобильный интернет ради безопасности, поскольку украинские беспилотники используют сотовые сети для связи с центрами управления. Проблема в том, что реальными средствами противодействия дронам региональные власти не располагают. Такой возможности нет даже у военных и систем ПВО, и тем более непонятно, что может противопоставить беспилотной угрозе администрация небольшого субъекта РФ. В условиях, когда с региона по умолчанию спрашивают за недопущение ущерба, но инструментов для этого не дают, и родилась идея отключать интернет — не столько ради результата, сколько ради отчётности перед федеральным центром.

Организационно это устроено вне правового поля. Насколько известно, решения об отключении принимают региональные рабочие группы, куда входят администрация субъекта, медицинская служба, МЧС, МВД и региональные подразделения ФСБ; именно они отдают операторам связи команду на отключение. Поскольку ни закона, ни иного нормативного акта, регулирующего эту процедуру, не существует, регионы действуют бессистемно: каждый отключает интернет по-своему, в своих границах и по собственным основаниям. Отсюда и разнобой на карте отключений, и невозможность заранее предсказать, где и когда пропадёт связь.

География первых месяцев подтверждает, что практика распространялась не сверху, а вширь, от регионов-первопроходцев. Больше всего отключений за первые два месяца пришлось на Нижегородскую область (21 случай) и Омскую область (20 случаев); в топ-5 вошли также Ростовская, Псковская, Саратовская и Тульская области — по 19 случаев в каждой. Судя по всему, приём отработали в одном из этих субъектов, а затем его переняли остальные.

Закрепиться этой практике помог своего рода обратный карго-культ. Логика региональных властей выстраивается так: интернет отключили — дрон не прилетел, следовательно, отключение сработало. Отсутствие атаки записывается в заслугу отключению, хотя причинной связи между ними нет, а корреляция объясняется тем, что подавляющее большинство отключений и без того приходится на регионы вне досягаемости дронов. Так самоподтверждающийся вывод превращает разовую меру в постоянную: отчётность требует продолжать, а мнимая эффективность даёт основание не останавливаться.

Глава 3. Белые списки: изнанка шатдаунов

Самым значимым следствием шатдаунов стало то, что прогнозировалось как отдаленный сценарий: переход от модели "черных списков" к модели "белых". И произошел он не как отдельное идеологическое решение, а как вынужденная техническая реакция на хаос отключений.

В терминах "лестницы блокировок" это и есть та самая инверсия логики, которую первая часть относила к отдаленному будущему: не "запрещено то, что в списке", а "разрешено только то, что в списке". Разница принципиальная — при модели "белых списков" по умолчанию недоступно все, кроме того, что явно разрешено.

1. Логика возникновения

Тотальное отключение мобильного интернета бьет не столько по дронам, сколько по экономике и по лояльности граждан: перестают работать банковские приложения, оплата, такси, госсервисы, карты. Убытки при этом несут все — от розничного продавца, у которого встают терминалы оплаты, до операторов связи, для которых отключенная сеть означает прямые потери выручки при сохранении всех издержек на ее содержание. Именно операторы и завязанный на мобильный интернет сегмент "цифровой экономики" оказались стороной, для которой шатдауны обернулись не абстрактным неудобством, а измеримыми финансовыми потерями.

Поэтому "белые списки" стоит рассматривать не как замысел бюрократии, а как вынужденный компромисс, к которому власти подтолкнула сама индустрия. Регулятору был нужен способ и дальше отключать сеть под предлогом борьбы с беспилотниками, и одновременно снять напряжение бизнеса, требующего сохранить хотя бы жизненно важные сервисы. "Белые списки" и стали этим механизмом: перечень ресурсов, доступ к которым сохраняется во время шатдауна, тогда как все остальное обрывается.

Публично идею озвучил министр цифрового развития Максут Шадаев на форуме "Цифровая эволюция" 7 августа 2025 года; техническую схему согласовали с операторами, а доступ к разрешенным ресурсам предполагалось защищать капчей, чтобы ими не воспользовались для управления беспилотниками.[13]

2. Развертывание (с сентября 2025)

Первый перечень появился 5 сентября 2025 года. В него вошли Госуслуги, "ВКонтакте",

[13] Минцифры подготовило схему доступа к мобильному интернету в условиях ограничений// ТАСС URL: https://tass.ru/ekonomika/24732149

"Одноклассники", Mail.ru, мессенджер Max, сервисы "Яндекса" и сайты органов власти.[14] Затем список расширялся — в ноябре, дважды в декабре 2025 года, в феврале и апреле 2026 года; к маю 2026 года он включал более 500 российских сервисов. Ключевое условие включения сформулировано прямо: все вычислительные мощности ресурса должны находиться в России.[15]

География режима росла параллельно с географией шатдаунов: к середине октября 2025 года "белые списки" применялись примерно в 48 регионах, к марту 2026 года — в 68–71 регионе.[16] Хронология первых недель, где известна точная дата подключения каждого региона, не только подтверждает эту оценку, но и показывает, насколько неравномерно шёл процесс.

Таблица 1. Хронология подключения регионов к режиму белых списков (16 сентября — 16 ноября 2025)

Дата	Регионов	Регионы	Всего
16.09.2025	9	Владимирская область, Волгоградская область, Камчатский край, Республика Башкортостан, Республика Дагестан, Ростовская область, Самарская область, Саратовская область, Ярославская область	9
17.09.2025	5	Воронежская область, Краснодарский край, Нижегородская область, Омская область, Приморский край	14
18.09.2025	3	Красноярский край, Москва, Орловская область	17
19.09.2025	6	Мурманская область, Новгородская область, Пензенская область, Республика Удмуртия, Томская область, Челябинская область	23
20.09.2025	3	Калужская область, Республика Татарстан, Свердловская область	26
21.09.2025	4	Амурская область, Республика Марий Эл, Республика Саха (Якутия), Тамбовская область	30

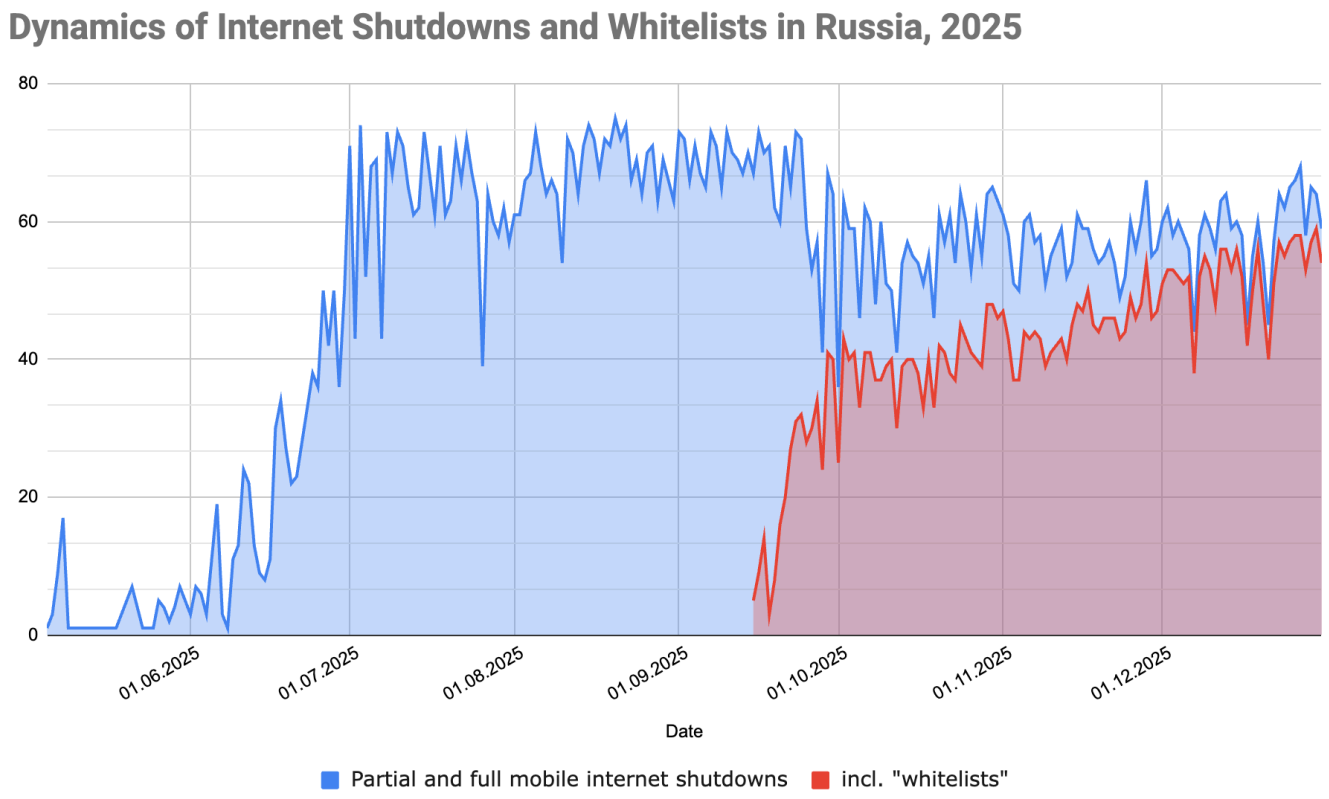
[14] Белый список сайтов в России: что доступно при шатдаунах // GoGov URL: https://gogov.ru/articles/site-white-list
[15] Белые списки интернета в России // Forbes Россия URL: https://www.forbes.ru/tekhnologii/559771
[16] Как умирает интернет: карта шатдаунов // Meduza URL: https://meduza.io/feature/2025/10/16/kak-umiraet-internet-karta-shatdaunov

Дата	Регионов	Регионы	Всего
22.09.2025	1	Иркутская область	31
24.09.2025	1	Псковская область	32
25.09.2025	3	Кировская область, Костромская область, Тульская область	35
26.09.2025	6	Алтайский край, Курская область, Санкт-Петербург, Сахалинская область, Тверская область, Ханты-Мансийский автономный округ	41
29.09.2025	1	Брянская область	42
30.09.2025	3	Астраханская область, Ивановская область, Тюменская область	45
01.10.2025	1	Смоленская область	46
02.10.2025	1	Ульяновская область	47
15.10.2025	1	Республика Коми	48
24.10.2025	1	Вологодская область	49
26.10.2025	1	Республика Адыгея	50
28.10.2025	1	Рязанская область	51
01.11.2025	1	Хабаровский край	52
13.11.2025	3	Оренбургская область, Архангельская область, Пермский край	55
14.11.2025	1	Кемеровская область	56
16.11.2025	1	Московская область	57

Хронология распадается на две фазы с разной динамикой. За первые пятнадцать дней, с 16 по 30 сентября, режим включили в 45 из 57 регионов этой выборки (79%); из них 30 (53%) — за первые шесть дней, 16–21 сентября, когда одновременно добавлялось по 3–9 регионов в сутки. Это не постепенное распространение практики, а фактически синхронный общенациональный запуск, растянутый на несколько дней технической ротацией регионов. После 30 сентября темп падает на порядок: за полтора месяца, с 1 октября по 16 ноября, добавилось лишь 12 регионов — в среднем один раз в четверо суток против трёх в день в сентябре. Оставшиеся регионы подключались по остаточному принципу: либо шатдауны там были не так интенсивны, либо сказались задержки с оборудованием ТСПУ.

Заметно выделяется случай Москвы: город получил доступ к режиму уже на третий день кампании, 18 сентября, тогда как Московская область — только 16 ноября, последней записью в этой хронологии. Разрыв в два месяца между столицей и её ближайшим окружением виден даже на фоне общей неравномерности процесса.

График 2. Отключения мобильного интернета и охват белыми списками, 2025



На графике — та же динамика веерных отключений (синяя область, см. График 1), но с наложением доли случаев, где отключение сопровождалось действующим белым списком (красная область). До начала сентября красная область равна нулю: механизма ещё не существовало. С запуском первого перечня 5 сентября она начинает расти, а резкое ускорение приходится на 16–30 сентября — те же даты, что и массовый ввод регионов по таблице выше; за это время красная область поднимается с нуля до 30–40. После короткого провала на рубеже сентября и октября, синхронного с провалом на синей кривой, рост возобновляется и продолжается весь четвёртый квартал: к концу декабря красная область достигает 55–58 против 60–68 у синей. Разрыв между кривыми, в октябре составлявший 20–25, к концу года сокращается до 5–10.

Здесь важно различать два измерения одного процесса. Таблица фиксирует географию доступности — когда режим технически стал возможен в каждом регионе; это почти целиком история сентября, за пятнадцать дней которой охватили 79% итогового списка. График показывает интенсивность применения — долю ежедневных отключений, реально проходящих с белым списком, а не как полное обнуление связи; здесь основной рост приходится уже на октябрь-декабрь, то есть на месяцы, когда прирост новых регионов почти остановился. Инфраструктура была развёрнута практически повсеместно уже к концу сентября, но переход от технической возможности к

применению по умолчанию занял ещё один квартал. Это подтверждает тезис, сформулированный в начале главы: переход от чёрных списков к белым — не одномоментное решение, а процесс с двумя разными скоростями, техническим развёртыванием и последующим закреплением в повседневной практике.

3. Техника белых списков

Технически режим реализован через фильтрацию по DNS, IP-адресам и подсетям: все, чего нет в списке, не открывается. Реализуют его сами операторы — на связке из установленного по требованию РКН оборудования ТСПУ и собственных систем DPI, которые операторы закупают на открытом рынке. Так, в начале сентября 2025 года Билайн объявил тендер на обновление своей DPI-платформы, попросив поставщика добавить к блокировке конкретных адресов возможность классифицировать трафик абонентов по тематическим категориям.[17] Принципиально важно, что смена IP-адреса или VPN здесь не помогает — зарубежные адреса блокируются как класс, а сам VPN-сервер находится вне списка.[18] Режим касается мобильного интернета; слухи о его распространении на проводной доступ Минцифры в марте 2026 года опровергло.[19]

Обход этих ограничений строится на "транспортном камуфляже" на базе протоколов семейства V2Ray/Xray (в частности, VLESS с технологией Reality), где запрещенный прокси-трафик упаковывается внутрь легитимных TLS-сессий, направленных к IP-адресам, входящим в белые списки, например к серверам Яндекса или ВК. Настраиваясь на имитацию подключения к разрешенному ресурсу из списка, технология копирует его TLS-рукопожатие и параметры шифрования, из-за чего системы DPI видят происходящее как стандартное обращение локального пользователя к одобренному сайту.

Важно понимать, что любая из этих технологий срабатывает лишь с некоторой вероятностью. Один и тот же метод не работает одинаково у разных операторов, в разных регионах и даже внутри одного оператора в одном регионе: результат зависит от конкретной прошивки оборудования, версии сигнатур и текущей волны ограничений. Со временем доля успешных подключений в режиме белых списков снижалась, и по имеющимся оценкам к середине 2026 года не превышает десяти процентов.

