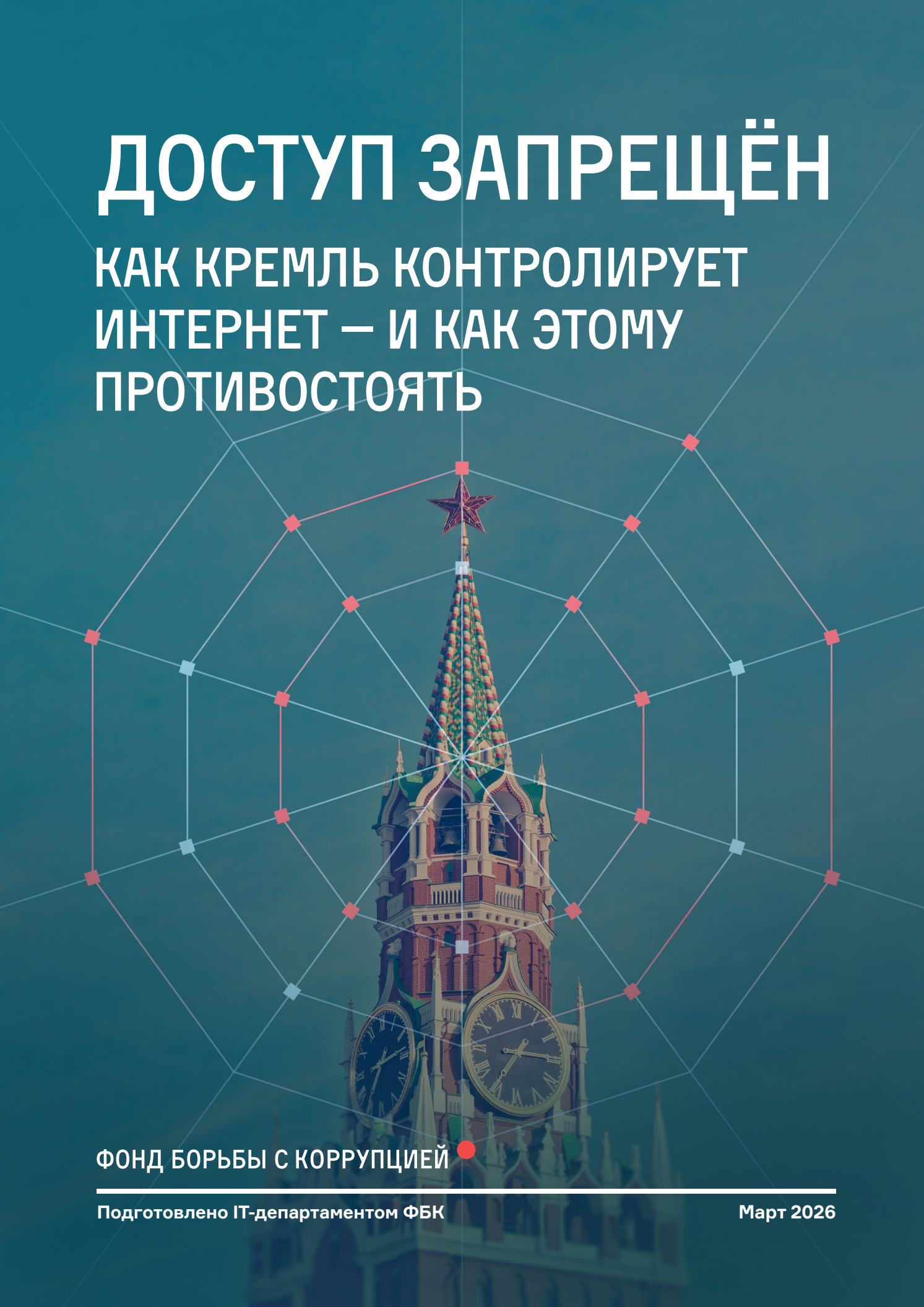
ДОСТУП ЗАПРЕЩЁН

КАК КРЕМЛЬ КОНТРОЛИРУЕТ ИНТЕРНЕТ — И КАК ЭТОМУ ПРОТИВОСТОЯТЬ



ФОНД БОРЬБЫ С КОРРУПЦИЕЙ

Подготовлено IT-департаментом ФБК

Март 2026

Содержание

Введение	3
Блокировки до ТСПУ	6
ТСПУ и его внедрение	9
Успешные кейсы противостояния Роскомнадзору	14
Современное состояние интернет-цензуры в России	18
Выводы и предложения	23

Введение

На протяжении двадцати шести лет у власти **Владимир Путин последовательно уничтожает свободу слова и подавляет любые формы горизонтальной самоорганизации** российских граждан.

В самом начале своего правления он взял под контроль телевидение. Затем он уничтожил свободную прессу, а в последние пятнадцать лет переключил своё внимание на интернет.

За это время российская система интернет-цензуры эволюционировала от сравнительно грубого и непоследовательного механизма блокировок к гораздо более **зрелой, централизованно управляемой и технологически гибкой модели.**

Эта трансформация имеет значение не только в техническом, но и в политическом смысле. Российское государство последовательно превращало интернет из пространства относительной свободы в среду управляемого доступа, где ограничения вводятся быстрее, точнее и единообразнее, а сами инструменты цензуры становятся всё менее заметными для внешнего наблюдателя.

Цель доклада

Цель этого доклада — описать, **как эволюционировала российская система интернет-ограничений**, почему после внедрения ТСПУ (технических средств противодействия угрозам) она стала качественно опаснее и к каким практическим выводам это приводит для стратегий, направленных на обход онлайн-блокировок.

В докладе мы приводим историческую справку и предлагаем конкретные решения, которые могут помочь большим технологическим компаниям и прочим цифровым платформам бороться за своих пользователей и имплементировать технологии обхода блокировок в свои продукты.

Охват и база источников

Этот доклад основан на четырёх категориях источников:

- публичные веб-публикации,
- академическая литература,
- экспертные социальные и технические каналы,
- внутренние документы, экспертиза ФБК.

Краткое резюме

Российская модель интернет-блокировок эволюционировала от блокировок по IP, реестра запрещённых сайтов и точечных блокировок, до **распределённой, но управляемой из единого центра системой DPI-контроля** (Deep Packet Inspection), построенной вокруг ТСПУ — внедрённых в рамках закона о «суверенном интернете» 2019 года, с покрытием в масштабах всей страны и большинства провайдеров.[1]

Вместо того чтобы полагаться на единую национальную точку контроля наподобие китайского Great Firewall, Россия выстроила тысячи точек принуждения на стороне провайдеров (включая точки «рядом с абонентом» в некоторых дата-центрах и на трансграничных каналах), работающих под централизованным государственным управлением.[2] Эта система даёт Роскомнадзору (цензурному ведомству) значительно более тонкий, быстрый и адаптивный контроль над трафиком.

Неудачная попытка заблокировать Telegram в 2018 году стала поворотным моментом. Более ранняя модель Роскомнадзора, известная как «Ревизор», в значительной степени опиралась на блокировки по IP, которые обеспечивали провайдеры, но контролировало государство, а также на побочное давление на инфраструктурных провайдеров.[3] На практике этот подход оказался неспособен отключить крупный сервис, который мог скрываться за общей инфраструктурой и быстро адаптироваться[4] [5] Последующие источники прямо **связывают изменение политики после 2018 года с развёртыванием ТСПУ** в рамках режима «суверенного интернета».

