Худшие времена Рунета

Обзор интернет-цензуры в России в 2024-м году

Оглавление

От чёрных списков к белым: как развивается интернет-цензура в России

Российский интернет всё больше становится похож на иранский. В реальном времени мы наблюдаем, как власти поэтапно разворачивают «белые списки», постепенно подготавливая переход к суверенному интернету.

В 2012 году цензура в Рунете официально началась с «чёрных списков» - реестра запрещенных сайтов. Эти списки годами публикует Роскомнадзор, российский государственный регулятор в сфере связи, информационных технологий и СМИ. Возникновение такого реестра было агрессивным наступлением на свободу информации и свободу слова, но всё же блокировки основывались на довольно открытой процедуре, что требовало от цензоров соблюдения формальностей и некой публичной ответственности за свои действия. В этой системе кое-как, но работали и инструменты общественного контроля, когда правозащитники могли придавать огласке самые резонансные блокировки, и судебная практика, позволяющая оспаривать неправомерные блокировки, и даже акции протеста, с помощью которых люди выражали своё отношение к запретительным действиям властей.

Теперь в России новая эпоха. Она характеризуется полным контролем властей над сетью внутри страны с помощью системы технических средств противодействия угрозам (ТСПУ). Эта система представляет собой специализированный программно-аппаратный комплекс, который все провайдеры интернета в стране обязаны установить на своих сетях. В обход «чёрных списков» ТСПУ занимается блокировками как отдельных интернет-ресурсов, так и неподконтрольных властям хостинг-провайдеров, протоколов-VPN, других технологических решений, которыми пользуются люди и организации для безопасного доступа в глобальную сеть. Система может также замедлять трафик или полностью отключать интернет в определённых регионах в интересах госбезопасности.

Активно разворачивать ТСПУ в России начали в 2020 году, постепенно охватив всех операторов связи. В 2024 году импортные системы DPI заменили отечественными, чтобы снизить зависимость от западных технологий.

ТСПУ находятся под полным контролем Роскомнадзора. При этом система работает исключительно непрозрачно, непредсказуемо и неизбирательно. Всё более сложные и глубокие блокировки и замедления различных ресурсов и протоколов негативным образом отражаются на связанности сети, вызывая внезапные шатдауны, разрывы и сбои в работе огромного количества ресурсов. Причем вместе с теми ресурсами, которые цензоры целенаправленно стремятся заблокировать, под блокировку попадают совершенно невинные сайты. Но сопутствующие жертвы не становятся поводом для властей пересмотреть свои планы.

А 20 марта 2025 года произошёл невиданный ранее по масштабу сбой Cloudflare. Он затронул регионы от Урала и до Приморья. По подсчётам экспертов по подсетям оказались заблокированы около 1,5 миллиона IP-адресов. Не работали не только VPN, но и многие популярные сайты, в том числе TikTok, Steam, Roblox, Twitch, Epic Games, DeepSeek, Figma, Miro, SoundCloud, Aviasales, Genshin Impact, Duolingo и сайты мобильных операторов.

Роскомнадзор по этому поводу заявил, что чиновники «проведут плановые технические проверки использования зарубежной серверной инфраструктуры российскими службами и операторами связи». Через какое-то время проблема была решена, но эксперты ещё настойчивее заговорили про «иранский сценарий». Этот инцидент был очень похож на тестирование в ходе подготовки к полной блокировке Cloudflare - как это уже сделано в Иране.

В апреле 2025 года на сайте Роскомнадзора появилась рекомендация для владельцев российских частных виртуальных сетей (virtual private network, VPN) отказаться от иностранных протоколов шифрования, «используемых, в том числе, приложениями, предоставляющими доступ к запрещенной информации». Или, если отказаться невозможно, передавать IP-адреса используемых VPN-серверов, чтобы их внесли в специальный список

исключений. Известно о том, что одно из подразделений Роскомнадзора уже ведёт «белый список» IP-адресов, использующих иностранные протоколы шифрования. По состоянию на апрель 2025 года там зарегистрировано 75 тыс. записей, что в 6 раз больше, чем в 2023 году.