Причина в том, что операторы и РКН целенаправленно борются с обходом. Фильтрация дополняется поведенческим анализом: система отслеживает аномалии трафика — например, несколько параллельных попыток установить TLS-соединение к одному и тому же SNI за короткий интервал

---

[17] Билайн объявил тендер на обновление DPI; система должна будет классифицировать трафик не только по отдельным адресам, но и по категориям. Медиазона, 3 сентября 2025. https://zona.media/news/2025/09/03/dpiline
[18] Белый список: что это и как работает // Kod.ru URL: https://kod.ru/bely-spisok
[19] "Белые списки" сайтов в России // Википедия URL: https://ru.wikipedia.org/wiki/%C2%AB%D0%91%D0%B5%D0%BB%D1%8B%D0%B5_%D1%81%D0%BF%D0%B8%D1%81%D0%BA%D0%B8%C2%BB_%D1%81%D0%B0%D0%B9%D1%82%D0%BE%D0%B2_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8

замораживают дальнейшие подключения.[20] Кроме того, под наблюдение и ограничения попали сами облачные площадки, через которые строится камуфляж. Провайдеры, чьи адреса входят в белые списки, — Yandex Cloud и VK Cloud (а также Selectel и Cloud.ru) — перестали быть гарантией доступности: РКН начал ограничивать целые подсети и автономные системы российских дата-центров, ранее считавшиеся безопасными.[21]

4. "Охлаждение" SIM-карт

В рамках внедрения "белых списков" и ограничения доступа к сети одной из ключевых мер по "недопущению подключения вражеских дронов к сетям общего пользования" стало жесткое регулирование SIM-карт. Под особый контроль попали устройства, которые регистрируются в сети после длительного отсутствия или возвращаются из международного роуминга. Для них применяется механизм под названием "период охлаждения": как только такая SIM-карта снова активируется на территории РФ, операторы связи автоматически блокируют на ней доступ к мобильному интернету и отправке/приему SMS-сообщений ровно на 24 часа.[22] Чтобы снять это ограничение по истечении суток и подтвердить, что картой пользуется реальный человек, а не автоматизированная система навигации беспилотника, абоненту необходимо пройти верификацию через капчу (CAPTCHA).[23] Для SIM-карт иностранных операторов подобный режим ограничений начал действовать в октябре 2025 года. Официально эта процедура позиционируется как защита инфраструктуры от управления дронами через сотовые сети, однако на практике она позволяет государству мгновенно изолировать и вручную контролировать подключение любого мобильного абонента.

5. Под контролем ФСБ

Формально белые списки формирует Минцифры, однако перечень утверждается только после согласования с ведомствами, отвечающими за безопасность, — прежде всего с ФСБ; это подтверждали и в самом министерстве.[24] Само распределение ролей лишний раз доказывает, что белые списки возникли не как элемент стратегии по отключению страны от мирового интернета, а как реакция на уже происходящие полные отключения: их вводили не для того, чтобы что-то отрезать, а чтобы удержать доступным хотя бы жизненно важный минимум. Однако именно этот компромиссный механизм силовой блок быстро перехватил и переоснастил под собственные задачи: за несколько

---

[20] О схеме ограничений РКН в июне 2026-го (реверс-инжиниринг механизма заморозки TLS-соединений по SNI). Хабр, июнь 2026. https://habr.com/ru/articles/1044396/
[21] Конец эпохи белых списков: РКН повлиял на работу облачных провайдеров. Хабр, январь 2026. https://habr.com/ru/articles/988862/
[22] Лимит SIM-карт и режим доступа // Российская газета URL: https://rg.ru/2025/11/11/rezhim-dostupa.html
[23] Россияне, вернувшиеся из-за границы, столкнулись с блокировкой SIM // CNews URL: https://www.cnews.ru/news/top/2025-11-11_rossiyanevernuvshiesya_iz-za
[24] Минцифры: сервисы вносятся в белый список после согласования с заинтересованными ведомствами и органами, отвечающими за безопасность, в том числе с ФСБ. Anti-Malware, 2 февраля 2026. https://www.anti-malware.ru/news/2026-02-02-114534/48900

месяцев контроль над содержимым списка фактически перешел к нему, а критерий включения сместился с технического на политический.

Если осенью 2025 года для попадания в список было достаточно разместить инфраструктуру сервиса на территории России, то в начале февраля 2026 года ФСБ запретила вносить в белые списки приложения банков, не установивших оборудование СОРМ.[25] Из-за невыполнения этого требования в перечнях отсутствуют приложения Сбербанка, Т-Банка и Газпромбанка — то есть сервисы, которыми пользуются десятки миллионов человек.[26]

Логика требования выстроена через статус организатора распространения информации (ОРИ). Еще в октябре 2025 года ФСБ уведомила крупные банки, что их приложения подпадают под ОРИ, поскольку содержат функцию обмена сообщениями — переписку со службой поддержки и между пользователями, — и обязала установить СОРМ до 2027 года.[27] Статус ОРИ влечет исполнение требований пакета Яровой: хранение метаданных и содержимого переписки на территории России и выдачу этих данных вместе с ключами шифрования по запросу правоохранительных органов. С января 2026 года срок обязательного хранения такой информации увеличен до трех лет, а за неисполнение предусмотрены штрафы и вплоть до блокировки ресурса.[28]

Так замкнулась конструкция: доступность банковского приложения для граждан во время отключения интернета поставлена в прямую зависимость от готовности банка обеспечить слежку за собственными клиентами. Белый список из инструмента, сохраняющего жизненно важные сервисы, превратился в рычаг принуждения — механизм, вынуждающий бизнес разворачивать инфраструктуру наблюдения под угрозой отключения.

Побочным эффектом стало искажение конкуренции. В марте 2026 года председатель Банка России Эльвира Набиуллина публично раскритиковала выборочное включение банков в список, назвав это нарушением правил равной конкуренции, и заявила, что в перечне должны быть все банки с

---

[25] Белый список цифровых платформ // TAdviser URL: https://www.tadviser.ru/index.php/Статья:Белый_список_цифровых_платформ

[26] РБК: в белых списках отсутствуют приложения Сбербанка, Т-Банка и Газпромбанка (изложение по Meduza). 2 февраля 2026. https://meduza.io/news/2026/02/02/rbk-fsb-zapretila-vnosit-v-belyy-spisok-prilozheniya-bankov-ne-ustanovivshih-sisteme-dlya-otslezhivaniya-i-hraneniya-perepiski-polzovateley

[27] ФСБ в октябре 2025 года потребовала от крупных банков установить СОРМ до 2027 года в связи со статусом ОРИ. Forbes, 2 февраля 2026. https://www.forbes.ru/finansy/554634-fsb-zapretila-vnosit-v-belyj-spisok-prilozenia-bankov-bez-sistemy-hranenia-dannyh

[28] Требования пакета Яровой к ОРИ: хранение переписки и ключей шифрования, передача по запросу; с января 2026 года срок хранения увеличен до трех лет. SecurityLab, 2 февраля 2026. https://www.securitylab.ru/news/568856.php

лицензией.[29] Сами банки, по данным участников рынка, медлят с установкой СОРМ, опасаясь оттока клиентов; спор при этом идет не о самой слежке, а о том, кто первым согласится о ней объявить.

Глава 4. Государственный мессенджер MAX

Одновременно с блокировками и ограничением доступа к привычным зарубежным сервисам государство выстраивало "положительную" часть своей стратегии. Она заключалась в форсированном создании и продвижении полностью подконтрольных российских платформ (таких как VK, Rutube, Дзен), куда, по замыслу властей, должны принудительно мигрировать пользователи, лишенные альтернатив.

1. От анонса к закону

25 марта 2025 года холдинг VK (генеральный директор — Владимир Кириенко) анонсировал мессенджер Max, прямо описывая его как аналог китайского WeChat: общение, платежи, госуслуги и мини-приложения в одном окне.[30] Уже 4 июня на совещании у президента глава Минцифры Максут Шадаев заявил о развитии национального мессенджера на базе Max, а в июне платформа была внесена в реестр отечественного ПО.[31]

24 июня 2025 года Владимир Путин подписал Федеральный закон № 156-ФЗ о создании "многофункционального сервиса обмена информацией" — правовую основу национального мессенджера.[32] 12 июля 2025 года распоряжением правительства № 1880-р оператором сервиса было определено ООО "MAX".[33]

---

[29] Набиуллина: включение только части банков в белый список нарушает правила равной конкуренции; в перечне должны быть все лицензированные банки. Forbes, март 2026. https://www.forbes.ru/finansy/557633-nabiullina-raskritikovala-vklucenie-v-belyj-spisok-mincifry-tol-ko-nekotoryh-bankov

[30] Max (мессенджер) // Википедия URL: https://ru.wikipedia.org/wiki/Max_(мессенджер)

[31] -//-

[32] О создании многофункционального сервиса обмена информацией (ФЗ № 156-ФЗ от 24.06.2025) // Официальное опубликование правовых актов URL: http://publication.pravo.gov.ru/document/0001202506240021

[33] Мессенджер MAX: оператор сервиса // Госуслуги (региональный портал) URL: https://co44-cherepovec-r19.gosweb.gosuslugi.ru/glavnoe/messendzher-mah/

2. Структура собственности и личный контроль Кремля

Официальным оператором национального мессенджера распоряжением правительства было назначено ООО "MAX" (до 24 июня 2025 года именовавшееся ООО "Коммуникационные платформы"). Компания была зарегистрирована 4 сентября 2024 года по юридическому адресу: г. Москва, Ленинградский проспект, д. 39, стр. 79. Пост генерального директора занимает Фарит Фаритович Хуснояров, а функции управляющей организации выполняет ООО "Коммуникационная платформа" — прямая дочерняя структура холдинга VK.

Через эту цепочку юридических лиц мессенджер Max полностью принадлежит МКПАО "ВК" (бывшая Mail.ru Group), управление и владение которой наглядно демонстрируют, что главная цифровая платформа страны контролируется Владимиром Путиным лично и его ближайшим окружением:

- **Руководство холдинга:** Генеральный директор VK — Владимир Кириенко, сын первого заместителя руководителя Администрации Президента РФ Сергея Кириенко, который в Кремле непосредственно отвечает за внутреннюю политику, идеологию и цензуру в российском интернет-сегменте.
- **Акционеры и бенефициары:** Контрольный пакет голосующих акций VK (через компанию "МФ Технологии") принадлежит консорциуму структур, неразрывно связанных с ближним кругом Путина. Главными акционерами выступают АО "СОГАЗ" и Газпромбанк. Крупнейшими совладельцами "СОГАЗа" являются давний личный друг президента Юрий Ковальчук, его семья и родственники самого Путина (в частности, его племянник Михаил Шеломов).

Таким образом, создание мессенджера Max — это не коммерческий проект частного рынка, а стратегическая государственная инициатива, оператором которой назначен цифровой холдинг, находящийся в прямом семейно-номенклатурном управлении Администрации Президента и финансируемый "кошельками" правящего клана.

3. Принуждение к переходу

Дальнейшие шаги превратили "национальный мессенджер" в обязательный. С сентября 2025 года Max начали предустанавливать на все новые смартфоны и планшеты, продаваемые в России, а учебные чаты и профили "Сферума" стали переводить в Max.[34] В ноябре 2025 года Минцифры письмом предписало государственным организациям перейти на Max до 1 января 2026 года, бюджетным учреждениям — до 1 февраля 2026 года, с отчетностью о переходе.[35] В марте 2026 года Max получил официальный статус социальной сети, и РКН начал регистрировать в нем каналы.[36]

---

[34] Новый российский мессенджер MAX // Образование (региональный портал) URL: https://xn--h1alcedd.xn--d1aqf.xn--p1ai/instructions/novyy-rossiyskiy-messendzher-makh/
[35] Госорганизации обяжут перейти на Max // GoGov URL: https://gogov.ru/news/924335
[36] Max получил статус социальной сети // Гарант URL: https://www.garant.ru/news/2024987/

29 декабря 2025 года был подписан закон, обязывающий вести "домовые чаты" управляющих компаний, ресурсоснабжающих организаций и фондов капремонта именно в Max (исключение сделали только для Москвы, которой разрешили использовать региональные системы).[37] Таким образом, пользователя подталкивали в мессенджер сразу с нескольких сторон: через школу, через работу в госсекторе, через коммунальные сервисы.

К марту 2026 года платформа отчиталась о 100 млн зарегистрированных пользователей и суточной аудитории свыше 55 млн.[38] Эти цифры нужно читать с поправкой на принудительный характер регистрации, но сам масштаб охвата сомнений не вызывает.

4. Приватность и слежка

Критика мессенджера Max сосредоточена вокруг угроз для приватности пользователей. В приложении полностью отсутствует сквозное шифрование (end-to-end), а его правила прямо предусматривают передачу данных по запросу государственных органов. Независимые исследователи зафиксировали, что Max собирает IP-адреса и проверяет, включен ли у пользователя VPN, а реверс-инжиниринг кода выявил внутри приложения скрытые сторонние библиотеки.[39] Юрист "Роскомсвободы" Саркис Дарбинян охарактеризовал этот проект как масштабный эксперимент над гражданами, который создает риски для выстраивания в России системы социального рейтинга по китайскому образцу.[40]

Связь между принудительным внедрением Max и искусственным удушением его конкурентов эксперты проговаривали открыто. Еще в августе 2025 года аналитик Эльдар Муртазин, который в целом поддерживает войну и действующую власть, комментируя начавшиеся тогда блокировки звонков в WhatsApp и Telegram, прямо предположил, что эти мессенджеры в России будут целенаправленно "ломать", чтобы вынудить людей перейти в Max.[41] Дальнейшие события полностью подтвердили эту логику.

5. MAX и VK вне App Store: санкционный парадокс

Летом 2026 года экосистема VK, включая продвигаемый государством MAX, лишилась доступа в App Store. 3 июня Apple удалила сам MAX, объяснив это соблюдением правил экспортного контроля и санкционных ограничений; приложение перестало отправлять пуш-уведомления на iPhone. 25 июня

---

[37] Домовые чаты переведут в мессенджер Max // Forbes Россия URL: https://www.forbes.ru/society/553066
[38] Max: статистика пользователей // GoGov URL: https://gogov.ru/news/927214
[39] Мессенджер Max проверяет IP пользователей и активность VPN: исследование // Skillbox URL: https://skillbox.ru/media/code/messendzher-max-proveryaet-ip-polzovateley-i-aktivnost-vpn-issledovanie/
[40] "Безопасный" мессенджер Max оказался под огнем критики // Tproger URL: https://tproger.ru/news/-bezopasnyj--messendzher-max-okazalsya-pod-ognem-kritiki
[41] Эксперт предупредил о возможной блокировке WhatsApp // Московский комсомолец URL: https://www.mk.ru/social/2025/08/12/

из магазина исчезли и остальные сервисы холдинга — около двух десятков приложений: ВКонтакте, Одноклассники, Дзен, Mail.ru, VK Видео, VK Музыка, VK Мессенджер, VK Знакомства, VK Play и другие. Apple сослалась на санкционное законодательство, не уточнив конкретных оснований; VK назвала действия односторонними и заявила, что никогда не фигурировала в санкционных списках, а Минцифры пожаловалось в ФАС на недобросовестную конкуренцию.[42]

Формально VK права: самой компании в списках OFAC, ЕС или Великобритании нет. Но санкционные режимы работают не только по прямому включению в список, но и по принципам владения и контроля — правилу OFAC о 50% и его британскому аналогу, по которым структура, контролируемая подсанкционными лицами, сама подпадает под действие санкций. По этим принципам положение VK иное. Гендиректор холдинга Владимир Кириенко (сын замглавы администрации президента Сергея Кириенко) под персональными санкциями США с февраля 2022 года. Большинством голосов в VK управляют через АО МФ Технологии: в 2021 году Газпромбанк выкупил у Сбера долю в этой структуре и передал ее Газпром-медиа. То есть VK контролируется цепочкой, замкнутой на подсанкционные стороны, — и по букве принципов контроля западные корпорации должны были бы прекратить с ней любое сотрудничество.