В данном случае ключевой вывод состоит в том, что **единая централизованная архитектура обхода цензуры для любого приложения в России была бы дорогой, хрупкой и, вероятно, недолговечной**, если только за ней не стоит постоянная итерация протоколов, быстрая ротация конечных точек и непрерывная телеметрия из реальных условий.

---

[1] Epifanova A., «Deciphering Russia's Sovereign Internet Law» («Расшифровка закона о суверенном интернете России»), German Council on Foreign Relations (DGAP), December 2019, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

[2] Xue D. и др., «TSPU: Russia's Decentralized Censorship System» («TSPU: децентрализованная система интернет-цензуры в России»), в: Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22) (New York: Association for Computing Machinery, 2022), с. 179–194, https://doi.org/10.1145/3517745.3561461.

[3] Ermoshina K., Musiani F., «The Telegram Ban: How Censorship "Made in Russia" Faces a Global Internet» («Запрет Telegram: как цензура "сделано в России" сталкивается с глобальным интернетом»), First Monday, т. 26, № 5 (2021), https://doi.org/10.5210/fm.v26i5.11704.

[4] Lyndell D., Zayakin A., Klimarev M., «Putin's Digital Iron Curtain: Russia Bypasses Sanctions, Buys Equipment to Block YouTube and Telegram» («Цифровой железный занавес Путина: Россия обходит санкции и закупает оборудование для блокировки YouTube и Telegram»), The Insider, October 11, 2023, https://theins.ru/en/politics/265749.

[5] «No Country for Telegram: Russia Starts Second Attempt to Block One of Its Most Popular Messengers» («Не страна для Telegram»), Mediazona, February 10, 2026, https://en.zona.media/article/2026/02/10/telegram.

Открытые публикации,[6] академический анализ,[7] и внутренние операционные данные ФБК указывают на один и тот же вывод: как только способ обхода становится единообразным, заметным и широко используемым, российские цензоры обычно выявляют его и начинают атаковать на уровне протокола, инфраструктуры или распространения.

Наиболее реалистичная стратегия — **гибридный подход:** поддерживать небольшую выделенную инженерную команду по обходу цензуры, измерять реальную доступность в первую очередь с помощью телеметрии продукта, а не одного внешнего зонда, избегать зависимости от стандартных VPN-протоколов (Virtual Private Network Provider) или статичных диапазонов дата-центров и поддерживать более широкую экосистему децентрализованных средств обхода, а не исходить из того, что любая компания в одиночку может выиграть постоянную централизованную гонку вооружений.

Эта рекомендация основана на нескольких сходящихся факторах: текущей архитектуре интернет-контроля в России,[8] снижении эффективности стандартных VPN-протоколов,[9] полевом опыте проектов, связанных с оппозицией, и недавнем появлении тестов «интернета по белому списку» в Москве.[10]

---

[6] "[Russia] Censor Has a New Method of Blocking #490," *Net4People BBS (GitHub),* https://github.com/net4people/bbs/issues/490 (accessed March 20, 2026).

[7] Xue et al., "TSPU: Russia's Decentralized Censorship System."

[8] «The VLESS Protocol: How It Bypasses Censorship in Russia and Why It Works» («Протокол VLESS: как он обходит цензуру в России и почему работает»), Habr, February 17, 2026, https://habr.com/en/articles/990144/.

[9] Human Rights Watch, «Russia: Digital Iron Curtain Falls on Internet Freedom Protection Day» («Россия: цифровой железный занавес в день защиты свободы интернета»), March 12, 2026, https://www.hrw.org/news/2026/03/12/russia-digital-iron-curtain-falls-on-internet-freedom-protection-day.

[10] Zadorozhnyy T., «Moscow Citizens Turn to Pagers, Printed Maps» («Жители Москвы переходят на пейджеры и бумажные карты»), The Kyiv Independent, March 14, 2026, https://kyivindependent.com/moscow-citizens-turn-to-pagers-printed-maps/.

Блокировки до ТСПУ

Блокировки интернета до внедрения ТСПУ

В ранний период система интернет-блокировок в России сочетала централизованное управление и неравномерную техническую реализацию. В 2012 году в России была введена **национальная система чёрных списков**[11] в рамках которой Роскомнадзор вёл единый реестр запрещённых сайтов, а провайдеры были обязаны блокировать внесённые туда ресурсы.[12]

В 2015 году Роскомнадзор начал внедрять систему под названием «Ревизор».[13] Она работала как простой инструмент мониторинга, который проверял, блокируют ли провайдеры сайты из национального чёрного списка. Если сайт оставался доступен, ответственному провайдеру автоматически выписывался штраф. Эта система сохраняется и сегодня как резервный инструмент на случай, если узел ТСПУ выходит из строя и его необходимо обойти.[14]

В 2016 году закон Яровой резко усилил давление в сфере наблюдения и подотчётности, потребовав от телекоммуникационных компаний хранить метаданные и предоставлять по запросу информацию, необходимую для расшифровки.[15] Сам по себе этот закон не привёл к созданию ТСПУ, но он усилил влияние государства на операторов сетей и платформ и нормализовал инфраструктурное вмешательство в коммуникации.[16]

В 2018 году Роскомнадзор попытался заблокировать Telegram с помощью старой модели: судебных предписаний, исполнения через реестр и массовой блокировки IP-адресов.[17] Эта **кампания прославилась масштабным**

---

[11] «Amendments to the Law on Protecting Children from Information Harmful to Their Health and Development» («Поправки к закону о защите детей от вредной информации»), Kremlin.ru, July 31, 2012, http://en.kremlin.ru/events/president/news/16095.

[12] «Russia Internet Blacklist Law Takes Effect» («В России вступил в силу закон о чёрном списке сайтов»), BBC News, November 1, 2012, https://www.bbc.com/news/technology-20096274.

[13] «Revizor — Website Blocking Control System in Russia» («Ревизор — система контроля блокировки сайтов в России»), TAdviser, https://www.tadviser.ru/index.php/Продукт:Ревизор_-_система_контроля_блокировки_сайтов_в_России.

[14] "Let's Count 'Revizor' Agents" (Сосчитаем агентов «Ревизор»), *Habr*, May 6, 2019, https://habr.com/en/articles/450362/ (accessed March 20, 2026).

[15] O'Brien D., Galperin E., «Russia Asks for the Impossible With Its New Surveillance Laws» («Россия требует невозможного: новые законы о слежке»), Electronic Frontier Foundation, July 19, 2016, https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.

[16] Human Rights Watch, «Russia: „Big Brother" Law Harms Security, Rights — Repeal Rushed Counterterrorism Legislation» («Россия: закон „Большого брата" угрожает безопасности и правам»), July 12, 2016 https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

[17] Ermoshina K., Musiani F., «The Telegram Ban: How Censorship „Made in Russia" Faces a Global Internet» («Запрет Telegram: как цензура „сделано в России" сталкивается с глобальным интернетом»), First Monday, т. 26, № 5 (2021), https://doi.org/10.5210/fm.v26i5.11704.

побочным ущербом (пострадали Microsoft Store, PlayStation Network и другие крупные ресурсы, особенно использующие AWS) и тем, что так и не смогла отключить Telegram. Этот провал широко рассматривается как один из главных катализаторов для последующей, более амбициозной архитектуры «суверенного интернета».