Российские цензоры работают над тем, чтобы сделать использование технологии VPN практически невозможной без официального разрешения властей. Все, кто своевременно не заявится и не попадёт в разрешительные списки — под угрозой блокировки.

Так в Иране «белые списки» начинались с запросов властей предоставить им информацию о том, какими иностранными ресурсами пользуются иранские чиновники и бизнес. Получившиеся списки легли в основу системы, когда запрещено всё, что не разрешено. Сейчас в Иране блокируются практически все внешние новостные и развлекательные сайты, все глобальные социальные сети и мессенджеры (Facebook, Twitter (X), YouTube, Telegram и пр.), а также большинство средств обхода блокировок. Исследователи из Article 19 отмечают, что согласно правительственному декрету «О стратегиях увеличения доли внутреннего трафика и противодействия VPN» от ноября 2023 использование VPN в Иране возможно только в случаях, когда это разрешено законом, а в остальных случаях - запрещено». При этом, что такое «законно разрешенные случаи», остаётся неясным, но известно, что власти предпринимают попытки внедрить некие разрешённые VPN для доступа к иностранному контенту, и для их использования нужна специальная регистрация.

В течение всего 2024 года в России происходили блокировки VPN-протоколов через ТСПУ, в результате чего популярные протоколы, которые используют массовые коммерческие VPN оказались неработоспособными. Трудности испытывали и OpenVPN, и WireGuard, и Shadowsocks, что значительно сузило рынок надёжных и доступных средств обхода блокировок. Регулярные крупные сбои у провайдеров, при которых становилась недоступной половина сайтов в интернете, также могут свидетельствовать о плановых тестах на ТСПУ предваряющих «белые списки».

В то же время мы говорим и о том, что в России начинают реализовываться «серые списки». Согласно им цензурируют не только запрещённое - то, что официально входит в «чёрные списки» - но и просто подозрительное,

непонятное. Блокировки тут осуществляются на основе глубокого анализа трафика с помощью DPI и и выявления «подозрительных» IP. Здесь речь снова может идти о примере Ирана. И даже Китая, а котором нет «белых списков» - там ограничиваются чёрными и серыми.

«Серые списки» - это более высокая степень развития цензуры, показатель того, что она долго и успешно работала, наращивала технологии и опыт, которыми умеет пользоваться. Это рука мастера, прошедшего путь совершенствования.

Таков образ российской интернет-цензуры с 12-летней историей.

Контекст 2024 года: самые сильные цензурные ограничения в истории Рунета

В 2024 году в России наблюдался самый высокий уровень цифровой цензуры. И это связано не только с замедлением и последующей блокировкой YouTube, и не только с общим большим количеством новых блокировок. Год назад в России по сути запретили публично говорить о том, что блокировки можно обойти с помощью различных антицензурных решений. Под угрозой наказания средства обхода блокировок нельзя рекламировать, популяризировать и даже делиться научной, технической и статистической информацией о них. А ещё такие решения власти вычисляют и блокируют с помощью системы DPI, а также удаляют из магазинов приложений.

Началось всё с запрета на «популяризацию» средств обхода блокировок, который вступил в силу 1 марта 2024 года (был опубликован 14 ноября 2023).

Он касается информации о любых подобных решениях - анонимайзеры, VPN, Tor, расширения для браузеров и другие инструменты. Невыполнение требований наказывается штрафами от 800 тыс. до 4 млн. рублей, повторное - от 1/20 до 1/10 совокупного размера годовой выручки компании.

Информационные ресурсы также могут попасть под блокировку, если на них размещены инструкции о том, как получить доступ к сайтам, заблокированным Роскомнадзором, или информация, которая убеждает в привлекательности использования таких средств. В тот момент в законе ещё была оговорка, допускающая, в качестве исключения, публикацию научной и статистической информации об антицензурных решениях. Однако к концу года и такие данные оказались под запретом. Запрет на научно-техническую и статистическую информацию о VPN вступил в силу с 30 ноября 2024 года и будет действовать до 1 сентября 2029 года. Юридически теперь осталась лишь одна возможность говорить о VPN - как о средстве обеспечения безопасного удаленного доступа.