Именно так однажды и произошло. В конце сентября 2022 года, после введения Великобританией санкций против руководителей Газпромбанка, Apple удалила приложения VK из App Store, а представитель компании прямо пояснил, что сервисы распространяются разработчиками, большинство которых принадлежит подсанкционным сторонам или контролируется ими. Но уже в октябре 2022 года Apple вернула приложения обратно, и сотрудничество возобновилось.[43] Нынешнее удаление — по сути возврат к последовательному применению тех же принципов, от которого уже отступили.

При этом удаление осталось половинчатым. На стороне Android приложения VK и MAX по-прежнему доступны в Google Play: Google, в отличие от Apple, сотрудничество с холдингом не прекратил.[44] Один и тот же набор фактов о владении и контроле две американские корпорации трактуют противоположным образом — что лишь подчеркивает, насколько применение санкционных принципов к VK остается вопросом корпоративного решения, а не автоматического следствия закона.

---

[42] Apple удалила приложения VK из App Store 25 июня 2026 года, сославшись на санкционные правила; мессенджер MAX удален 3 июня; VK отрицает нахождение под санкциями, Минцифры пожаловалось в ФАС; гендиректор VK Владимир Кириенко под санкциями США с февраля 2022 года. Коммерсантъ, 26 июня 2026. https://www.kommersant.ru/doc/8765165

[43] Контроль над большинством голосов в VK через АО МФ Технологии (Газпромбанк выкупил долю Сбера в 2021 году и передал Газпром-медиа); удаление приложений VK в сентябре 2022 года из-за санкций Великобритании против руководителей Газпромбанка и их восстановление в октябре 2022 года; пояснение представителя Apple о распространении сервисов подсанкционными сторонами. Forbes, 14 октября 2022. https://www.forbes.ru/tekhnologii/479753-apple-vernula-zablokirovannoe-v-konce-sentabra-prilozenie-socseti-vk-v-v-app-store

[44] На момент удаления приложений VK из App Store они оставались доступны для Android в Google Play, RuStore, Huawei AppGallery и других магазинах. CNews, 25 июня 2026. https://zoom.cnews.ru/news/item/694702

Здесь скрыта и обратная причинно-следственная связь, объясняющая всю кампанию против мессенджеров в следующей главе. Если бы Apple и Google с самого начала последовательно применили принципы контроля и удалили MAX и VK из своих магазинов, у государства не осталось бы национального мессенджера, ради которого стоило зачищать рынок. Продвигать было бы просто нечего — и тогда блокировка WhatsApp и Telegram теряла бы смысл: незачем силой сгонять аудиторию в сервис, которого нет в сторах. Именно готовность корпораций (прежде всего Google, а до июня 2026 года и Apple) продолжать размещать и обновлять MAX сделала ставку на него реалистичной, а значит — сделала осмысленной и саму блокировку конкурентов. Иными словами, блокировка WhatsApp и Telegram стала возможна не вопреки, а благодаря тому, что западные платформы все эти месяцы держали MAX и VK в своих магазинах.

Глава 5. Удушение WhatsApp и Telegram

Кампания против Telegram и WhatsApp — двух последних массовых независимых мессенджеров в России — разворачивалась поэтапно, пройдя путь от точечного ухудшения работы отдельных функций (например, блокировки звонков) до фактического закрытия доступа к приложениям. Официально эти ограничения оправдывались риторикой о борьбе с телефонным мошенничеством и спамом. Однако за этой ширмой скрывалось очевидное желание Кремля полностью зачистить информационное поле от неподконтрольных каналов связи и принудительно перевести российскую аудиторию на одобренный государством мессенджер Max.

1. Атака на звонки (август 2025)

В августе 2025 года начались массовые сбои голосовых и видеозвонков. 13 августа РКН официально подтвердил "частичное ограничение" звонков в Telegram и WhatsApp, объяснив его борьбой с мошенничеством и вовлечением граждан в "диверсионную и террористическую деятельность".[45] Технически ограничение реализовали в первую очередь через инфраструктуру ТСПУ, нацеленную на VoIP-трафик.[46]

Удар именно по звонкам выглядел расчетливо: голосовая связь в мессенджерах была массово востребована и считалась защищённой. Подрывая ее, власти одновременно снижали ценность сервисов и создавали спрос на отечественную альтернативу.

2. Блокировка WhatsApp

[45] РКН подтвердил ограничение звонков в Telegram и WhatsApp // РБК URL: https://www.rbc.ru/politics/13/08/2025/689c8c7c9a79479b1087586d
[46] Как РКН ограничивает звонки в мессенджерах // РБК URL: https://www.rbc.ru/technology_and_media/13/08/2025/689cab709a7947a32eb24afb

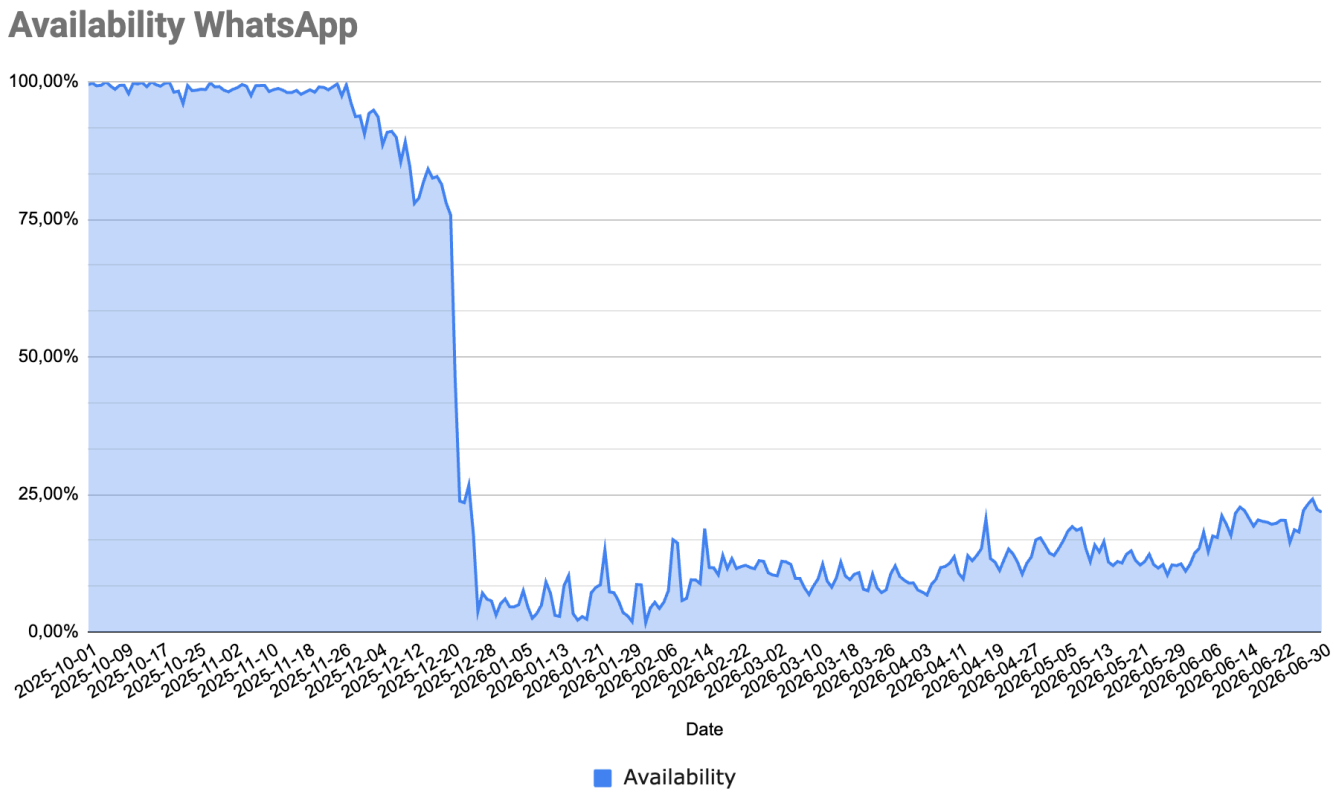
Ограничения, начатые в августе 2025 года с блокировки звонков в WhatsApp и Telegram, к осени переросли в проблемы с доступом к самим мессенджерам. Сбои начались 20–21 октября в южных регионах, а к 22 октября распространились на десятки регионов, включая Москву и Санкт-Петербург; в тот же день РКН вновь признал "частичное ограничение" работы WhatsApp и Telegram. Многие наблюдатели сходились в том, что подлинная цель — перевод аудитории в Max.[47]

В декабре 2025 года давление усилилось: по данным РБК, скорость WhatsApp снизили на 70–80%, а РКН допустил возможность полной блокировки сервиса.[48] Тогда же, в декабре, под ограничения попали Snapchat, FaceTime и игровая платформа Roblox.[49]

Хронологию этого перехода наглядно фиксирует график доступности WhatsApp (данные OONI). До конца ноября 2025 года показатель держался у отметки 100%, колеблясь в пределах обычного статистического шума. 1 декабря доступность впервые опустилась ниже 90%, то есть вышла за границы этих колебаний, — первый измеримый признак преднамеренной деградации, а не случайных сбоев. Затем в течение трех недель шло планомерное снижение — та самая фаза замедления на 70–80%: 21 декабря доступность упала ниже 50%, а 25 декабря сервис был фактически заблокирован, показатель обвалился ниже 10%.

[47] Частичная блокировка Telegram и WhatsApp в России // Википедия URL: https://ru.wikipedia.org/wiki/Частичная_блокировка_Telegram_и_WhatsApp_в_России
[48] В России замедлили WhatsApp на 70–80% // E1 URL: https://www.e1.ru/text/world/2025/12/24/76185979/
[49] Что заблокировали в России в декабре 2025 // Новая газета Европа URL: https://novayagazeta.eu/articles/2025/12/29/

График 3. Блокировка WhatsApp, график доступности



Характерна сама форма кривой: это не мгновенное отключение, а управляемый спуск от замедления к блокировке, растянутый почти на месяц. Такая растянутость объясняется устройством системы фильтрации. Оборудование ТСПУ установлено у операторов по всей стране, в разных регионах, и не может быть переключено одномоментно — раскатка любой новой блокировки идет постепенно, узел за узлом. К тому же отключение сервиса с аудиторией порядка 97 млн пользователей[50] чревато непредсказуемыми последствиями, поэтому резкий обрыв связи рискован. РКН и его подразделение ЦМУ ССОП отработали осторожную тактику еще на замедлении YouTube: блокировку раскатывают ступенчато, начиная, по всей видимости, с сегментов с наименьшим объемом трафика и постепенно распространяя на остальные.

После 25 декабря доступность не обнулилась, а закрепилась на уровне ниже 10%. Довести блокировку до полного нуля не удается по структурной причине: в России действует "слишком большое" число операторов связи, и ЦМУ ССОП не контролирует все узлы одинаково плотно. Часть

[50] По данным Mediascope (исследование Group4Media), в августе 2025 года месячный охват WhatsApp в России превысил 97 млн уникальных пользователей. Коммерсантъ, 22 сентября 2025. https://www.kommersant.ru/doc/8058240

трафика продолжает проходить через средства обхода, часть — из-за инцидентов маршрутизации, когда маршруты по ошибке или намеренно утекают в обход ТСПУ. С начала июня 2026 года на графике заметен постепенный рост: к концу месяца доступность поднялась примерно до 20–25%. Это отражает не смягчение политики, а адаптацию инструментов обхода, которым к лету 2026 года удалось частично восстановить связь.

3. Блокировка Telegram

10 февраля 2026 года РКН официально объявил о замедлении Telegram по всей стране, мотивируя это несоблюдением российского законодательства.[51] 16 марта Таганский суд Москвы оштрафовал Telegram на 35 млн рублей за отказ удалять запрещенный контент.[52]

Между официальным заявлением 10 февраля и фактической блокировкой в апреле прошло около двух месяцев — и это была не техническая пауза, а время открытого спора внутри самой лоялистской среды. Замедление Telegram вызвало необычно широкую волну критики: против выступили военнослужащие и Z-военкоры, депутаты Госдумы, провластные пропагандисты и представители духовенства. Лидер "Справедливой России" Сергей Миронов назвал авторов инициативы "идиотами", а военные утверждали, что ограничения бьют по фронтовой связи, для которой Telegram оставался ключевым каналом.[53] О недовольстве заявил и Владимир Соловьев, потерявший после замедления часть аудитории; аналитики называли происходящее первым заметным расколом в прокремлевских сообществах.[54] Реакция властей была половинчатой: Кремль публично преуменьшал опасения, а Минцифры пообещало не замедлять мессенджер "в зоне СВО".[55]

---

[51] РКН начал замедлять Telegram по всей России // РБК URL: https://www.rbc.ru/technology_and_media/10/02/2026/698afe729a79470c08a17b91

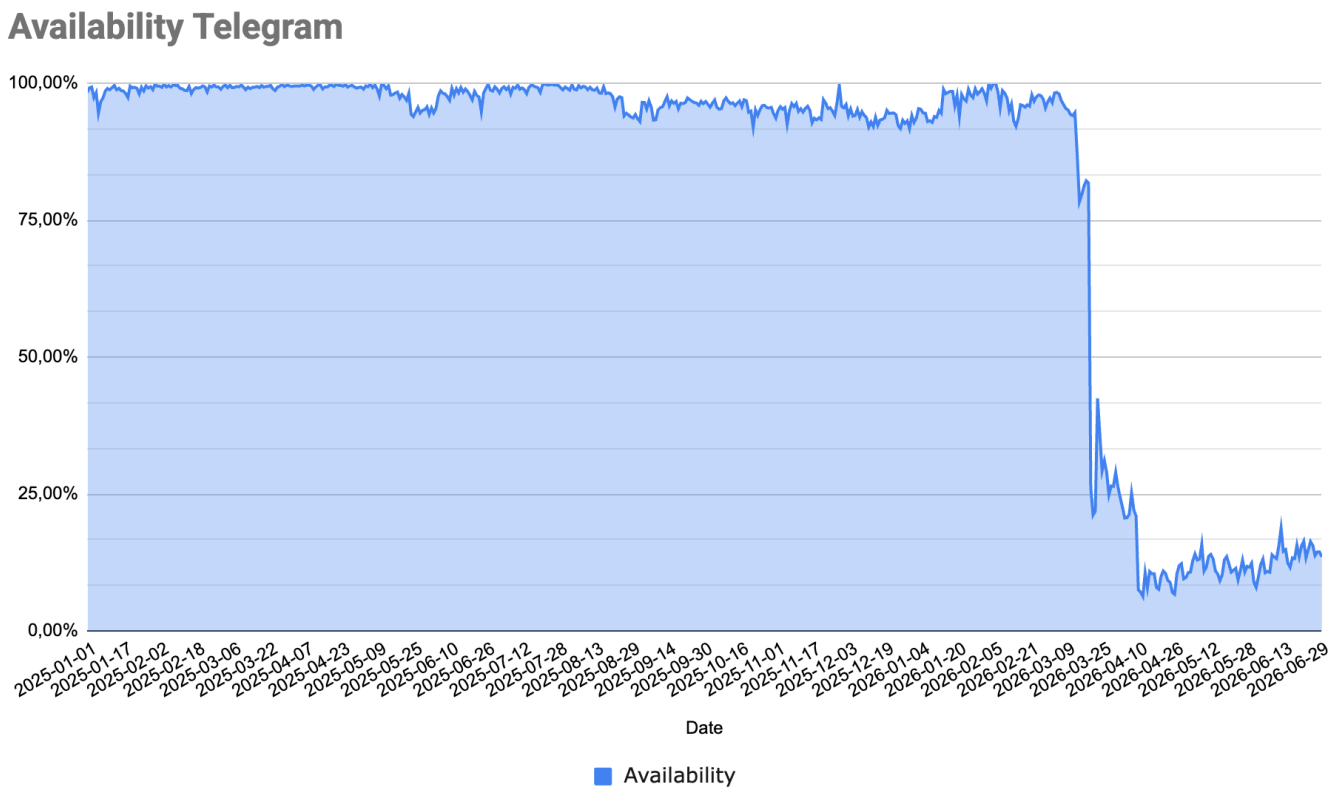
[52] Таганский суд Москвы оштрафовал Telegram на 35 млн рублей (пять эпизодов по ч. 4 ст. 13.41 КоАП) за отказ удалять запрещённый контент, 16 марта 2026 // Forbes URL: https://www.forbes.ru/society/557296-sud-v-moskve-ostrafoval-telegram-ese-na-35-mln-rublej