В ноябре 2019 года закон о суверенном интернете дал Роскомнадзору правовую основу для **требования установки ТСПУ у операторов и создал рамку для централизованного управления телекоммуникационными сетями**, национального DNS-слоя (Domain Name System) и прямого государственного контроля над маршрутизацией и фильтрацией.[18]

Заметный переломный момент наступил **в марте 2021 года, когда РКН скоординировано замедлил работу Twitter** на территории РФ, что исследователи позднее связали с ТСПУ.[19] То есть к этому моменту ТСПУ уже, наконец, было установлено. Это было важно и показательно: теперь государство умеет не только грубо блокировать через реестры и импровизацию на уровне провайдеров, но и осуществлять выборочное замедление ресурса в национальном масштабе.

С начала полномасштабной войны в 2022 году режим цензуры в России сместился от выборочного замедления к системному подавлению: власти заблокировали или ограничили крупные иностранные платформы (YouTube, Facebook, Instagram и другие),[20] усилили давление на магазины приложений и хостинг-провайдеров и использовали TLS-вмешательство (Transport Layer Security) на базе ТСПУ, чтобы сделать интернет-ограничения гораздо более единообразными, чем в довоенный период.[21]

В 2024 году OONI (Open Observatory of Network Interference) подтвердил блокировку **как минимум 279 доменов новостных медиа в России**,[22] а Human Rights Watch задокументировала устойчивое замедление таких сервисов, как YouTube, а также более широкий государственный курс

---

[18] Epifanova A., «Deciphering Russia's Sovereign Internet Law» («Расшифровка закона о суверенном интернете России»), German Council on Foreign Relations (DGAP), December 2019, Epifanova A., «Deciphering Russia's Sovereign Internet Law» («Расшифровка закона о суверенном интернете России»), German Council on Foreign Relations (DGAP), December 2019, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

[19] Xue D. и др., «TSPU: Russia's Decentralized Censorship System» («TSPU: децентрализованная система интернет-цензуры в России»), в: Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22) (New York: Association for Computing Machinery, 2022), с. 179–194, https://doi.org/10.1145/3487552.3487858.

[20] Human Rights Watch, Disrupted, Throttled, and Blocked: State Censorship, Control, and Increasing Isolation of Internet Users in Russia («Нарушено, замедлено и заблокировано: государственная цензура и изоляция пользователей интернета в России»), New York: Human Rights Watch, July 30, 2025, https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation.

[21] RKS Global и др., Censorship Chronicles: The Systematic Suppression of Independent Media in Russia («Хроники цензуры: системное подавление независимых медиа в России»), OONI, December 9, 2024, https://ooni.org/post/2024-russia-report/.

[22] Human Rights Watch, Disrupted, Throttled, and Blocked: State Censorship, Control, and Increasing Isolation of Internet Users in Russia («Нарушено, замедлено и заблокировано: государственная цензура и изоляция пользователей интернета в России»).

на изоляцию российского интернета не только юридически, но и архитектурно.[23]

Адреса видеопотоков Youtube были в конечном счёте заблокированы, а на части российских DNS-серверов домен youtube.com перестал быть доступным вовсе.24

В 2025–2026 годах репрессии усилились ещё больше: Роскомнадзор начал масштабную кампанию против VPN, ограничил звонки в Telegram и WhatsApp в августе 2025 года, подтвердил блокировку сотен VPN-сервисов к началу 2026 года, а затем перешёл к прямым ограничениям против самого Telegram и расширению тестирования модели «интернета по белому списку» — от регионов военного положения до Москвы.[25]

Стратегия Роскомнадзора до внедрения ТСПУ

До широкого распространения ТСПУ (примерно до 2021 года) Роскомнадзор в основном полагался на правовую и административную цензурную инфраструктуру: **централизованный реестр запрещённых сайтов, судебные и внесудебные предписания об удалении, давление на хостинг-провайдеров и поисковики, DNS-манипуляции и простую блокировку IP** на стороне провайдеров.[26] Эта модель часто работала неравномерно в разных сетях, поскольку качество исполнения зависело от провайдера, его оборудования и его готовности или способности точно исполнять предписания.[27]

Модель до ТСПУ всё ещё могла быть эффективной, особенно для сайтов на выделенных IP или с легко различимыми доменами, но у неё были структурные слабости. Её было проще обходить с помощью CDN (Content Delivery Network), общей облачной инфраструктуры, смены доменов, прокси или VPN, а при попытках блокировать крупные диапазоны адресов она приводила к значительному побочному ущербу. Самый наглядный пример — устойчивость Telegram в 2018 году, но та же особенность проявлялась и в более широком спектре оппозиционных проектов.

---

[23] RKS Global и др., Censorship Chronicles: The Systematic Suppression of Independent Media in Russia («Хроники цензуры: системное подавление независимых медиа в России».

[24] Strelnikov A., «YouTube, WhatsApp Blocked in Russia» («YouTube и WhatsApp заблокированы в России»), Deutsche Welle, February 12, 2026, https://www.dw.com/en/youtube-whatsapp-blocked-in-russia/a-75940102.

[25] Zadorozhnyy T., «Moscow Citizens Turn to Pagers, Printed Maps» («Жители Москвы переходят на пейджеры и бумажные карты»), The Kyiv Independent, March 14, 2026, https://kyivindependent.com/moscow-citizens-turn-to-pagers-printed-maps.

[26] "Russia Internet Blacklist Law Takes Effect," *BBC News,* November 1, 2012, https://www.bbc.com/news/technology-20096274.

[27] Epifanova A., «Deciphering Russia's Sovereign Internet Law» («Расшифровка закона о суверенном интернете России»), German Council on Foreign Relations (DGAP), December 2019, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

ТСПУ и его внедрение

Внедрение ТСПУ

ТСПУ — «технические средства противодействия угрозам». Это навязанная государством система фильтрации трафика на стороне провайдеров, которую широко понимают как DPI-систему, хотя она включает и сопутствующие функции управления, контроля и маршрутизации. Публичный анализ политики, академические исследования, свидетельства операторов и журналистские расследования описывают ТСПУ как **сочетание аппаратного и программного обеспечения, поставляемого операторам, но контролируемого государством.**

Наиболее важное техническое отличие — архитектурное. Россия не воспроизвела китайскую модель. Вместо того чтобы полагаться главным образом на небольшое число пограничных «бутылочных горлышек», что практически невозможно с учётом того, как развивался интернет в России, она переместила инструмент блокировки ближе к конечным пользователям, устанавливая ТСПУ внутри или совсем рядом с сетями доступа провайдеров. Академические измерения выявили более одного миллиона российских конечных точек в 650 автономных системах за как минимум одним устройством ТСПУ и пришли к выводу, что 70 процентов устройств ТСПУ находятся максимум в двух «переходах» от конечного IP.

Это размещение имеет значение, потому что даёт системе лучшую видимость пользовательского трафика и позволяет проводить избирательное вмешательство. Исследователи установили, что блокировки через ТСПУ срабатывают по SNI, IP и характеристикам QUIC, а поведение системы настолько приближено к конечным пользователям, что одного лишь удалённого измерения часто недостаточно, чтобы увидеть весь механизм блокировки на территории страны.[28]

ТСПУ состоит из высокоскоростного аппаратного слоя проверки политик, который либо пропускает/отклоняет трафик, либо отправляет его на низкоскоростной CPU-слой, выполняющий сложный анализ пакетов, сборку сегментов или модификацию трафика.[29]

По нашему опыту, система способна перехватывать трафик, выполнять проверку сайта назначения в реальном времени и, в зависимости от результата, разрешать или отклонять запросы.

---

[28] Xue D. и др., «TSPU: Russia's Decentralized Censorship System» («TSPU: децентрализованная система интернет-цензуры в России»), в: Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22) (New York: Association for Computing Machinery, 2022), с. 179–194, https://doi.org/10.1145/3517745.3561461

[29] "How TSPU and DPI Work: An Analysis of Traffic Filtering and Blocking Mechanisms" (Как работают ТСПУ и DPI: разбор механизмов фильтрации и блокировок трафика), *Habr,* February 3, 2026, https://habr.com/en/articles/992232/ (accessed March 18, 2026)

ГРЧЦ, или кто на самом деле управляет системой

Роскомнадзор — это регулятор и политико-административный центр системы цензуры, но её техническим крылом выступает Главный радиочастотный центр, или ГРЧЦ. Расследование The Insider, основанное на документах утечки описывает ГРЧЦ как заказчика и центр управления поставкой, установкой и эксплуатацией ТСПУ, где компания ДЦОА выступает системным интегратором, а такие поставщики, как RDP.ru и Yadro, участвуют в поставке оборудования и программного обеспечения.[30] Иными словами, ГРЧЦ выступает как организация, управляющая развёрнутым оборудованием.

Данные со стороны провайдеров подтверждают ту же картину. Один из сотрудников провайдера заявил, что система проектируется, устанавливается, настраивается и проверяется Роскомнадзором или его подрядчиками. Оператор связи не может её отключить, но в случае поломок все равно несёт ответственность за любой трафик проходящий мимо системы.[31]

Официальное разъяснение ГРЧЦ, о котором сообщала «Цифровая Россия», добавляет важные процедурные детали. Малые операторы с трафиком до 10 Гбит/с могут не устанавливать оборудование локально только в том случае, если маршрутизируют трафик через вышестоящего оператора, у которого он уже проходит через ТСПУ; крупные операторы и точки обмена трафиком обязаны устанавливать ТСПУ в собственных сетях. Иными словами, Россия выстроила политико-правовые механизмы, чтобы **минимизировать пробелы в покрытии даже тогда, когда локальный провайдер слишком мал, чтобы сам размещать это оборудование.**

Как ТСПУ устанавливали у российских провайдеров

Закон о суверенном интернете 2019 года **сделал ТСПУ обязательным** и возложил на Роскомнадзор обязанность по его поставке. В раннем анализе DGAP (German Council on Foreign Relations) отмечалось, что закон требует от всех провайдеров установить ТСПУ, причём Роскомнадзор должен предоставлять его бесплатно, одновременно наделяя государство полномочиями по централизованному управлению сетью в случаях, которые оно определяет как угрозы.

---

[30] Vasilyev P., «TSPU Installation» («Установка ТСПУ»), https://pavel.su/internet/setting-up-tspu/

[31] «Traffic Routing Schemes Through TSPU — GRFC» (О схемах пропуска трафика через ТСПУ — ГРЧЦ), *Digital Russia*, February 16, 2024, https://d-russia.ru/o-shemah-propuska-trafika-cherez-tspu-grchc.html.

Позднее журналистские расследования раскрыли и сторону закупок. The Insider сообщал о контрактной фазе 2020 года на **4,3 миллиарда рублей** и о запланированных расходах на 2022–2024 годы в размере **24,7 миллиарда рублей** на поставку и эксплуатацию, включая DPI-устройства EcoFilter, серверы Huawei и другие сетевые компоненты, причём ТСПУ размещалось в точках соединения операторов с «большим интернетом».

Публичные сообщения 2024 и 2026 годов указывают, что развёртывание стало почти повсеместным среди крупных операторов. В публикации Habr от января 2026 года, суммирующей заявления Роскомнадзора, говорилось, что с августа 2023 года все узлы подключения у крупных провайдеров были оснащены ТСПУ, а регулятор теперь сосредоточен на соблюдении требований по установке и постоянной модернизации.[32]

В той же публикации на Habr отмечается, что операторы обязаны предоставлять место, электропитание и удалённый доступ для ГРЧЦ, Роскомнадзора и производителей и не должны препятствовать удалённому управлению. Таким образом, российское государство не просто требует от операторов купить оборудование — оно встраивает управляемое государством оборудование в сети провайдеров и сохраняет над ним оперативный контроль.

Описания со стороны операторов ещё конкретнее. Процесс установки начинается с того, что Роскомнадзор или его подрядчик связывается с оператором, запрашивает информацию о топологии и нагрузке, согласует схему врезки и затем размещает ТСПУ на uplink-каналах так, чтобы весь трафик, включая транзитный, проходил через него.

ТСПУ — непрерывно развивающаяся программно управляемая система

В 2026 году мы видим, что ТСПУ — это непрерывно обновляемая платформа.

Публикация Habr от января 2026 года раскрывает, что уже установленные комплекты ТСПУ требуют постоянной модернизации из-за роста трафика и что на узлах устанавливается дополнительное оборудование, чтобы поспевать за нагрузкой.

Роскомнадзор описывает явно программно эволюционирующий слой противодействия обходу. TAdviser в январе 2026 года сообщал,

[32] «Roskomnadzor Identified Violations in TSPU Installation at 33 Telecom Operators in Russia» («Роскомнадзор выявил нарушения установки ТСПУ у 33 операторов»), Habr, February 12, 2026, https://habr.com/en/news/984470/.

что Роскомнадзор планирует систему фильтрации трафика на основе машинного обучения стоимостью 2,27 миллиарда рублей, предназначенную для расширения функциональности ТСПУ и более точечной деградации конкретных типов трафика.[33]

Reuters сообщал в сентябре 2024 года, что Россия планирует выделить почти 60 миллиардов рублей за пять лет на усиление системы цензуры.[34] Более свежие публикации TechRadar в 2026 году со ссылкой на экспертов и VPN-операторов указывают, что анализ трафика с помощью ИИ уже стал частью текущей среды принуждения.

В данном случае это означает, что **рассматривать ТСПУ как статичный список сигнатур было бы ошибкой**. Система становится всё более итеративной: сигнатуры, эвристики, активный мониторинг и правила на уровне инфраструктуры непрерывно обновляются.

Почему централизованный обход стал настолько трудным

Первоначальные версии режима цензуры часто можно было обойти, скрывшись за общей инфраструктурой или сменив домены. Современное ТСПУ **позволяет единообразно и почти в реальном времени управлять множеством сетей**, вне зависимости от технической квалификации каждого отдельного провайдера. В статье на Habr говорится, что новая архитектура даёт Роскомнадзору возможность навязывать единообразную цензуру по всей стране в реальном времени без опоры на технические возможности провайдеров или только на реестр блокировок.

Это делает централизованный обход особенно уязвимым. Если бы ваша компания развернула небольшое число общих fallback-транспортов, узкий набор relay-endpoints или стабильную сигнатуру, которую использует очень большая российская аудитория, такой паттерн был бы особенно легко заметен и классифицируем для цензора.[35] Система как раз и создана для того, чтобы выявлять повторяющиеся отпечатки протоколов, подозрительные паттерны SNI и потоки трафика, связанные с известной инфраструктурой обхода.[36]

---

[33] «Roskomnadzor's Policy on Internet Control» («Политика Роскомнадзора по контролю интернета»), TAdviser, 25 марта 2026 г., https://tadviser.com/index.php/Article:Roskomnadzor%60s_policy_on_Internet_control.