[53] Российские власти продолжают ломать телеграм и вотсап: критика Z-блогеров и депутатов Госдумы, Миронов назвал РКН "идиотами". Meduza, 14 февраля 2026. https://meduza.io/feature/2026/02/14/rossiyskie-vlasti-prodolzhayut-lomat-telegram-i-votsap

[54] Блокировка Telegram вызвала крупнейший раскол в лагере прокремлевских пропагандистов (Соловьев; оценка Татьяны Становой). The Moscow Times, 17 февраля 2026. https://ru.themoscowtimes.com/2026/02/17/kreml-shokiroval-provoennih-propagandistov-blokirovkoi-telegram-a187503

[55] Власти пообещали не замедлять Telegram в "зоне СВО" после критики военных и Z-военкоров; Песков преуменьшил опасения. The Moscow Times, 18 февраля 2026. https://ru.themoscowtimes.com/2026/02/18/vlasti-poobeschali-nezamedlyat-telegram-vzone-svo-posle-kritiki-voennih-iz-voenkorov-a187582

График 4. Блокировка Telegram, график доступности



Чем закончилась эта дискуссия, показывает сам факт блокировки. Ни возражения военных, ни жалобы пропагандистов, ни доводы о фронтовой связи не перевесили — Telegram все равно заблокировали. Значит, спор в очередной раз выиграл силовой блок, по всей видимости — вторая служба ФСБ, отвечающая за защиту конституционного строя, для которой контроль над каналом массовой коммуникации оказался важнее издержек, на которые указывали лоялисты.

Независимые измерения не только подтверждают деградацию, но и позволяют датировать ее фазы. На протяжении всего 2025 года и в первые недели марта 2026-го доступность Telegram держалась у отметки 100%, оставаясь в пределах обычных статистических колебаний. 15 марта показатель впервые опустился ниже 80% — первый выход за границы шума; в тот же день OONI фиксировал долю аномалий около 21%, а к 16 марта доля неудачных запросов к доменам мессенджера в среднем достигла почти 80%.[56] 20 марта доступность обрушилась примерно до 26%, после чего последовал частичный откат — короткое смягчение, характерное для ступенчатой и обратимой раскатки ограничений. Решающий обвал произошел 10 апреля: доступность упала ниже 10%, доля неудачных запросов приблизилась к 100%, а аномалии OONI достигли 95% — выше, чем у WhatsApp

[56] Резкое ухудшение доступности Telegram в России // Верстка URL: https://verstka.media/rezkoe-uhudshenie-dostupnosti-telegram-v-rossii

и Signal.[57] Для сравнения: WhatsApp был недоступен более чем на 85% измерений как минимум с 17 февраля.[58]

После 10 апреля доступность не обнулилась, а закрепилась на уровне ниже 10% с последующим медленным ростом — на графике заметно постепенное восстановление к лету 2026 года за счет адаптации средств обхода. Масштаб этой адаптации признавал и сам Telegram: по словам Павла Дурова, к апрелю 2026 года мессенджером ежедневно пользовались через VPN около 65 млн россиян, а более 50 млн отправляли сообщения каждый день.[59]

Здесь важна точность формулировок. Официально РКН нигде не объявлял "полную блокировку" Telegram — только "замедление" и "частичное ограничение" из-за нарушения закона. Сообщения о грядущей полной блокировке "в начале апреля" исходили от анонимных источников в ведомствах, на которые ссылался РБК, а не из опубликованного нормативного акта.[60] При этом фактический результат — невозможность нормально пользоваться сервисом — был достигнут техническими средствами, как и в случае с YouTube двумя годами ранее. Форма кривой это подтверждает: не разовое отключение по приказу, а управляемая деградация с фазой замедления, обвалом, откатом и закреплением на нижнем уровне. Для понимания масштаба: за 2025 год сам Telegram заблокировал 44 млн каналов и групп, что в 2,7 раза больше, чем годом ранее.[61]

Глава 6. Блокировка протоколов обхода

Пока шла кампания против мессенджеров, на техническом фронте разворачивалась новая фаза борьбы с VPN. Если в 2023 году ТСПУ научились распознавать классические протоколы (OpenVPN, WireGuard, IPsec), то в 2025–2026 годах под удар попали протоколы нового поколения, специально разработанные для маскировки под обычный трафик.

1. Конец "невидимых" протоколов

К концу 2025 года ТСПУ достигли практически полного покрытия сетей, а суммарная нагрузка на систему оценивалась в десятки терабит в секунду.[62] На этой базе РКН перешел к детектированию

[57] Хроника блокировки Telegram // Xakep URL: https://xakep.ru/2026/05/04/telegram-chronicle/
[58] OONI: недоступность WhatsApp в России превышает 85% как минимум с 17 февраля 2026 (для сравнения с деградацией Telegram); данные приводит Вёрстка со ссылкой на М. Климарёва // Вёрстка URL: https://verstka.media/rezkoe-uhudshenie-dostupnosti-telegram-v-rossii
[59] По заявлению Павла Дурова (апрель 2026), около 65 млн россиян ежедневно используют Telegram через VPN, более 50 млн отправляют сообщения каждый день // The Insider URL: https://theins.ru/news/291084
[60] Блокирование Telegram и WhatsApp в России // Википедия URL: https://ru.wikipedia.org/wiki/Блокирование_Telegram_и_WhatsApp_в_России
[61] Telegram за 2025 год заблокировал 44,085 млн каналов и групп — почти в 2,7 раза больше, чем в 2024 году // ТАСС URL: https://tass.ru/ekonomika/26125941
[62] Как РКН блокирует VLESS и другие протоколы // Habr URL: https://habr.com/ru/news/973082/

протоколов VLESS, REALITY, XTLS и Shadowsocks, которые до того считались устойчивыми к блокировкам.

24 ноября 2025 года появились первые сообщения о тестировании блокировки VLESS и инструментария XRay — жалобы шли из Красноярска, Новосибирска, Екатеринбурга, Казани, Волгограда. Удар пришелся по транспортному уровню, из-за чего пострадали и легитимные сервисы на обычном TLS.[63] К концу ноября жалобы охватили более десятка регионов, а в декабре РКН, обновив ТСПУ, начал блокировать SOCKS5, VLESS и L2TP. Это подтверждали независимые специалисты, в том числе Игорь Бедеров и Алексей Учакин.[64]

2. Как устроено детектирование

Принципиальное отличие новой фазы в том, что система перестала полагаться только на сигнатуры. По разборам специалистов, детектирование выстроено в несколько слоев, работающих одновременно:

1. Сигнатурный анализ первых байтов соединения. Самый простой слой: характерные последовательности в начале сессии позволяют сразу распознать и оборвать чистый Shadowsocks, OpenVPN и другие протоколы с узнаваемым рукопожатием.[65]
2. Фингерпринтинг TLS-рукопожатия (JA3/JA4). Система снимает отпечаток параметров TLS и отличает нестандартный клиент от рукопожатия обычного браузера, даже если содержимое зашифровано.
3. Активное зондирование (active probing). Сервера РКН (или их подрядчиков) обращаются к подозрительному серверу и проверяют, ведет ли он себя как настоящий веб-сайт или как прокси, отвечающий только на правильный ключ.
4. Анализ по IP, подсетям и репутации. Соединения с подсетями известных зарубежных хостеров (Hetzner, DigitalOcean, OVH) считаются подозрительными; при плохой репутации блокируются целые подсети дата-центров, а не отдельные адреса.
5. Поведенческий (статистический) анализ трафика. VLESS по содержимому неотличим от обычного HTTPS, поэтому его вычисляют по косвенным признакам: обращению к зарубежным IP-адресам дата-центров, несовпадению SNI и реального источника, нетипичным паттернам объема, направления и ритма трафика.[66]
6. "Завеса 16 КБ". Соединение обрывается после первых 15–20 килобайт, если оно установлено с подсетью известного зарубежного хостера.[67]

Это и есть реализация того самого "статистического метода", который первая часть описывала как

[63] РКН начал тестировать блокировку VLESS // Meduza URL: https://meduza.io/news/2025/11/24/
[64] РКН блокирует VLESS, SOCKS5 и L2TP // Xakep URL: https://xakep.ru/2025/12/05/rnk-vless/
[65] Как ТСПУ детектируют протоколы обхода // Habr URL: https://habr.com/ru/articles/1009542/
[66] РКН блокирует VLESS, SOCKS5 и L2TP // Xakep URL: https://xakep.ru/2025/12/05/rnk-vless/
[67] Памятка по блокировкам // Dept.one URL: https://dept.one/memo/blokirovky/

гипотезу: система не вскрывает шифрование, а вычисляет пользователя VPN по форме его сетевого поведения.

3. Индустрия блокировок: закупки и мощности

За технической эскалацией стоит не абстрактный "Роскомнадзор", а выстроенная индустрия с собственным подрядчиком и бюджетами. Ключевой интегратор систем суверенного интернета и поставщик ТСПУ — АО "ДЦОА" (Данные — центр обработки и автоматизации), созданное в 2019 году под закон о суверенном Рунете и подконтрольное Ростелекому через спецкомпанию "Градиент". Та же структура владеет и АО "РДП.РУ", ключевым разработчиком систем блокировок, и получила около 12 млрд рублей докапитализации и займов.[68]

В июне 2026 года ДЦОА объявило закупку не менее 154 российских серверов на 1,31 млрд рублей. Характеристики показывают направление развития: два процессора Intel Xeon Gold поколения Emerald Rapids на сервер, не менее 1 ТБ памяти DDR5, PCIe 5.0 с числом линий, достаточным для установки GPU. Последнее прямо указывает на подготовку к фильтрации трафика средствами машинного обучения. При этом серверы обязаны быть российского производства по реестру Минпромторга — но собраны на импортных процессорах Intel, поскольку отечественным комплектующим по производительности противопоставить нечего.[69]

Эта закупка объясняет и обратную сторону системы — почему блокировки не достигают 100%. Мощностей глубокой фильтрации хронически не хватает: объем трафика растет, методы обхода усложняются, и когда ТСПУ не справляются, включается режим bypass — трафик идет напрямую, мимо фильтра. Именно поэтому в середине марта 2026 года часть заблокированных ресурсов временно заработала. В ответ РКН усилил давление на операторов: с конца 2025 года по весну 2026-го десятки компаний получили крупные штрафы за то, что пускали часть трафика в обход ТСПУ. Само ведомство при этом наличие проблем с мощностью отрицало.[70]

Масштаб замысла виден из планов финансирования. Мощность ТСПУ к 2030 году должна вырасти в 2,5 раза, на федеральный проект закладывается около 84 млрд рублей, а целевая пропускная способность системы — 954 Тбит/с (для сравнения: средний трафик всего Рунета в 2024 году оценивался примерно в 30 Тбит/с). К концу 2026 года через систему планируется пропускать весь трафик российских пользователей. Отдельно около 40 млрд рублей выделяется структурам РКН, в том числе на борьбу с VPN, а система фильтрации на базе машинного обучения должна помочь

---

[68] Компания, отвечающая за блокировки Рунета, готовится к расширению: ДЦОА (Ростелеком) закупает не менее 154 серверов на 1,31 млрд рублей на базе Intel Xeon Gold; структура собственности (Градиент, РДП.РУ); дефицит мощностей, режим bypass, штрафы операторам за обход ТСПУ. CNews, 9 июня 2026. https://www.cnews.ru/news/top/2026-06-09_glavnyj_integrator_filtratsii

[69] -//-

[70] -//-

выявлять и запрещенный контент, и средства обхода.[71]

4. Чистка магазинов приложений

Параллельно шла атака на канал распространения самих средств обхода. Спрос при этом только рос: по данным на март 2026 года число скачиваний VPN-сервисов из топ-5 в Google Play выросло за год в 14 раз, до 9,2 млн, а всего за март 2025 — март 2026 зафиксировано 35,7 млн загрузок.[72] Давление на магазины приложений нарастало весь период. За 2025 год Apple удалила из российского App Store более 1200 приложений по требованиям российских властей, преимущественно VPN-сервисов.[73] К середине января 2026 года РКН ограничил доступ к 439 VPN-сервисам — на 70% больше, чем в октябре 2025 года.[74] 28 марта 2026 года из App Store были удалены сразу более двух десятков популярных VPN-клиентов (v2RayTun, Streisand, Happ и другие), что публично раскритиковал Павел Дуров.[75]

5. Гонка продолжается

17 февраля 2026 года блокировки VLESS резко усилились и охватили больше регионов и провайдеров. Сообщество обхода отреагировало переходом на новые транспорты — VLESS поверх XHTTP и gRPC, протоколы Hysteria2 и AmneziaWG.[76] Цикл "блокировка — обход — блокировка обхода", описанный в первой части, вышел на новый виток: теперь он идет уже не на уровне отдельных сервисов, а на уровне фундаментальных транспортных протоколов.

6. Проникновение VPN: модель и данные

Точное число пользователей VPN в России неизвестно — судить о нем по количеству скачиваний нельзя, поскольку один человек ставит несколько приложений, а установка не равна использованию. Поэтому приведенный график строится как оценочная модель: динамика поискового интереса по

---

[71] Планы по наращиванию мощности ТСПУ (рост в 2,5 раза к 2030 году, около 84 млрд рублей, целевые 954 Тбит/с), выделение около 40 млрд рублей структурам РКН на борьбу с VPN, система фильтрации на базе машинного обучения; рост числа скачиваний VPN в 14 раз год к году (данные Digital Budget). CNews, 9 июня 2026. https://www.cnews.ru/news/top/2026-06-09_glavnyj_integrator_filtratsii

[72] -//-

[73] Apple удалила более 1200 приложений из российского App Store // Meduza URL: https://meduza.io/video/2026/05/26/

[74] Павел Дуров раскритиковал Apple за блокировку VPN // Эксперт URL: https://expert.ru/news/pavel-durov-raskritikoval-apple-za-blokirovku-vpn

[75] Apple удалила популярные VPN-приложения по требованию РКН // Forbes Россия URL: https://www.forbes.ru/tekhnologii/558320

[76] Роскомнадзор усилил блокировку VLESS 17 февраля 2026 (охват регионов и провайдеров вырос); сообщество перешло на XHTTP/gRPC, Hysteria2 и AmneziaWG // The Moscow Times URL: https://ru.themoscowtimes.com/2026/02/17/roskomnadzor-usilil-blokirovku-odnogo-iz-populyarnih-vpn-protokolov-a187470

Google Trends и Yandex Wordstat служит опережающим индикатором, откалиброванным по данным опросов. На графике три ряда: поисковый интерес (Google Trends, синяя линия, нормирована так, что 100 пунктов — максимум за весь период), оценочное число пользователей в миллионах (красная линия) и уровень проникновения в процентах (желтые столбцы).