[34] Stolyarov G., Papachristou L., «Russia to Spend Over Half a Billion Dollars to Bolster Internet Censorship System» («Россия потратит более полумиллиарда долларов на усиление интернет-цензуры»), Reuters, 11 сентября 2024 г., https://www.reuters.com/world/europe/russia-spend-over-half-billion-dollars-bolster-internet-censorship-system-2024-09-10/.

[35] Castro C., «Russia's Battle Against VPNs Is Entering a New Phase: Here's What to Expect in 2026» («Борьба России с VPN вступает в новую фазу: чего ожидать в 2026 году»), TechRadar, 24 января 2026 г., https://www.techradar.com/vpn/vpn-services/russias-battle-against-vpns-is-entering-a-new-phase-heres-what-to-expect-in-2026.

[36] «[Russia] Censor Has a New Method of Blocking #490», Net4People BBS (GitHub), https://github.com/net4people/bbs/issues/490.

Наш собственный опыт приводит к тому же практическому выводу, но уже не из исследований, а из практики. Приложение «Навальный» специально строилось так, чтобы выдерживать ограничения Роскомнадзора: оно использовало специальный сервис с режимом ротации адресов и автоматически перенаправляло пользователей от заблокированных серверов (см. ниже раздел об «Умном голосовании» для дополнительных деталей).

Иными словами, наиболее устойчивая модель сочетает децентрализованное распространение, гибкость конфигурации и маскировку протокола. Это противоположность стандартной идее использования единого метода обхода блокировок.

Успешные кейсы противостояния Роскомнадзору

Telegram как успешный кейс противодействия блокировкам

В 2018 году Роскомнадзор принял решение о блокировке мессенджера Telegram. Но потерпел неудачу — сервис в итоге пришлось официально снять блокировки в 2020 году, но фактически они закончились гораздо раньше.

Устойчивость Telegram стала поворотным моментом: она продемонстрировала слабость старого подхода к интернет-контролю и объясняет последующий разворот политики. Пользователи и сам Telegram опирались на прокси, VPN, инфраструктурные манёвры и другие низовые тактики, тогда как правовые и технические усилия Роскомнадзора оставались неполными и дорогостоящими.

Эксперты прямо связывают провал кампании против Telegram в 2018 году с последующим политическим решением установить DPI-оборудование у провайдеров за государственный счёт и формализовать эту программу в рамках закона о суверенном интернете.[37]

Это важно, потому что означает, что успех Telegram не является подходящим прецедентом для какого бы то ни было приложения сегодня, если не учитывать, что тогда это происходило в «до-ТСПУ-эпоху». То, что работало против тяжеловесной блокировки по IP в 2018 году, нельзя считать работающим против распределённого, управляемого государством DPI в 2026-м.

По состоянию на февраль 2026 года контраст очевиден: нынешняя кампания против Telegram опирается на ТСПУ, установленное у всех крупных российских провайдеров, позволяет точечно замедлять отдельные типы трафика, например зашифрованные голосовые звонки, и её сложнее обойти, чем прежнюю грубую блокировку.[38] У государства теперь **есть необходимые инструменты и средства, чтобы заблокировать Telegram полностью**.[39]

---

[37] Ermoshina K., Musiani F., «The Telegram Ban: How Censorship „Made in Russia“ Faces a Global Internet» («Запрет Telegram: как цензура „сделано в России“ сталкивается с глобальным интернетом»), First Monday, т. 26, № 5 (2021), https://doi.org/10.5210/fm.v26i5.11704.

[38] «No Country for Telegram: Russia Starts Second Attempt to Block One of Its Most Popular Messengers» («Не страна для Telegram»), Mediazona, February 10, 2026, https://en.zona.media/article/2026/02/10/telegram.

[39] Lyndell D. и др., «Putin's Digital Iron Curtain: Russia Bypasses Sanctions, Buys Equipment to Block YouTube and Telegram» («Цифровой железный занавес Путина»), The Insider, October 11, 2023, https://theins.ru/en/politics/265749.

«Умное голосование»: более релевантный кейс в современных условиях

Умное голосование — электоральная стратегия на выборах, которая позволяла благодаря координации избирателей снижать итоговые проценты у кандидатов от власти на выборах разного уровня. В 2021 году для реализации данной стратегии использовалось приложение «Навальный» для доставки рекомендованных кандидатов.

Кейс этого приложения крайне релевантен, потому что он демонстрирует весь **путь эскалации российского давления**: блокировку доменов, DPI-вмешательство, инфраструктурную адаптацию со стороны цели, давление на магазины приложений и, в конечном итоге, принуждение, направленное уже на само распространение.

Внутренние ретроспективные материалы нашей команды показывают, что после того, как ТСПУ было широко развёрнуто у провайдеров, поддерживать сам сайт имело всё меньше смысла, потому что он уже был заблокирован Роскомнадзором и оставался доступным в основном через VPN. Это подтолкнуло команду использовать приложения для Android и iOS, а также Telegram-бот как альтернативные каналы доставки.

Самый важный технический урок заключается в том, что **приложение «Навальный» не опиралось на один статичный бэкенд** и не зависело от обычного цикла обновления приложения в магазинах приложений Apple и Google, чтобы оставаться доступным. Ему была нужна синхронизация списков кандидатов почти в реальном времени, потому что рекомендации «Умного голосования» публиковались незадолго до выборов и зависели от подбора кандидата по адресу, а задержки с ревью в Google Play и App Store делали обновления через магазины приложений слишком медленными для среды активной цензуры. Чтобы решить эту проблему, команда создала собственный механизм обнаружения на основе подписанной JSON-конфигурации с учётом ротации с низким TTL, обнаружения через DNS-over-HTTPS и подделки SNI, что позволяло приложению узнавать новые адреса backend без необходимости выпускать новый релиз в магазине каждый раз, когда Роскомнадзор блокировал очередную точку подключения.

Затем наша **стратегия обхода развилась в «превентивную ротацию»**. Команда перебирала домены третьего уровня, субдомены App Engine, большие пулы заранее зарегистрированных доменов второго уровня, а позднее — домены за CDN у таких провайдеров, как Bunny, Fastly и Amazon CloudFront, используя то обстоятельство, что Роскомнадзору часто требовались минуты, а не секунды, чтобы обнаружить и подавить новый endpoint. Публичный отчёт ФБК описывает, как некоторые из этих

подходов вынуждали цензора делать всё более дорогой выбор: либо продолжать гоняться за отдельными точками, либо эскалировать к более широким блокировкам по регулярным выражениям, зонам или целым платформам, рискуя побочным ущербом. Команда отслеживала эту борьбу операционно через распределённую сеть мониторинга на базе более 50 точек наблюдения у российских провайдеров. Эта система использовалась для принятия решения о следующей ротации адресов. Позднее сеть мониторинга не могла продолжать существование из-за наличия рисков преследования со стороны российских властей которые возникли в результате необходимости установки конечного оборудования у реальных пользователей в России.

Приложение также экспериментировало с более серьёзными fallback-слоями, чем обычное проксирование. Клиентский domain fronting, fallback-обнаружение через DoH и облачное хранилище, а также даже экспериментальная интеграция идей peer-to-peer-транспорта в духе NewNode были направлены на снижение зависимости от обычного DNS и прямой связности.

Именно поэтому этот кейс важен: приложение «Навальный» уже тогда использовало модель, в которой устойчивость обеспечивалась не каким-то одним «рабочим прокси» или стабильным доменом, а **гибкостью транспорта, гибкостью обнаружения и распространением вне нормальных веб-потоков**.

Открытые публикации показывают, как на это отвечало государство. Apple и Google под давлением российских властей удалили приложение «Навальный» накануне выборов сентября 2021 года, а Telegram также ограничил связанные каналы распространения.[40] Это показало, что, когда сетевых мер оказалось недостаточно, российские власти переключились на постепенное уничтожение экосистемы доставки вокруг продукта.[41] Внутренние оценки команды шли ещё дальше и предполагали, что если бы удаление из магазинов не сработало, государство было готово эскалировать к более широким краткосрочным нарушениям работы сети. Хотя к этому следует относиться как к внутренней операционной оценке, а не как к полностью задокументированному публичному факту, это соответствует технической и политической траектории российского интернет-управления.

---

[40] Feldstein S., Weiss A., «Sideswiped: Apple, Google, and the Kremlin's Make-Believe Election» («Удар сбоку: Apple, Google и фиктивные выборы Кремля»), Фонд Карнеги за международный мир, September 23, 2021, https://carnegieendowment.org/russia-eurasia/posts/2021/09/sideswiped-apple-google-and-the-kremlins-make-believe-election.

[41] Navalny Team, «РКН против приложения „Навальный“: борьба за доступность», Dev.to, 14 сентября 2023 г., https://dev.to/navalnyteam/rkn-protiv-prilozhieniia-navalnyi-borba-za-dostupnost-2gg6.

Для любого, готового сопротивляться цензуре, вывод не в том, что его приложение столкнётся ровно с тем же профилем уязвимости в магазинах приложений, что и «Навальный». Более важный урок в том, что, если российское государство сочтёт цензуроустойчивое приложение достаточно политически опасным, оно может быть **готово на очень высокий побочный ущерб** и эскалировать от блокировки конкретного сервиса к значительно более широким сетевым сбоям, лишь бы ухудшить его доступность. В этом смысле «Навальный» лучше понимать не просто как случай подавления оппозиционного приложения, а как раннее предупреждение о том, насколько далеко российское государство готово зайти, когда **адаптивная технология обхода цензуры воспринимается как прямая политическая угроза**.

Современное состояние интернет-цензуры в России

Состояние блокировок VPN в 2025–2026 годах

Имеющиеся данные сейчас убедительно подтверждают вывод, что **Россия способна блокировать или существенно ухудшать работу большинства популярных VPN-протоколов**. Human Rights Watch сообщала в марте 2026 года, что Роскомнадзор заблокировал 469 VPN-сервисов и с декабря 2025 года блокирует три самых популярных VPN-протокола.

Экспертные социальные и технические каналы задокументировали и более ранние волны. Архив Telegram-канала SecurityLab сообщал о массовом нарушении работы OpenVPN в мае 2023 года, о крупных блокировках OpenVPN и WireGuard в августе 2023 года, а вскоре после этого — о более широких сбоях OpenVPN, IKEv2, IPsec и WireGuard как у мобильных, так и у фиксированных операторов.[42]

К 2026 году публичный консенсус сместился от «используйте VPN» к **«используйте правильное семейство транспортов, аккуратно настроенное, и ожидайте постоянной турбулентности»**. В публикации TechRadar за январь 2026 года со ссылкой на Amnezia и других операторов говорится, что большинство VPN-протоколов блокируется, а более устойчивыми вариантами остаются протоколы, маскирующиеся под обычный трафик, включая, VLESS, а также NaiveProxy, Hysteria и AmneziaWG при правильной настройке.

Статья Habr о VLESS делает похожий, хотя и более субъективный вывод: OpenVPN, WireGuard, Shadowsocks, Trojan и VMess уже в значительной степени деградированы или детектируются, тогда как VLESS с TLS, WebSocket и CDN-fronting остаётся одним из немногих сравнительно живучих подходов.[43] Даже если относиться к некоторым процентам из статьи осторожно, её техническое направление соответствует более широким публикациям и полевой практике.

Внутренняя документация и обсуждения ФБК независимо приходят к тому же выводу. Большинство протоколов блокируется, а VPN-провайдеры ведут **постоянную войну технологий с ГРЧЦ**.

---

[42] Chiara Castro, “Russia’s Battle Against VPNs Is Entering a New Phase: Here’s What to Expect in 2026,” *TechRadar,* January 24, 2026, https://www.techradar.com/vpn/vpn-services/russias-battle-against-vpns-is-entering-a-new-phase-heres-what-to-expect-in-2026.

[43] «The VLESS Protocol: How It Bypasses Censorship in Russia and Why It Works» («Протокол VLESS: как он обходит цензуру в России и почему работает»), Habr, February 17, 2026, https://habr.com/en/articles/990144/.

Подозрительные подсети и репутация IP-адресов теперь тоже имеют значение

Российская интернет-цензура теперь уже **не ограничивается отпечатками протоколов**. Похоже, она всё больше учитывает репутацию инфраструктуры, эвристики назначения и регионально специфические правила.

В отчёте Net4People за июнь 2025 года описывается метод, при котором TCP-соединения с «подозрительными» IP иностранных дата-центров зависают после примерно 15–20 КБ данных ответа сервера, особенно в мобильных сетях, даже когда соединение выглядит как HTTPS-трафик, похоже на HTTPS или VLESS, Reality over TLS 1.3. В примерах прямо упоминаются Hetzner, DigitalOcean, Cloudflare, OVH, Oracle и AWS.

Независимое обсуждение на форуме Tor Project задокументировало схожую реальную поломку для диапазонов IP Hetzner: TCP на всех портах перестаёт получать ответы SYN, UDP не работает, ICMP при этом продолжает работать, блокировка временная, но легко воспроизводимая, и эффект может распространяться и на другие сети дата-центров, например OVH.[44]

Внутри нашей IT-команды мы также замечали множество ситуаций с таким же поведением у российских провайдеров и пришли к тому же выводу, который сформулирован выше.

В данном случае практический вывод очевиден: стратегия обхода, которая слишком сильно концентрируется на нескольких известных иностранных облачных провайдерах или стабильных ASN дата-центров уязвима. Даже если протокольный слой замаскирован, инфраструктурный слой всё равно может быть **оценён как подозрительный и подвергнут деградации**.

Encrypted Client Hello (ECH): заблокирован и неэффективен

Encrypted Client Hello (ECH) — это расширение TLS 1.3, которое шифрует сообщение ClientHello, включая поле SNI (Server Name Indication), традиционно используемое DPI-системами для определения того, к какому домену направлено соединение. Хотя ECH задумывался как «последний недостающий элемент приватности» в TLS, в условиях государственной цензуры в России **он показал высокую уязвимость**.

[44]«Tor and Hetzner Block in Russia», Tor Project Forum, December 2024, https://forum.torproject.org/t/tor-and-hetzner-block-in-russia/16134 (accessed March 20, 2026).