Методика расчетов: за точку отсчета взята оценка числа пользователей VPN до начала войны — порядка 1,6 млн человек в феврале 2022 года; после блокировки соцсетей этот показатель за несколько месяцев вырос примерно в пятнадцать раз, до 24 млн к маю 2022-го.[77] Дальше база наращивается помесячно: прирост за каждый месяц вычисляется из динамики поисковых запросов (Google Trends и Yandex Wordstat), умноженной на эмпирически подобранный коэффициент. Прямое сложение здесь недопустимо — нельзя просто прибавлять число запросов к числу пользователей, потому что один и тот же человек ищет способ обхода многократно, а всплеск запросов лишь частично конвертируется в новых пользователей. Коэффициент откалиброван по независимым оценкам аудитории на разные даты: помимо точек 2022 года, использованы данные Левада-центра за март 2024 года, по которым VPN хотя бы иногда пользовалась примерно четверть россиян,[78] и опрос Russian Field за апрель 2026 года с 40% активных пользователей.[79] Между этими опорными точками кривая интерполируется по поисковому сигналу.

[77] До начала войны VPN пользовались около 1,6 млн россиян (февраль 2022); после блокировки соцсетей число выросло примерно в 15 раз, до 24 млн к маю 2022 года. Радио Свобода, 7 июня 2022. https://www.svoboda.org/a/chislo-poljzovateley-vpn-vyroslo-v-15-raz-s-nachala-voyny/31886155.html

[78] По данным Левада-центра (март 2024), VPN хотя бы иногда пользуется около четверти россиян. Левада-центр, 14 июня 2024. https://www.levada.ru/en/2024/06/14/the-audience-of-internet-users-social-networks-messengers-and-vpn-services/

[79] Опрос Russian Field (15–22 апреля 2026, 1600 респондентов): 40% россиян активно пользуются VPN, 74% осведомлены о технологии, в Москве — 62%, в Санкт-Петербурге — 58%. SecurityLab, 6 мая 2026. https://www.securitylab.ru/news/572416.php

График 5. Google Trends и проникновение VPN

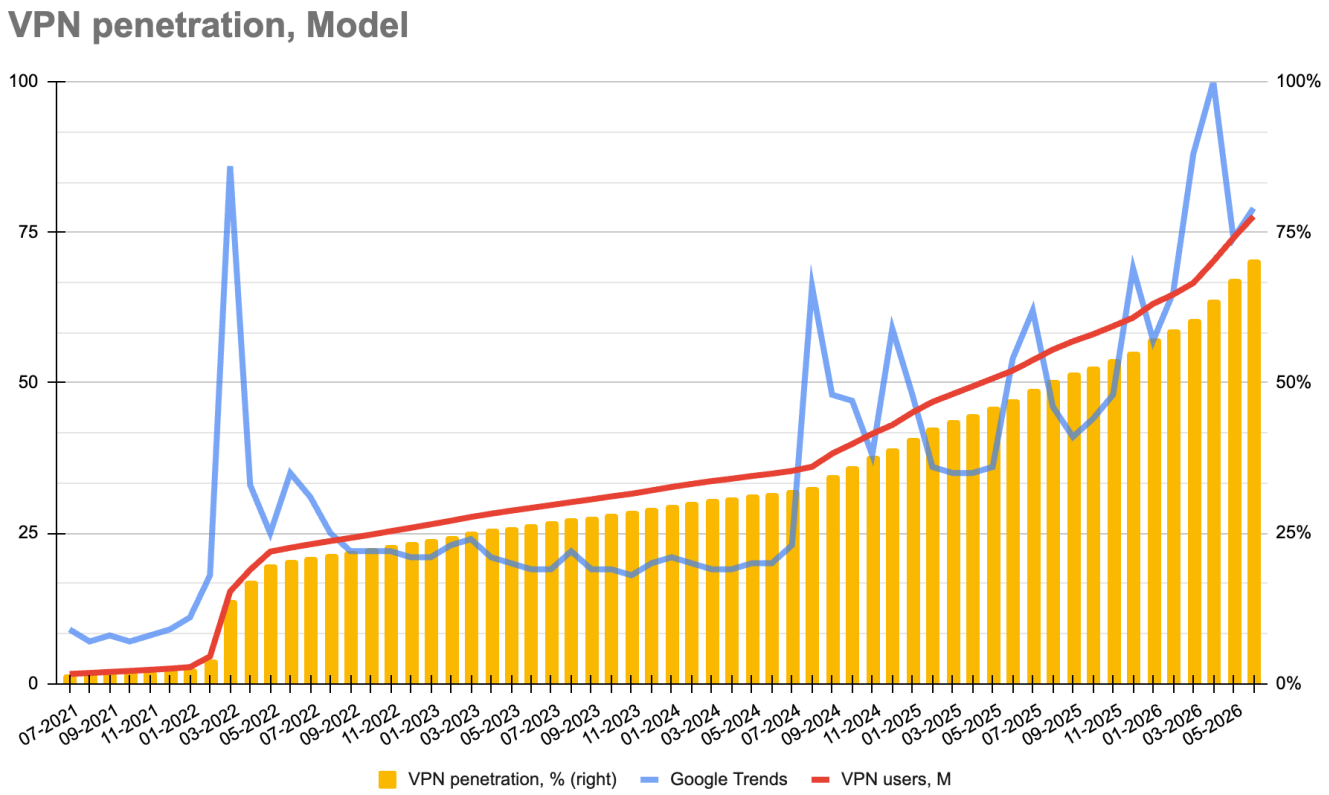


График делится на три характерных периода, и каждый совпадает с крупной волной блокировок.

Первый резкий всплеск — март 2022 года, блокировка социальных сетей после начала войны, в первую очередь Instagram. Поисковый интерес взлетает почти до 90 пунктов. Именно с этого момента прежде пологая красная линия меняет угол наклона и начинает уверенно расти, увлекая за собой и проценты проникновения. После пика интерес в поиске спадает, но база пользователей не откатывается: до середины 2024 года держится плато.

Вторая серия волн — июль 2024 — июль 2025 года, замедление и блокировка YouTube. Летом 2024-го синяя линия снова идет вверх (примерно до 68 пунктов), затем следуют новые всплески осенью 2024-го и в начале 2025-го. На этом фоне рост реальной базы ускоряется: красная линия преодолевает отметку в 50 млн, а проникновение переходит за 50%.

Третий период — весна 2026 года, блокировка Telegram. Поисковый интерес достигает 100 пунктов, максимума всей шкалы, после чего к лету происходит откат примерно до 80. Этот всплеск выводит потребление на новый уровень: к июню 2026 года оценочное число пользователей приближается к 70 млн, а проникновение — к 65–68%.

Модель подтверждается независимыми данными. По опросу Russian Field (апрель 2026 года), VPN активно пользуются 40% россиян, о технологии осведомлены 74%, а в Москве доля пользователей достигает 62%; среди граждан 18–45 лет о регулярном использовании заявляли более половины.[80][81] Более ранние замеры дают тот же порядок величины и ту же однонаправленную динамику: около трети по данным Левада-центра и 46% по данным Института социального маркетинга признавали, что хотя бы раз пользовались VPN.[82] Опережающий индикатор модели тоже верифицируется: в марте 2026 года число поисковых запросов о VPN выросло примерно в 3,3 раза год к году, причем Yandex Wordstat и Google Trends показали согласованную картину, а пиковые значения оказались сопоставимы с уровнем весны 2022 года.[83]

Общий вывод модели прост: краткосрочные триггеры формируют долгосрочную привычку. Как только медийный шум вокруг очередной волны блокировок утихает и синяя линия идет вниз, красная линия и желтые столбцы не возвращаются к прежним значениям — они движутся только вверх. Каждая новая блокировка не сокращает аудиторию обхода, а расширяет ее, закрепляя VPN в статусе повседневного инструмента для большинства пользователей. В этом и состоит структурный парадокс политики: борьба с обходом блокировок сама выступает главным драйвером его распространения.

Глава 7. Контроль периметра

Технические меры против VPN дополнялись правовыми и административными — причем государство перенесло часть работы по цензуре на самих пользователей, на бизнес и на инфраструктуру. Параллельно достраивался контроль над всей цепочкой: кто публикует, кто рекламирует, где размещается контент и кто вообще выходит в сеть.

1. Наказание за поиск экстремизма (281-ФЗ)

31 июля 2025 года был подписан Федеральный закон № 281-ФЗ, вступивший в силу 1 сентября 2025 года.[84] Он ввел в КоАП статью о штрафах за умышленный поиск "заведомо экстремистских материалов" из реестра Минюста, в том числе с использованием VPN: для граждан — от 3 до 5

---

[80] Опрос Russian Field (15–22 апреля 2026, 1600 респондентов): 40% россиян активно пользуются VPN, 74% осведомлены о технологии, в Москве — 62%, в Санкт-Петербурге — 58%. SecurityLab, 6 мая 2026. https://www.securitylab.ru/news/572416.php

[81] Страна победившего VPN: по данным Russian Field на апрель 2026 года более 50% россиян 18–45 лет пользуются VPN; обзор оценок (Левада-центр, Институт социального маркетинга) и цели РКН по эффективности блокировок. Carnegie, 28 мая 2026. https://carnegieendowment.org/ru/russia-eurasia/politika/2026/05/russia-vpn-usage-political

[82] -//-

[83] В марте 2026 года поисковый интерес к VPN достиг пятилетнего рекорда (Google Trends — 100 баллов); данные Яндекс Вордстат согласуются с Google Trends, комментарий М. Климарёва // The Moscow Times URL: https://ru.themoscowtimes.com/2026/03/30/rossiyane-postavili-rekord-po-zaprosam-o-vpn-v-google-a191239

[84] Подписан закон о штрафах за поиск экстремистских материалов // Pravo.ru URL: https://pravo.ru/news/259848/

тысяч рублей. К моменту вступления закона в силу реестр насчитывал свыше 5400 записей; глава Минцифры подчеркивал, что наказывать будут только за умышленный просмотр, а доказывать умысел — задача правоохранителей.[85]

Тот же пакет резко ужесточил ответственность за рекламу средств обхода блокировок: за рекламу VPN штрафы для граждан составили от 50 до 80 тысяч рублей, для должностных лиц — до 150 тысяч, для юридических лиц — до 500 тысяч (при повторе — до миллиона).[86] Отдельным законом использование VPN при совершении преступления было признано отягчающим обстоятельством.[87]

Принципиальная новизна здесь в смещении объекта репрессии: наказуемым стало не только распространение запрещенного, но и само действие пользователя по поиску информации — впервые ответственность переносится на конечного потребителя контента.

На практике, однако, массового применения статья не получила. Несмотря на то что закон действует с 1 сентября 2025 года, а реестр Минюста насчитывает свыше 5400 записей, за все время известен по сути лишь один случай реального наказания. В декабре 2025 года мировой суд Каменска-Уральского оштрафовал на 3 тысячи рублей 20-летнего Сергея Глухих — по версии следствия, он искал в браузере изображение шеврона батальона "Азов".[88]

Обстоятельства этого единственного дела показательны. Инициатором выступила не автоматическая система, а ФСБ: фигурант, по признанию сотрудника спецслужбы, давно был "в поле зрения", а протокол составили по обращению неустановленного лица.[89] Защита указывала, что шеврон "Азова" стоит в списке экстремистских материалов на 3269-м месте — запомнить, что именно запрещено искать, невозможно, а запрос из четырех букв выдает и Азовское море, и города. Это обнажает встроенное противоречие нормы: ни оператор связи, ни РКН технически не видят содержания поисковых запросов — ТСПУ умеют лишь блокировать типы трафика. Установить умысел и вообще узнать о запросе можно только через изъятие устройства и оперативную работу спецслужб. Поэтому статья работает не как инструмент сплошного контроля, а как избирательное, демонстративное оружие точечного давления — угроза, адресованная всем, но применяемая выборочно.

---

[85] Штрафы за поиск экстремистских материалов вступили в силу // РБК URL: https://www.rbc.ru/society/01/09/2025/68b03edf9a79470b449c7b8e

[86] Путин подписал закон о штрафах за рекламу VPN (для граждан 50–80 тыс. руб.) и о признании использования VPN при совершении преступления отягчающим обстоятельством (ст. 63 УК); оба закона от 31.07.2025, вступление 01.09.2025 // Forbes URL: https://www.forbes.ru/society/543070-putin-podpisal-zakon-o-strafah-za-poisk-ekstremistskih-materialov-i-reklamu-vpn

[87] -//-

[88] В России впервые оштрафовали за поиск экстремистских материалов: мировой суд Каменска-Уральского назначил 3 тысячи рублей 20-летнему Сергею Глухих (ст. 13.53 КоАП). РБК, 10 декабря 2025. https://www.rbc.ru/politics/10/12/2025/6939684f9a7947ac893c161e

[89] Обстоятельства дела: инициатива ФСБ, фигурант давно был "в поле зрения", протокол по обращению неустановленного лица; аргументы защиты о невозможности установить умысел. Радио Свобода, 10 декабря 2025. https://www.svoboda.org/a/v-rf-naznachen-pervyy-shtraf-za-poisk-ekstremistskih-materialov-/33619184.html

2. Отключение Apple

Чтобы понять смысл этой меры, нужно вспомнить, как устроена оплата в экосистеме Apple в России. До 2022 года пользователи платили за приложения, подписки и место в iCloud обычными банковскими картами. В апреле 2022 года, после ухода Visa и Mastercard, Apple перестала принимать карты российских банков, включая Мир, — прямая оплата картой стала невозможна. На следующие четыре года основным каналом осталось пополнение баланса Apple ID со счета мобильного телефона: пользователь заходил в профиль App Store, указывал сумму, и деньги списывались с баланса. МТС и Билайн предоставляли эту услугу напрямую, МегаФон и Т2 — через партнеров. Не требуя зарубежных карт и сторонних сервисов, этот способ стал массовым.[90]

Именно по нему и был нанесен удар. Прямое удаление VPN-приложений из магазинов, описанное в предыдущей главе, не останавливало пользователей окончательно, поэтому власти зашли с финансовой стороны. По итогам совещания Шадаева с операторами связи в конце марта, с 1 апреля 2026 года МТС, Билайн, МегаФон и Т2 отключили возможность пополнять баланс Apple ID со счета мобильного телефона. Цель формулировалась прямо — вынудить Apple вернуть удаленные приложения, перекрыв компании платежный канал в России.[91] После отключения у пользователей остались в основном подарочные карты Apple для российского региона и обходные схемы со сменой региона и зарубежными картами.