В октябре 2024 года Cloudflare включил ECH по умолчанию для своих клиентов. Уже через месяц, 5 ноября 2024 года, Роскомнадзор **начал блокировать ECH-соединения через ТСПУ**. Блокировка срабатывает, когда ClientHello содержит одновременно и расширение ECH, и значение SNI. Подходящие пакеты незаметно отбрасываются, что затрагивает как TLS, так и QUIC-трафик, но только в отношении IP-диапазонов, анонсируемых Cloudflare. Тысячи сайтов, размещённых за Cloudflare, стали недоступны для российских пользователей. Роскомнадзор заявил, что ECH **«нарушает российское законодательство и ограничивается средствами ТСПУ»**.[45]

ECH не работает как инструмент обхода цензуры по нескольким причинам. Cloudflare остаётся практически единственным крупным провайдером, который его поддерживает. Фиксированный внешний Cloudflare SNI делает фильтрацию тривиальной. ECH зависит от зашифрованного DNS для получения конфигурации сервера, поэтому **достаточно заблокировать сами DNS-резолверы, чтобы помешать использованию ECH**. ECH создавался как механизм приватности, а не как инструмент обхода цензуры, и этой второй роли он не выполняет. Он может дополнять инструменты обхода DPI вроде Zapret или GoodbyeDPI, но как самостоятельное решение против фильтрации государственного уровня он неэффективен.

Тесты интернета по «белому списку» в Москве

Сообщения из Москвы в марте 2026 года указывают на то, что Россия экспериментирует с ещё более жёстким режимом: не просто блокировать отдельные направления, а разрешать доступ только к одобренному набору сайтов и сервисов во время отключений или в исключительных условиях.[46]

Согласно этим сообщениям, модель белого списка на данном этапе позволяет доступ лишь к провластным социальным платформам, государственным медиа и официальным государственным ресурсам, что означает качественный сдвиг по сравнению с более ранними фазами цензуры, сосредоточенными только на блок-листах и замедлении. На практике такой режим особенно враждебен централизованному обходу, потому что глобальный relay, стабильный fallback-домен или любой устойчивый альтернативный control plane можно просто не включить в разрешённый набор на сетевом уровне.

---

[45] «Encrypted Client Hello Didn't Solve Censorship», AdGuard DNS Blog, November 25, 2024, https://adguard-dns.io/en/blog/encrypted-client-hello-misconceptions-future.html.

[46] Zadorozhnyy T., «Moscow Citizens Turn to Pagers, Printed Maps» («Жители Москвы переходят на пейджеры и бумажные карты»), The Kyiv Independent, March 14, 2026, https://kyivindependent.com/moscow-citizens-turn-to-pagers-printed-maps/.

В то же время ранняя полевая практика уже показывает, что даже **ограничения в стиле белого списка в некоторых случаях можно обходить**, если туннелировать трафик через инфраструктуру, которая остаётся доступной, потому что принадлежит одобренным внутренним сервисам. Один показательный пример — vk-turn-proxy, открыто опубликованный инструмент, который проксирует трафик WireGuard или Hysteria через TURN-серверы VK Calls, а ранее также Yandex Telemost, вместо того чтобы отправлять этот трафик напрямую на иностранный VPN-endpoint. Как указано в его документации, инструмент генерирует TURN-учётные данные из ссылки на звонок VK, инкапсулирует пакеты в DTLS 1.2, отправляет их по параллельным TCP- или UDP-потокам с использованием STUN ChannelData, а затем TURN-сервер пересылает трафик по UDP на собственный сервер пользователя, где он расшифровывается и передаётся WireGuard. Тот же проект также документирует пути интеграции для клиентов V2Ray/Xray, позволяя использовать SOCKS- или HTTP-проксирование поверх того же транспорта, а не только обычный туннель в стиле WireGuard.[47]

Это важное свидетельство, потому что оно показывает: даже **режим белого списка не гарантирует полной блокировки** — если цензор оставляет доступной внутреннюю платформу реального времени, её media-relay- или TURN-инфраструктура потенциально может быть переиспользована как транспортная основа для обхода цензуры. Но было бы ошибкой чрезмерно обобщать этот факт. Сам репозиторий документирует и практические ограничения, включая прекращение поддержки Yandex Telemost, ограничения скорости, связанные с VK, необходимость ручного выбора TURN в некоторых случаях, настройку MTU, маршрутизационные трюки и риск того, что менее замаскированные режимы приводят к банам или быстрому выходу из строя.

Ключевой вывод: хотя обход белого списка технически может быть возможен на периферии, гораздо **менее ясно, как такой подход можно было бы превратить в централизованную, продуктовую систему** масштаба «крупного bigtech-приложения»: массовое развёртывание было бы гораздо заметнее, зависело бы от российской инфраструктуры третьих сторон, которую вы не контролируете, и почти наверняка вызвало бы быстрые контрмеры. Иными словами, даже если обход белого списка в принципе возможен, превращение его в устойчивую централизованную стратегию для приложения потребовало бы значительных постоянных инженерных усилий, непрерывной адаптации и готовности к стремительно эскалирующему противостоянию с цензором.

[47] "vk-turn-proxy," *GitHub*, https://github.com/cacggghp/vk-turn-proxy.

Проблема мониторинга: почему нельзя полагаться на простой внешний зонд

Одна из самых трудных практических проблем — это мониторинг. До сих пор **нет простого, полного и надёжного способа извне страны ответить на вопрос «доступен ли сейчас этот сервис из России?»**. В статье с измерениями ТСПУ прямо говорится, что отвечать на такие вопросы трудно, потому что исследователям нужны локальные точки наблюдения в российских сетях, где развёрнуто ТСПУ, а асимметричный характер ограничений ТСПУ делает стандартные удалённые измерения недостаточными для многих случаев. К тем же выводам пришла и наша команда в ходе внутренней разработки некоторых приложений.

OONI — это наиболее важная открытая инициатива по сетевым измерениям в этой сфере, и она по-прежнему ценна, но даже OONI не снимает проблему полностью. Её данные зависят от добровольческих probe-узлов, покрытие различается в зависимости от сети и времени, а в 2024 году Россия заблокировала OONI Explorer именно потому, что он содержал информацию, связанную с обходом цензуры.[48]

Собственный недавний анализ OONI подтверждает и ценность, и ограниченность открытых измерений. Он находит убедительные признаки **широко распространённого TLS-вмешательства** во множестве российских сетей и утверждает, что цензура, по-видимому, централизованно управляется через децентрализованное развёртывание ТСПУ, но этот вывод по-прежнему опирается на распределённые волонтёрские точки наблюдения, а не на некий простой универсальный мониторинг.

Наша команда также раньше управляла сетью мониторинга внутри России, используемой для тестирования доступности интернет-ресурсов у разных провайдеров, и эта сеть позднее была демонтирована под давлением государства, а некоторые участники были вынуждены покинуть страну. Аналогичные средства мониторинга, связанные с несколькими другими проектами, также частично деградировали или стали недоступны. Это показывает, что российское государство воспринимает такие усилия как угрозу своему цензурному процессу.

В данном случае практическое следствие состоит в том, что внешние пробы необходимы, но недостаточны. Более масштабируемым сигналом, вероятно, является продуктовая телеметрия: показатели успешности соединений, типы ошибок handshake, сдвиги задержек, частота перехода на fallback-транспорты, выявление аномалий по географии и ASN и сравнительная успешность разных транспортных вариантов.

---

[48] Xynou M., «Russia Blocked OONI Explorer, a Large Open Dataset on Internet Censorship» («Россия заблокировала OONI Explorer — крупный набор данных о цензуре интернета»), OONI, September 25, 2024, https://ooni.org/post/2024-russia-blocked-ooni-explorer/.

Выводы и предложения

Обход DPI

Когда полноценный VPN недоступен или нежелателен, в качестве fallback-варианта можно использовать такие инструменты, как Zapret и GoodbyeDPI. Оба решения работают локально, не требуют подключения через сторонние серверы и предназначены для обхода DPI на базе ТСПУ; Zapret описывается как автономный многоплатформенный инструмент обхода DPI, а GoodbyeDPI предлагает аналогичный подход для систем Windows.

На практике это означает, что **они всё ещё могут помогать восстанавливать доступ к таким сервисам, как Telegram или WhatsApp**, когда прямое соединение не работает. GoodbyeDPI поддерживает такие техники, как фрагментация пакетов, модификация HTTP/TLS-запросов, инъекция поддельных пакетов и специальная обработка QUIC/HTTP3, а Zapret включает методы десинхронизации DPI, повторную передачу поддельных пакетов и специализированные профили для протоколов и сервисов, включая QUIC и Discord; по этой причине имеет смысл добавлять сопоставимую клиентскую fallback-логику и автоматически переключаться на поведение обхода DPI, когда клиент не может достичь целевых хостов по обычному пути соединения.[49] Однако некоторые из этих методов требуют низкоуровневых сетевых API, которые обычно ограничены на Android и iOS, что делает **необходимым сотрудничество с разработчиками ОС**.[50]

Выводы для стратегии обхода

Исходя из приведённых выше данных, наша команда **рекомендует следующее**:

1. Централизованная программа обхода жизнеспособна только как постоянная инженерная функция

Данные показывают, что **можно сохранить доступность для части пользователей с помощью централизованно управляемого слоя обхода**, но только если относиться к нему как к **постоянной операционной функции**, а не как к «одноразовой акции». Российская система обновляет сигнатуры, масштабирует инфраструктуру, атакует распространение приложений и всё больше оценивает как протоколы, так и среды хостинга.

---

[49] ValdikSS, «goodbyeDPI», GitHub, https://github.com/ValdikSS/goodbyeDPI.

[50] bol-van, «zapret», GitHub, https://github.com/bol-van/zapret.

На практике это требует **выделенной команды, ежедневно работающей над изменениями транспортов, диверсификацией endpoint, анализом телеметрии и реагированием на инциденты**. Без этого любое фиксированное решение, скорее всего, быстро деградирует.

2. Избегайте стандартных предположений о VPN

Слой обхода в приложении не должен исходить из того, что OpenVPN, IKEv2, IPsec или vanilla WireGuard — это надёжные технологии для России. Открытые публикации и операционные данные показывают повторяющиеся массовые сбои этих протоколов.

Более устойчивые подходы сегодня включают VLESS, транспорты в стиле XRay, AmneziaWG, NaiveProxy, Hysteria и другие протоколы с тяжёлой маскировкой, но и к ним следует относиться как к **подвижным целям, а не как к постоянным решениям**.

3. Распространение и обнаружение — это часть модели угроз

Если функции обхода зависят от очевидных страниц настроек, обновлений через store, одного домена или стабильного опубликованного списка endpoint, эти поверхности станут целями.

Следует исходить из необходимости тихой серверной активации, remote config, нескольких путей обнаружения, piggybacking на сервисы, которые вряд ли будут заблокированы целиком, а также продумать внеполосные bootstrap-методы, не зависящие от одного публичного домена. Эта рекомендация напрямую следует из опыта обновления и распространения методов обхода блокировок, наблюдавшихся в «Умном голосовании».

4. Измеряйте доступность прежде всего через телеметрию, а не через один внешний стек мониторинга

Поскольку ТСПУ располагается в непосредственной близости к конечным пользователям, а стандартные удалённые измерения не дают полной картины, собственную телеметрию следует рассматривать как основной источник оценки доступности. При этом **мониторинг, выполняемый изнутри России, остаётся полезными, но должен использоваться лишь как дополнительный уровень** подтверждения.

5. Низовая стратегия может оказаться реалистичнее, чем централизованная гонка технологий

Наиболее реалистичным среднесрочным вариантом может быть **низовая стратегия, а не полностью централизованная система обхода**. Публичная коммуникация, поощряющая использование VPN, поддержка

проектов по обходу, совместимость с устойчивыми транспортами и выборочные функции P2P или peer-assisted delivery могут дать более долговечный результат, чем единый протокол, который государство сможет классифицировать как ещё одну цель.

Однако peer-to-peer-доставка может осложняться тем, что вас потенциально **могут признать экстремистами в России**. Решение этой проблемы может потребовать **нетривиальных мер** — например, обеспечения того, чтобы коммуникационные каналы оставались трансграничными, и внедрения механизмов информированного согласия для пиров, чтобы избегать проблем, если, к примеру, человек поедет в Россию, используя гипотетическое приложение «App P2P relay». Поэтому необходим дополнительный юридический анализ, чтобы оценить риски для сотрудничающих пиров и возможный ущерб вашей репутации, если эти риски реализуются. Примечательные примеры преследования пользователей за использование софта включают, во-первых, преследование пользователей мессенджера ByLock в Турции в 2016 году (см. решение Европейского суда по правам человека по делу Yalçınkaya v. Türkiye). Во-вторых, пользователей BitTorrent преследовали не за скачивание защищённого авторским правом материала, а за его распространение («сидирование»).

Рекомендуемые шаги, которые стоит сделать уже сейчас

1. **Создать выделенную функцию по противодействию цензуре в России** с ответственностью за протоколы, инфраструктуру, SRE и измерения.
2. **Построить внутренние метрики доступности в России**, основанный прежде всего на телеметрии вашего приложения по ASN, типу сети, версии приложения, типу handshake и успешности fallback-путей.
3. **Избегать стандартных VPN-протоколов и концентрации на статичных дата-центрах**; диверсифицировать инфраструктуру.
4. **Разработать подключаемые транспорты с тяжёлой маскировкой и механизмы гибкой конфигурации**, которые можно обновлять без необходимости очевидных действий со стороны пользователя.
5. **Изучить, могут ли ограниченные peer-assisted или store-and-forward-компоненты снизить зависимость от небольшого числа централизованно видимых relay** в периоды острых блокировок.
6. **Рассмотреть системный подход, включая поддержку внешних проектов** по обходу цензуры и обучение пользователей, поскольку наиболее живучий паттерн в России — это распределённая адаптация, а не один стабильный централизованный обход.

Заключение

Российскую система интернет-ограничений больше **нельзя описывать как набор разрозненных блокировок, которые можно обойти одной универсальной технической уловкой**. За последние годы государство построило распределённую, но централизованно управляемую систему цензуры, которая стала ближе к пользователю, быстрее реагирует на новые способы обхода и всё активнее сочетает сетевое давление с давлением на инфраструктуру и каналы распространения.

Сейчас противодействовать любым ограничениям мессенджеров в России возможно, но не стоит недооценивать, насколько это сложно и дорого. Рассмотренные здесь данные указывают на то, что любая серьёзная централизованная попытка обхода должна работать как **постоянная система с выделенными инженерами, быстрой итерацией и сильной телеметрией**.

Более реалистичный долгосрочный подход — **гибридный**: сочетать внутреннюю гибкость транспортов и мониторинг с более широкой низовой и экосистемной стратегией. **Российская система цензуры специально спроектирована так, чтобы обнаруживать и отключать единообразные централизованные методы обхода, как только они становятся заметны в масштабе**.

Электронная почта: fbk@fbk.info