3. Цензура руками корпораций

Наиболее показательным новшеством стало принуждение российских IT-компаний самостоятельно выявлять и ограничивать пользователей VPN. В конце марта — начале апреля 2026 года Минцифры провело совещания более чем с двадцатью платформами (Сбер, Яндекс, VK, Wildberries, Ozon, Авито, 2ГИС, ivi и другими), разослало методичку по выявлению VPN и установило срок внедрения ограничений — 15 апреля.[92]

15 апреля 2026 года Ozon, Wildberries, Кинопоиск, ivi, Яндекс Пэй и ряд других сервисов перестали полноценно работать при включенном VPN.[93] Механизм прост: приложение отправляет IP-адрес

---

[90] С апреля 2022 года, после отказа Apple принимать карты российских банков, оплата со счета мобильного телефона стала основным способом пополнения Apple ID; МТС и Вымпелком (Билайн) предоставляли услугу напрямую, Т2 и МегаФон — через партнеров. Forbes, 1 апреля 2026. https://www.forbes.ru/tekhnologii/558358-kartocnaa-sistema-kak-popolnit-balans-apple-id-bez-ucastia-operatorov-svazi

[91] Россиянам запретят оплачивать сервисы Apple с баланса телефона // Meduza URL: https://meduza.io/cards/rossiyanam-hotyat-zapretit-oplachivat-servisy-apple

[92] Минцифры обязало IT-компании выявлять пользователей VPN // Habr URL: https://habr.com/ru/news/1018576/

[93] С 15 апреля 2026 года Ozon, Wildberries, Кинопоиск, ivi, Яндекс Пэй и другие сервисы перестали работать при включённом VPN по требованию Минцифры // Meduza URL: https://meduza.io/feature/2026/04/15/krupneyshie-rossiyskie-servisy-perestayut-rabotat-pri-vklyuchennom-vpn-kak-i-trebovalo-mintsifry

клиента на сервер и сверяет его с базами VPN и прокси. Исследование проекта RKS Global показало, что 22 из 30 популярных Android-приложений отслеживают использование VPN, и большинство из них передает этот статус на свои серверы.[94]

Это новый виток войны с VPN — и, вероятно, самый тревожный за всю историю цензурных технологий. Прежде государство блокировало трафик собственными руками, силами ТСПУ и менеджеров РКН. Теперь оно делегировало детектирование тем, кто заведомо делает это лучше: инженеры Сбера, Яндекса или Ozon по квалификации превосходят операторов государственной системы, их приложения стоят на десятках миллионов устройств и уже собирают данные о клиентах. Государству больше не нужно догонять обходные технологии — достаточно заставить работать на цензуру тех, кто эти технологии понимает.

Принуждение при этом построено на рычаге, аналога которому в истории цензуры не было. За отказ внедрять детектирование VPN компании грозит исключение из белых списков и лишение IT-аккредитации.[95] Но аккредитация — это не только налоговые льготы: именно она дает сотрудникам отсрочку от призыва и бронь от мобилизации, и с ее потерей отсрочка аннулируется для всех работников разом.[96] То есть невыполнение требований РКН превращается в прямую угрозу отправить на войну весь мужской призывной состав компании. Цензура впервые обеспечивается не штрафом и не блокировкой, а риском мобилизации сотрудников: государство принуждает бизнес к соучастию, ставя на кон не прибыль, а жизни его работников.

Для самих компаний это оборачивается и прямыми издержками. По оценкам отраслевых аналитиков, потери маркетплейсов от ограничения VPN-пользователей исчислялись миллиардами рублей, а трафик приложений просел на единицы процентов.[97]

4. Запрет рекламы на запрещенных ресурсах

7 апреля 2025 года был подписан Федеральный закон № 72-ФЗ, вступивший в силу 1 сентября 2025 года: он дополнил статью 5 закона "О рекламе" новой частью 10.7 и запретил рекламу на ресурсах нежелательных, экстремистских и террористических организаций, а также на любых платформах, доступ к которым ограничен в России, — в первую очередь в Instagram и Facebook (Meta признана в России экстремистской), а также в X (бывший Twitter). Критерии того, что считать рекламой на таких ресурсах, правительство закрепило постановлением № 1087 от 24 июля 2025 года.[98]

---

[94] 22 из 30 приложений отслеживают VPN: исследование // Habr URL: https://habr.com/ru/articles/1021392/
[95] Минцифры обязало IT-компании выявлять пользователей VPN // Habr URL: https://habr.com/ru/news/1018576/
[96] Государственная аккредитация IT-компании даёт сотрудникам право на отсрочку от призыва (Указ Президента № 83 от 02.03.2022; правила — ПП № 490 от 28.03.2022); при отзыве аккредитации право аннулируется // ГАРАНТ URL: https://www.garant.ru/consult/military/1717264/
[97] Потери бизнеса от ограничения VPN-пользователей // Forbes Россия URL: https://www.forbes.ru/biznes/560978
[98] Запрет рекламы на запрещенных ресурсах (ФЗ № 72-ФЗ, ч. 10.7 ст. 5 закона "О рекламе", вступление 1 сентября 2025; критерии — ПП № 1087 от 24.07.2025) // Гарант.ру URL: https://www.garant.ru/article/1845542/

Запрет охватывает не только прямые интеграции, но и любые публикации с рекламным подтекстом — посты, сторис, рилсы, обзоры и распаковки, если в них есть признаки продвижения товара; бартер и бесплатное размещение приравниваются к платной рекламе. Ответственность несут одновременно рекламодатель и рекламораспространитель. Штрафы установлены по статье 14.3 КоАП: для граждан — от 2 до 2,5 тысячи рублей, для должностных лиц и индивидуальных предпринимателей — от 4 до 20 тысяч, для юридических лиц — от 100 до 500 тысяч рублей за каждое размещение.[99] Отдельно юристы указывают на риск уголовного преследования по статье 282.3 УК (финансирование экстремизма), если оплата рекламы проходит через структуры Meta.[100]

Старые публикации удалять не требуется, но за действия по их повторному распространению — репост, закрепление, простановку ссылок — наказывают наравне с новой рекламой. Это подтверждали и Роскомнадзор, и ФАС.[101]

С первых недель правоприменение стало показательным — знакомым по норме о поиске экстремизма: удар пришелся не по крупным рекламодателям, а по отдельным блогерам, причем составы оказались спорными. Первый известный штраф — 30 тысяч рублей — получила блогер-юрист Евгения Тутушкина из Краснодара за рилс об отеле с промокодом, опубликованный еще летом 2025 года; формально ее наказали за отсутствие маркировки, но публично это стало прецедентом наказания за рекламу в запрещенной сети.[102] Первое дело собственно по новому запрету омское УФАС возбудило 22 октября 2025 года против инфлюенс-продюсера Аси Сивоконевой (21 тысяча подписчиков): поводом стал ироничный ролик с распаковкой косметики под названием "Все блогеры после 1 сентября", где бренды упоминались без прямого названия. Ее решили оштрафовать дважды — и как рекламодателя, и как рекламораспространителя.[103]

Экономический смысл запрета прозрачен: он бьет по доходной базе неподконтрольных площадок и перенаправляет рекламные бюджеты на отечественные сервисы — VK, Rutube, Дзен. По мере блокировки новых сервисов ограничение распространялось и на них. 5 марта 2026 года ФАС признала нарушением рекламу в Telegram и на YouTube, сославшись на введенные Роскомнадзором ограничения доступа. Однако уже 25 марта, после негативной реакции рынка, ведомство объявило для этих двух площадок переходный период: до конца 2026 года меры ответственности за рекламу в них применяться не будут. На Instagram, Facebook и VPN-сервисы отсрочка не распространяется —

---

[99] Штрафы за рекламу в Instagram и ответственность рекламодателя и рекламораспространителя (ст. 14.3 КоАП) // РБК URL: https://www.rbc.ru/life/news/67e2964c9a794762d0a5ffe3

[100] Риск уголовной ответственности по ст. 282.3 УК при оплате рекламы через Meta // Contra Legal Firm URL: https://contralegal.ru/ru/articles/analitika/instagram-pod-zapretom-kakie-shtrafy-groziat-biznesu-i-kak-minimizirovat-riski

[101] Реклама, размещенная до 1 сентября: удаление необязательно, но повторное распространение — нарушение // Гарант.ру URL: https://www.garant.ru/article/1845542/

[102] Первый штраф за рекламу в Instagram — блогер Евгения Тутушкина, 30 тыс. рублей // Forbes URL: https://www.forbes.ru/forbeslife/548314-v-rossii-vpervye-naznacili-straf-za-reklamu-v-instagram

[103] Первое дело ФАС по новому запрету — блогер Ася Сивоконева, Омское УФАС, дело № 055/05/18.1-1292/2025 // ADPASS URL: https://adpass.ru/pervoe-delo-za-reklamu-v-instagram-2025/

там запрет действует в полную силу.[104]

5. Регулирование хостинг-провайдеров

Реестр хостинг-провайдеров, без включения в который оказывать услуги в России запрещено, действует с 1 февраля 2024 года; формировать его Роскомнадзор начал в декабре 2023-го.[105] К апрелю 2026 года в нем числилось около 566 организаций.[106] Условия пребывания в реестре жесткие: идентификация клиентов, подключение к государственной системе ГосСОПКА, размещение оборудования СОРМ (без которого следует исключение), использование точек обмена трафиком из официального реестра и размещение инфраструктуры в России.[107]

С 1 января 2026 года эти требования подкреплены административной ответственностью: Федеральный закон № 508-ФЗ от 28 декабря 2025 года ввел штрафы до одного миллиона рублей за оказание хостинга вне реестра и запретил государственным и муниципальным органам размещать свои системы у нереестровых провайдеров.[108] Издержки регулирования ложатся на рынок и в конечном счете на клиентов: по оценке главы RUVDS Никиты Цаплина, подорожание оборудования, рост НДС и внедрение СОРМ за счет самих хостеров уже подняли стоимость услуг более чем на 30 процентов, а интеграция с базами Роскомнадзора приведет к новому росту цен и вытеснению мелких игроков.[109]

Отдельно стоит выделить превращение хостеров в инструмент "антифрода". Практика отрабатывалась вручную еще до принятия закона: с конца 2025 года Роскомнадзор рассылал провайдерам списки IP-адресов из их собственных сетей с требованием удалить размещенные там VPN-серверы в течение 24 часов — иначе блокировке подлежала вся подсеть. Показательно, что система научилась находить и обфусцированные протоколы (Xray, VLESS) в "чистых" подсетях, где прежде не запускали легко детектируемые OpenVPN и WireGuard. Весной 2026 года эту практику закрепили законодательно: поправки, известные как "Антифрод 2.0", распространили на всех

---

[104] ФАС о рекламе в Telegram и на YouTube: признание нарушением (5 марта) и переходный период до конца 2026 года // Forbes URL: https://www.forbes.ru/tekhnologii/557924-fas-ob-avila-perehodnyj-period-dla-reklamy-v-telegram-i-youtube

[105] Реестр провайдеров хостинга: работа вне реестра запрещена с 1 февраля 2024 года // Роскомнадзор URL: https://rkn.gov.ru/press/news/news74803.htm

[106] В реестре около 566 организаций (апрель 2026) // Forbes URL: https://www.forbes.ru/tekhnologii/559360-uznal-o-vozmoznom-uzestocenii-trebovanij-k-hosting-provajderam-dla-bor-by-s-vpn

[107] Требования к реестровым хостерам: идентификация, ГосСОПКА, СОРМ, точки обмена трафиком, локация в РФ // Хабр (ispmanager) URL: https://habr.com/ru/companies/ispmanager/articles/818525/

[108] Штрафы до 1 млн рублей за хостинг вне реестра и запрет госорганам (ФЗ № 508-ФЗ от 28.12.2025) // Law.ru URL: https://www.law.ru/news/44280-vstupil-v-silu-zakon-o-shtrafah-do-1-mln-rubley-dlya-hosting-provayderov-ne-iz-reestra-rkn

[109] Рост цен на услуги хостинга более чем на 30% из-за СОРМ, НДС и интеграции с базами РКН (Н. Цаплин, RUVDS) // The Insider URL: https://theins.ru/news/291587

участников реестра обязанность самостоятельно выявлять и отключать клиентов, чьи мощности используются для обхода блокировок. Это меняет саму модель ответственности хостера — от реакции на жалобу к упреждающей проверке: провайдер больше не может ссылаться на нейтральный статус технической площадки.[110]

Параллельно ужесточился контроль над инфраструктурным уровнем в целом. Летом 2026 года Роскомнадзор перешел от блокировки отдельных адресов к веерному ограничению целых подсетей и автономных систем дата-центров — под фильтр попали площадки как зарубежных (Leaseweb), так и российских провайдеров (Selectel, Яндекс Облако, Cloud.ru, Beget), ранее считавшихся безопасными.[111]

В итоге, хостинг-уровень из нейтральной технической прослойки превратился в полноценный инструмент контроля, работающий сразу в трех измерениях. Реестр решает, кто вообще вправе оказывать услуги; СОРМ и ГосСОПКА встраивают в каждого провайдера точку наблюдения; обязанность искать и отключать VPN делает хостера соучастником цензуры. Это тот же прием, что и с маркетплейсами и банками из предыдущих разделов: государство перекладывает саму работу по фильтрации на бизнес, оставляя себе роль контролера. Побочный эффект предсказуем — консолидация рынка, рост цен и уход мелких провайдеров, то есть плата за контроль, переложенная на инфраструктуру и ее клиентов.

6. Запрет авторизации через “иностранные сервисы”

В июле 2023 года в России был принят Федеральный закон номер 406-ФЗ, запрещающий регистрацию на российских сайтах с использованием иностранных систем авторизации, включая зарубежные почтовые службы вроде Gmail или Apple ID. Изначально ограничение вступило в силу с 1 декабря 2023 года. Согласно установленным нормам, легальными способами регистрации и входа для пользователей в Рунете остались только российский номер телефона, портал Госуслуг, Единая биометрическая система либо иная информационная система, контролируемая гражданином РФ или российским юридическим лицом.[112]

В июне 2026 года регулирование перешло в практическую плоскость: был подписан Федеральный закон номер 199-ФЗ, вводящий административную ответственность за несоблюдение этих требований.[113] Наказание накладывается непосредственно на владельцев интернет-ресурсов,

---

[110] Обязанность реестровых хостеров выявлять и отключать VPN-клиентов ("Антифрод 2.0"); ручные предписания РКН с 24-часовым сроком; обнаружение обфусцированных протоколов // te-st.org URL: https://te-st.org/2026/05/12/hostingrules/

[111] Веерная блокировка подсетей и автономных систем дата-центров, июнь 2026 // Хабр URL: https://habr.com/ru/articles/1044396/

[112] Требования к авторизации пользователей на российских сайтах (ФЗ № 406-ФЗ от 31.07.2023, вступление в силу 1 декабря 2023) // КонсультантПлюс URL: https://www.consultant.ru/law/hotdocs/81325.html

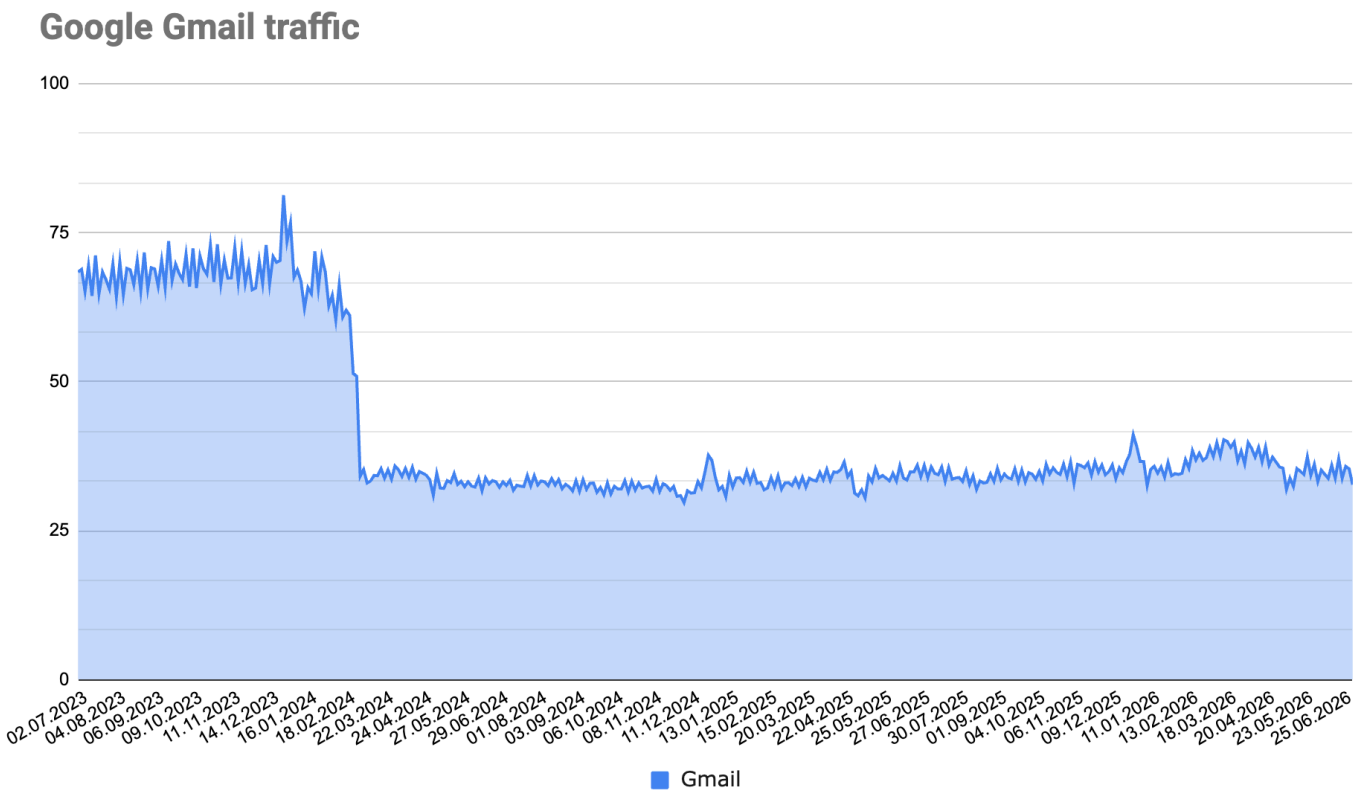
[113] Административная ответственность за нарушение правил авторизации (ФЗ № 199-ФЗ от 26.06.2026, ст. 13.55 КоАП, вступление в силу 7 июля 2026) // Гарант.ру URL: https://www.garant.ru/article/2136195/

которые продолжают предоставлять возможность авторизации через запрещенные зарубежные сервисы. Штрафы для юридических лиц составляют от 500 до 700 тысяч рублей, для должностных лиц — от 30 до 50 тысяч рублей, а для физических лиц (собственников сайтов) — от 10 до 20 тысяч рублей.[114]

Для обычных граждан прямых штрафов за использование зарубежных ящиков закон не предусматривает.[115] Тем не менее, жесткие санкции для бизнеса вынуждают российские платформы, интернет-магазины и государственные порталы массово отключать кнопки входа через Google ID или Apple ID и принудительно требовать от пользователей перепривязать аккаунты на отечественные e-mail адреса (Mail.ru, Яндекс) или номера телефонов, что планомерно изолирует иностранные почтовые сервисы от российской цифровой инфраструктуры.

[114] Размеры штрафов за авторизацию через иностранные сервисы // Ведомости URL: https://www.vedomosti.ru/society/news/2026/06/09/1204637-shtrafi-za-avtorizatsiyu
[115] Штрафы касаются владельцев сайтов, а не пользователей иностранной почты // 360.ru URL: https://360.ru/tekst/obschestvo/fejk-v-rossii-vvodjat-shtrafy-za-avtorizatsiju-na-sajtah-cherez-inostrannuju-pochtu/

График 6. Трафик Gmail в России, 2023–2026



На графике — динамика трафика Gmail в России, нормированная к 100. Из него следуют три вывода. Первый: с почтой проблем не было ни до войны, ни в первые её годы — весь 2023 год Gmail и другие иностранные ящики работали свободно, и кривая держится высоко, в коридоре 65–75 пунктов. Второй: решающим оказался запрет 2023 года — по мере его практического применения трафик в начале 2024 года падает почти вдвое, примерно с 62 до 33 пунктов, и закрепляется на этом уровне. Третий: введение штрафов в 2026 году на использовании Gmail не отразилось — после обвала 2024 года линия идёт ровным плато до середины 2026-го, без нового спада.

7. Антифродовые пакеты и оплата обхода

Параллельно с техническим и правовым давлением на VPN государство выстроило третий контур — финансовый. Формально он оформлен как борьба с мошенничеством: за 2025–2026 годы приняты два больших пакета мер против телефонного и кибермошенничества. Первый (апрель 2025 года) вводил обязательную верификацию звонков, ограничение числа сим-карт в одни руки и запрет использовать зарубежные мессенджеры для связи госорганов и банков с клиентами. Второй,

известный как "Антифрод 2.0", пошел дальше.[116] Он ограничил число банковских карт двадцатью на человека во всех банках сразу, ввел единую систему их учета и "период охлаждения" — право банка на шесть часов задержать подозрительный перевод.[117] В тот же пакет вошли запрет расторгать договор связи раньше чем через 90 дней, база IMEI для блокировки устройств "по железу" и "красная кнопка" для жалоб через Госуслуги и мессенджер MAX.[118]

Официальная логика понятна: лимиты на сим-карты и карты бьют по "дропперским" схемам, когда мошенники используют десятки подставных номеров и счетов, чтобы обналичивать украденное и запутывать следы. Но ровно та же инфраструктура — множество анонимных сим-карт, десятки карт, быстрые переводы между людьми — после 2022 года стала основным способом оплаты зарубежных сервисов, недоступных для прямой оплаты российской картой. После ухода Visa и Mastercard платежи за иностранные подписки, аренду серверов и VPN держатся именно на "серых" рельсах: пополнение с баланса телефона, пулы карт, переводы через посредников и криптовалюта. Ограничивая число сим-карт и карт, деанонимизируя каждый платеж и получая право замораживать переводы, государство перекрывает не столько канал вывода краденого, сколько канал оплаты обхода.

Что мишенью служит именно обход, а не только мошенничество, показывает состав самого пакета. В "Антифрод 2.0" прямо включен запрет хостинг-провайдерам предоставлять ресурсы для размещения VPN-сервисов — мера, не имеющая отношения к телефонным аферам, но полностью укладывающаяся в антивпновскую кампанию предыдущих глав.[119] Антимошеннический закон, таким образом, служит носителем для нормы, которая по существу принадлежит не финансовому, а цензурному контуру.

Прецедент был отработан заранее и описан выше — в разделе о "налоге на Apple", когда операторы по требованию властей отключили пополнение Apple ID с баланса телефона, чтобы перекрыть платежный канал и вынудить Apple вернуть удаленные VPN-приложения. Антифродовые пакеты обобщают этот прием: если технически заблокировать VPN не удается, а юридически преследовать пользователя трудно, остается сделать оплату обхода дорогой, редкой и прослеживаемой.

При этом заявленной цели меры достигают плохо. Мошеннический рынок они не уничтожают, а лишь повышают стоимость расходников — сим-карт и дроп-аккаунтов — и загоняют схемы глубже в тень. Зато законопослушный пользователь получает деанонимизацию платежей, задержки переводов и лимиты на привычные сервисы. Итог тот же, что и во всей главе: под вывеской безопасности

---

[116] Второй антифрод-пакет "Антифрод 2.0": состав, принятие Госдумой 9 июня и подписание 26 июня 2026 года // Коммерсантъ URL: https://www.kommersant.ru/doc/8728414
[117] Лимит 20 банковских карт на человека во всех банках и "период охлаждения" 6 часов // РИА Новости URL: https://ria.ru/20260609/gosduma-2097923590.html
[118] База IMEI, "красная кнопка" через Госуслуги и MAX, запрет расторгать договор связи ранее 90 дней // SecurityLab URL: https://www.securitylab.ru/news/574218.php
[119] Запрет хостинг-провайдерам предоставлять ресурсы для размещения VPN-сервисов в составе антифрод-пакета // Коммерсантъ URL: https://www.kommersant.ru/doc/8728414

выстраивается инфраструктура контроля, а реальная нагрузка ложится не на преступника, а на обычного человека и на его способность платить за доступ к свободному интернету.

Глава 8. Разделение интернета

Самым стратегически значимым направлением 2026 года стала попытка разделить трафик на внутренний и международный — то есть подступиться к той самой изоляции, которую первая часть описывала как финальную стадию лестницы. В основе замысла лежит признание технического предела: заблокировать VPN методом фильтрации не удается, поскольку для сплошного детектирования нужны все большие вычислительные мощности, а вероятность ложных срабатываний DPI при ужесточении правил приближается к единице. Отсюда смена подхода — от технического подавления к экономическому сдерживанию. Задача формулируется так: сделать обход заведомо дорогим, не отключая зарубежный трафик полностью, поскольку он необходим для доступа к деловым и технологическим сервисам, обновлений программного обеспечения и внешнеэкономической деятельности. Отсюда два параллельных механизма — лимит на международный трафик в мобильных сетях и мораторий на расширение трансграничных каналов.

1. Плата за международный трафик в мобильных сетях

28 марта 2026 года на совещании с операторами связи Максут Шадаев предложил ввести плату за международный трафик в мобильных сетях сверх лимита в 15 ГБ в месяц, со стартом до 1 мая 2026 года.[120] Логика прямо увязана с борьбой против обхода: VPN-трафик технически неотличим от обычного зарубежного, поэтому мера бьет по всему международному трафику разом. Размер лимита обосновывался расчетом Минцифры, согласно которому средний абонент потребляет около 10 ГБ международного трафика в месяц, а стоимость превышения оценивалась примерно в 150 рублей за гигабайт.[121]

Первоначальный срок сорвался из-за особенностей договорного регулирования. Тарифы на услуги связи оператор устанавливает и изменяет самостоятельно, но закон разграничивает изменение цены и изменение тарифного плана как набора услуг. Согласно статье 28 Федерального закона № 126-ФЗ "О связи" и Правилам оказания услуг телефонной связи, оператор вправе в одностороннем порядке изменить цену действующего тарифа, уведомив абонента не менее чем за 10 календарных дней через сайт и SMS.[122] Однако раздельная тарификация внутреннего и международного трафика — это не повышение цены, а введение нового параметра тарификации, то есть изменение существенных

[120] Минцифры предложило плату за зарубежный трафик свыше 15 ГБ // Фонтанка URL: https://www.fontanka.ru/2026/03/30/76339405/
[121] Россиянам с осени могут ввести плату за зарубежный интернет // The Moscow Times URL: https://ru.themoscowtimes.com/2026/06/25/rossiyanam-s-oseni-mogut-vvesti-platu-za-zarubezhnii-internet-a199232
[122] Минцифры / ПП № 59 от 24.01.2024, право оператора изменять тариф с уведомлением за 10 дней, ст. 28 ФЗ-126 — https://digital.gov.ru/ru/appeals/faq/374/

условий договора, которое затрагивает набор и структуру услуг.[123] Такое изменение требует перестройки биллинговых систем, способных отделять зарубежный трафик от внутреннего в реальном времени, и переоформления договорных условий с абонентами.

22 апреля 2026 года операторы попросили отсрочку, сославшись на неготовность биллинговых систем, и решение перенесли на период после осенних выборов в Госдуму.[124] 27 апреля Минцифры подтвердило, что отдельная тарификация международного трафика находится в проработке.[125] Перенос объясняется совокупностью причин. Технически раздельная тарификация требует доработки биллинга. Юридически введение платы упирается в отсутствие нормативной базы: у Минцифры нет прямых полномочий, а значит, требуются поправки в законодательство. Политически запуск механизма, напрямую удорожающего доступ к интернету для массового абонента, был отложен, чтобы не создавать раздражающего фактора накануне голосования.

К концу второго квартала 2026 года механизм нормативно не закреплен, однако направление зафиксировано официальными документами и совещаниями. Конечная цель остается двойной: экономически сдержать обход блокировок и принудить зарубежные сервисы размещать инфраструктуру в российской юрисдикции, под СОРМ.

2. Мораторий на международные каналы

16 апреля 2026 года стало известно, что около двадцати компаний — владельцев каналов связи, идущих из России в Европу, подписали с Минцифры соглашение о приостановке их расширения.[126] По данным источников на телеком-рынке, документ был подписан на одном из совещаний с Максутом Шадаевым, посвященном ограничению работы VPN. Среди участников назывались MSK-IX (ММТС-9), "Транстелеком", МТС, "ВымпелКом" ("Билайн"), "Т2 Мобайл" и "Уфанет".[127] Срок действия ограничения операторам не назвали.

Причина введения меры прямо связана с VPN. Трафик сервисов обхода для оператора выглядит как обычный зарубежный, и чем активнее растет использование VPN, тем быстрее заполняются полосы для пропуска трансграничного трафика. Логика регулятора состоит в том, что запасы этих полос ограничены, а естественный рост трафика приведет к их исчерпанию. Помимо приостановки расширения, участников рынка обязали ежемесячно отчитываться о трансграничном трафике: его

---

[123] Роспотребнадзор, разграничение изменения цены тарифа и тарифного плана (набора услуг) как существенного условия договора — https://zpp.rospotrebnadzor.ru/handbook/svyaz/memos/207553
[124] Операторы попросили отсрочку по тарификации зарубежного трафика // Ведомости URL: https://www.vedomosti.ru/technology/articles/2026/04/22/1192083
[125] Минцифры о тарификации международного трафика // Habr URL: https://habr.com/ru/news/1029090/
[126] Операторы подписали мораторий на расширение международных каналов // GoGov URL: https://gogov.ru/news/927744
[127] Meduza, состав участников совещания и подписантов моратория, срок не назван — https://meduza.io/news/2026/04/16/rbk-operatory-svyazi-soglasilis-zamorozit-rasshirenie-kanalov-svyazi-v-evropu-chtoby-borotsya-s-ispolzovaniem-vpn

объеме, ресурсах-источниках и узлах связи, через которые он проходит.[128] Второй заявленной целью источники называют принуждение зарубежных сервисов, желающих сохранить работу в России, размещать инфраструктуру внутри страны — чтобы скорость доступа для российских пользователей не снижалась по мере заполнения каналов.[129]

Формально речь идет не о запрете, а о согласительном порядке, введенном еще в марте 2026 года: оператор, желающий расширить зарубежные каналы, обязан получить разрешение.[130] На момент публикации материалов согласительный порядок не прошел ни один оператор, а критерии выдачи разрешений участникам рынка не сообщили.[131] При этом у Минцифры отсутствуют полномочия для такого дополнительного согласования: чтобы порядок стал законным, требуется внесение поправок в закон или принятие постановления правительства.[132]

3. Последствия для рынка

Прогноз последствий уже озвучен участниками отрасли публично. Руководитель направления развития телеком-бизнеса "Транстелекома" Илья Гуденко на Night Telecom Forum в Санкт-Петербурге в июне 2026 года описал сценарий: к осени 2026 года действующие каналы могут оказаться утилизированы, а новые не получат разрешения на полное расширение.[133] В этом случае провайдеры начнут вытеснять менее рентабельных клиентов, расчищать полосу и вводить дифференцированные тарифы, разделяя доступ на два вида — с российским интернетом дешевле или по текущей цене и с зарубежным дороже.[134] Тем самым нагрузка по сдерживанию VPN перекладывается на самих операторов: при заполненных каналах и запрете на их расширение бизнес вынужден либо фильтровать трафик обхода, либо устанавливать экономический барьер, поднимая стоимость зарубежного доступа.[135]

Отдельная сложность связана с механизмом различения российского и зарубежного трафика. Наиболее вероятным инструментом разметки становится РАНР — Реестр адресно-номерных

---

[128] Forbes, ежемесячная отчетность о трансграничном трафике и цель принудить сервисы размещать серверы в РФ — https://www.forbes.ru/tekhnologii/559280-rbk-uznal-o-moratorii-na-rassirenie-kanalov-svazi-v-evropu-radi-bor-by-s-vpn

[129] -//-

[130] Хабр, согласительный порядок с марта 2026, никто не прошел, критерии не сообщены — https://habr.com/ru/news/1052072/

[131] -//-

[132] Meduza, для дополнительного согласования Минцифры нужны поправки в закон или постановление правительства — https://meduza.io/news/2026/04/16/rbk-operatory-svyazi-soglasilis-zamorozit-rasshirenie-kanalov-svyazi-v-evropu-chtoby-borotsya-s-ispolzovaniem-vpn

[133] Хабр, прогноз Ильи Гуденко (ТТК) на Night Telecom Forum о дифференцированных тарифах к осени 2026 — https://habr.com/ru/news/1052072/

[134] -//-

[135] Эксперт, экономический фильтр — операторы сами будут фильтровать VPN или поднимать цену на зарубеж — https://expert.ru/news/rbk-uznal-o-moratorii-operatorov-na-rasshirenie-kanalov-svyazi-v-evropu-radi-borby-s-vpn/

ресурсов российского сегмента сети Интернет, который ЦМУ ССОП при ГРЧЦ запустил в публичном доступе в апреле 2024 года как национальный аналог whois и базы данных RIPE.[136] За неподключение к РАНР статья 13.44 КоАП уже предусматривает штрафы вплоть до пятидесяти тысяч рублей для юридических лиц.[137] Реестр в теории позволяет размечать, какие IP-адреса и автономные системы считаются российскими, и строить на этой основе раздельную маршрутизацию и тарификацию. Однако значительная часть ресурсов российских компаний физически размещена на иностранных хостингах — в том числе из-за нехватки отечественных мощностей, особенно в области искусственного интеллекта. Это создает риск того, что раздельная тарификация затронет легальный бизнес-трафик, а обход через обратные прокси и VPN сохранит принципиальную возможность.

Предельную форму этого регулирования показывает опыт Ирана. После восстановления доступа в интернет летом 2025 года иранские власти сначала вернули работу дата-центров, но в течение нескольких дней вновь ограничили ее, столкнувшись с массовым разворачиванием VPN на арендованных серверах. Правила ужесточили: для покупки любых услуг дата-центра теперь обязателен подтвержденный профиль в государственной системе верификации абонентов "Шахкар", причем номер телефона и национальный идентификатор должны принадлежать одному лицу, а сведения о подключенных цифровых услугах отображаются в личном кабинете гражданина на государственном портале. Ответственность за идентификацию конечных пользователей возложена либо на сам дата-центр, либо на хостинг-компанию-посредника, которой выделяется пул адресов. Система "Шахкар", изначально созданная для операторов связи и затем распространенная на банковские и государственные сервисы, а теперь и на хостинг, по документам, разобранным Citizen Lab, входит в состав иранской системы законного перехвата и поддерживает жесткую привязку один пользователь — один профиль.[138] Российский РАНР пока решает более узкую задачу разметки адресного пространства, но вектор совпадает: привязка каждого сетевого ресурса к верифицированному владельцу с перекладыванием ответственности за идентификацию на бизнес.

Глава 9. Новый куратор: ФСБ берет управление

Институциональным итогом периода стало смещение центра управления цензурой от Роскомнадзора к силовому блоку.

---

[136] Запуск публичного сервиса РАНР (реестр адресно-номерных ресурсов) и whois-аналога ГРЧЦ/ЦМУ ССОП, апрель 2024, аналог базы RIPE // Хабр URL: https://habr.com/ru/news/806591/ ; RoskomSvoboda URL: https://roskomsvoboda.org/ru/post/suveren-whois-ranr/

[137] ОрдерКом, штрафы по ст. 13.44 КоАП за неподключение к РАНР до 50 тыс. руб. для юрлиц — https://www.ordercom.ru/analitika/suvenirans

[138] Citizen Lab, "Шахкар" как компонент системы законного перехвата, связка один пользователь — один профиль — https://citizenlab.ca/research/uncovering-irans-mobile-legal-intercept-system/

Постановлением правительства № 1667 от 27 октября 2025 года были утверждены новые правила централизованного управления сетью связи общего пользования, вступившие в силу 1 марта 2026 года. Управление инфраструктурой ТСПУ закрепили совместно за Роскомнадзором, ФСБ и Минцифры, а решение о введении режима централизованного управления (фильтрация, блокировка направлений, изоляция сегмента сети) передали межведомственной комиссии.[139]

Еще дальше пошел отдельный закон (законопроект № 1069501-8, принятый Госдумой в третьем чтении 17 февраля 2026 года и одобренный Совфедом 18 февраля): он обязал операторов связи приостанавливать любые услуги по мотивированному требованию ФСБ. Новое основание — "угрозы безопасности граждан и государства", содержание которых определяется закрытыми актами, при этом операторы освобождены от ответственности перед абонентами за такие отключения.[140] В январе 2026 года Госдума отдельно рассматривала поправки, дающие ФСБ право отключать не только мобильную, но и стационарную связь и телефонию.[141]

За обезличенной формулировкой "ФСБ" стоит конкретное подразделение. Судя по совокупности признаков — прежде всего по тому, кто выиграл аппаратный спор вокруг блокировки Telegram (см. главу 5), — управление интернет-цензурой с февраля 2026 года сосредоточилось во Второй службе ФСБ, Службе по защите конституционного строя и борьбе с терроризмом (на внутреннем жаргоне — "двойка"). Это подразделение считается прямым наследником Пятого управления КГБ, отвечавшего за борьбу с "идеологическими диверсиями", и исторически специализируется на угрозах в социально-политической сфере, то есть на внутреннем инакомыслии. Передача ему контроля над блокировками означает, что интернет-цензуру в России окончательно перестали считать технической или отраслевой задачей и отнесли к той же категории, что и политический сыск.[142]

Службу с марта 2006 года бессменно возглавляет генерал-полковник Алексей Семёнович Седов (род. 1954, Сочи). Выходец из ленинградского управления КГБ, в 1990-е годы он работал в налоговой полиции, затем был заместителем директора Госнаркоконтроля, а в 2006 году вернулся в ФСБ уже на пост главы "двойки". В 2021 году Седов попал под санкции Великобритании, США, Канады и Украины как руководитель службы, координировавшей действия подразделения, причастного к отравлению Алексея Навального.[143] Профильным управлением внутри службы — Управлением по

---

[139] Правила централизованного управления сетью связи общего пользования (ПП № 1667 от 27.10.2025, вступление 1 марта 2026) // КонсультантПлюс URL: https://www.consultant.ru/law/hotdocs/91389.html

[140] Закон об обязанности операторов приостанавливать услуги связи по требованию ФСБ (законопроект № 1069501-8, принят Госдумой 17 февраля 2026, одобрен Совфедом 18 февраля) // Право.ру URL: https://pravo.ru/news/262459/

[141] Госдума в первом чтении (27 января 2026) — о праве ФСБ требовать отключения не только мобильной, но и стационарной связи и телефонии (законопроект № 1069501-8) // ComNews URL: https://www.comnews.ru/content/243470/2026-01-28/2026-w05/1008/otklyuchenie-interneta-pereydet-pod-kontrol-fsb

[142] Служба по защите конституционного строя и борьбе с терроризмом (Вторая служба, "двойка"): сфера ответственности, структура, заместитель руководителя А. Жало (УЗКС) // Центр Досье URL: https://fsb.dossier.center/2s/

[143] Алексей Седов — руководитель Второй службы ФСБ с марта 2006 года, генерал-полковник; биография и санкции по делу об отравлении А. Навального (2021) // Википедия URL: https://ru.wikipedia.org/wiki/Седов,_Алексей_Семёнович

защите конституционного строя (УЗКС) — руководит генерал-лейтенант Алексей Жало.[144] Обе фигуры остаются публично почти невидимыми, что типично для этого подразделения: его контакты с прессой и остальными отделами ФСБ намеренно ограничены.

Смысл сдвига в том, что роль Роскомнадзора меняется. Из ведомства, которое определяло угрозы и принимало решения о блокировках, он превращается в технического исполнителя при силовом кураторе. Управление доступом к информации в России окончательно переходит из административной плоскости в плоскость безопасности — со всей сопутствующей закрытостью процедур и оснований.

Практические последствия этого перехода двоякие. Во-первых, блокировки стали заметно жестче. Служба, чья задача — подавление угроз в социально-политической сфере, а не баланс экономических издержек, готова платить ту цену, перед которой прежде останавливались Минцифры и операторы: именно поэтому Telegram все же заблокировали вопреки протестам военкоров, депутатов и провластных блогеров. Во-вторых, столкнувшись с тем, что выиграть техническую гонку с VPN не удается, силовой куратор изменил саму тактику. Вместо того чтобы и дальше догонять средства обхода собственными руками, государство придумало ход, проходящий красной нитью через всю эту главу, — переложить борьбу с VPN на бизнес. Маркетплейсы, банки и хостеров принуждают самостоятельно выявлять и отключать пользователей обхода под угрозой исключения из белых списков, потери аккредитации и мобилизации сотрудников, а антифродовые пакеты перекрывают саму оплату обхода. Так функция цензуры окончательно распределяется между теми, кто по квалификации и охвату способен исполнять ее лучше государственной системы, — под контролем и по заданию силового куратора.

Заключение: какие ступени пройдены

Сопоставление с прогнозом первой части дает наглядную картину. Из шести вероятных будущих ступеней, перечисленных весной 2025 года, к середине 2026 года пройдены или активно проходятся почти все. Telegram фактически заблокирован, хотя формально это не объявлено. Статистические методы выявления VPN внедрены — именно по поведению трафика детектируются VLESS и REALITY. Блокировка крупных блоков IP-адресов стала рутиной: под нее попали и Cloudflare, и подсети зарубежных хостеров. Тактика "серых списков" и намеренного ухудшения качества связи — основной инструмент против мессенджеров. Переход к "белым спискам", который описывался как отдаленный сценарий, реализован и развернут в большинстве регионов на мобильных сетях. И даже движение к полной изоляции — через лимит международного трафика и мораторий на расширение каналов — перестало быть гипотезой.

---

[144] Служба по защите конституционного строя и борьбе с терроризмом (Вторая служба, "двойка"): сфера ответственности, структура, заместитель руководителя А. Жало (УЗКС) // Центр Досье URL: https://fsb.dossier.center/2s/

К этому прогнозируемому набору период добавил то, чего прежний анализ не считал центральным: повседневные веерные шатдауны и принуждение десятков миллионов пользователей к государственному мессенджеру. Логика "лестницы" при этом сохранилась полностью — каждая новая мера проходит те же четыре стадии (политическое решение, правовое оформление, техническая реализация, ресурсное обеспечение), что были описаны в первой части. Изменился лишь масштаб и скорость.

Не изменилась и фундаментальная дилемма. Веерные отключения и "белые списки" наносят прямой удар по экономике, оцениваемый в миллиарды долларов; перенос функций цензуры на бизнес оборачивается для компаний прямыми издержками; разделение трафика грозит изоляцией от глобальной инфраструктуры, на которой держится в том числе экспортная экономика. Власти по-прежнему выбирают "хирургические" и "тихие" методы, чтобы не платить полную цену изоляции сразу — отсюда замедление вместо блокировки, "период охлаждения" вместо отключения, лимит трафика вместо обрыва каналов.

И не изменилась расстановка сил в главном противостоянии. Несмотря на все перечисленные меры, проникновение VPN среди российских пользователей по разным оценкам держится на уровне около 40%, а по отдельным исследованиям в столицах превышает 60%.[145] Это значит, что сценарий, при котором значительная часть населения сохраняет доступ к независимой информации, остается реальным. "Лестница блокировок" продолжает строиться вверх — но и встречное движение тех, кто эту лестницу обходит, не прекращается. Исход этой борьбы по-прежнему не предрешен.

Выводы

1. Прогноз стал хроникой. Из шести ступеней, названных вероятными весной 2025 года, к середине 2026-го пройдены или активно проходятся почти все: фактическая блокировка Telegram, статистическое детектирование VPN, блокировка крупных блоков IP, намеренная деградация связи, переход к "белым спискам" и первые шаги к разделению трафика. К этому набору период добавил то, чего прежний анализ не считал центральным, — повседневные веерные шатдауны и принуждение десятков миллионов пользователей к государственному мессенджеру.
2. Сменилась сама логика цензуры. Модель "запрещено то, что в списке" уступила место модели "разрешено только то, что в списке". При этом "белые списки" возникли не как идеологический замысел, а как вынужденная реакция на хаос отключений — и силовой блок быстро перехватил этот механизм, превратив его из способа сохранить жизненно важные сервисы в рычаг принуждения: доступность банковского приложения поставлена в зависимость от установки СОРМ.
3. Цензуру переложили на бизнес и пользователей. Компании принуждают самостоятельно

[145] Доля использующих VPN россиян выросла до 39% // НСН URL: https://nsn.fm/society/smi-dolya-ispolzuuschih-vpn-rossiyan-vyrosla-do-39

выявлять VPN под угрозой исключения из "белых списков", потери IT-аккредитации и, как следствие, мобилизации сотрудников; ответственность впервые сместилась и на конечного пользователя — вплоть до наказания за сам поиск информации. Государству больше не нужно догонять технологии обхода — достаточно заставить работать на цензуру тех, кто понимает их лучше всех.

4. Логика "лестницы" сохранилась, изменились масштаб и скорость. Каждая новая мера проходит те же четыре стадии — политическое решение, правовое оформление, техническая реализация, ресурсное обеспечение. За техникой стоит выстроенная индустрия с собственным подрядчиком, бюджетами в десятки миллиардов рублей и переходом к фильтрации на базе машинного обучения.
5. Центр управления сместился от Роскомнадзора к ФСБ. РКН из ведомства, определявшего угрозы и принимавшего решения, превратился в технического исполнителя при силовом кураторе. Управление доступом к информации окончательно перешло из административной плоскости в плоскость безопасности — с закрытыми процедурами и основаниями.
6. Исход не предрешен. Несмотря на все меры, проникновение VPN держится около 40%, а в столицах превышает 60%, и каждая новая волна блокировок расширяет аудиторию обхода, а не сокращает ее. Власти по-прежнему выбирают "тихие" методы — замедление вместо блокировки, лимит трафика вместо обрыва каналов, — чтобы не платить полную цену изоляции сразу. Лестница блокировок продолжает строиться вверх, но встречное движение тех, кто ее обходит, не прекращается.