В июле 2024 года в России началось замедление YouTube и уже к концу года его трафик упал до 20% от нормальных показателей. Практику замедления власти назвали вынужденной в ответ на «бездействие Google» и несоблюдение компанией российского законодательства. При этом замедление, как средство цензуры не обозначено в российском законодательстве, но оно активно применяется уже не в первый раз - в 2021 году замедление использовали для ограничения работы Twitter за неудаление с площадки запрещенного в России контента.

В декабре 2024 года Роскомнадзор опубликовал проект приказа, которым предлагается обязать операторов предоставлять Роскомнадзору данные о пользователях, посещающих заблокированные сайты - сетевые адреса, место проживания, номера технических средств и IP. Фактически это означает контроль за теми, кто каким-то образом обходит цензуру, отслеживание VPN-пользователей. Однако власти заявляют, что эти меры вводятся в целях кибербезопасности, а не слежки и наказаний.

Развитие темы произошло уже весной 2025 года. Приказ № 5 Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, который был зарегистрирован в Минюсте 31 марта 2025 года снова всколыхнул общество. Судя по заявлению экспертов, ведомство

получает новые полномочия и возможности для наблюдения за пользовательским трафиком. Приказ описывает его взаимодействия с операторами связи, которые теперь обязаны собирать и передавать в Роскомнадзор дополнительные данные, позволяющие идентифицировать подключенные устройства в интернете: IP-адреса, MAC-адреса, IMEI, серийные номера, геолокацию (до уровня муниципального образования)

Уже несколько лет в России для совершения цензуры применяется ТСПУ - технические средства противодействия угрозам. Компоненты ТСПУ интегрированы в сеть операторов связи, что позволяет блокировать сайты и отдельные страницы в интернете, замедлять работу сервисов, а также ограничивать возможность подключения к VPN-протоколам, которые подвергаются блокировкам. В сентябре 2024 года стало известно, что ближайшие 5 лет на модернизацию ТСПУ планируют выделить 60 млрд рублей. Средства направят, в том числе, на более на эффективную борьбу с VPN и другим инструментам обхода цензуры, а также на приобретение нового оборудования и программного обеспечения и разработку новых методов блокировок.

Помимо внереестровых, которые проводятся через ТСПУ, в России всё ещё работают классические блокировки. По данным Роскомсвободы, которая мониторит Реестр запрещённых сайтов, за 2024 год в России было заблокировано 419 140 сайтов (62 тысячи из них без указания госоргана, инициировавшего блокировку). Это вдвое больше чем за 2023 год, когда эксперты зафиксировали 197 тысяч.

По данным OONI для блокировки сайтов в России применяются разные методы, в том числе манипуляции с DNS и TLS man-in-the-middle блокировки, а сами блокировки осуществляются децентрализованно. Провайдеры в некоторых регионах могут применять одновременно несколько методов для блокировки, что может затруднить их обход.

Согласно исследованию OONI российские интернет-провайдеры используют следующие методы для блокировки сайтов:

- Манипуляции с DNS, в некоторых случаях перенаправляющие на блок-страницы
- HTTP man-in-the-middle, показывающий блок-страницы
- TLS man-in-the-middle блокировки
- Вброс RST-пакета после ClientHello во время TLS-рукопожатия
- Завершение сеанса после ClientHello во время TLS-рукопожатия
- Закрытие соединения после ClientHello во время TLS-рукопожатия

В России по-прежнему недоступны сайты независимых медиа, НКО, а также глобальные социальные сети, такие как X, Facebook, Instagram. В 2024 году в этот список добавились мессенджеры Signal, Discord, Session, SimpleX Chat, Viber, а ещё десятки новых российских медиа, зарубежные СМИ и внушительный список сайтов VPN-сервисов и других средств для обхода цензуры.

Российские власти объявили, что планируют увеличить эффективность блокировки VPN до 96% к 2030 году.

Блокировки за информацию про обход блокировок

Ещё в апреле 2024, через месяц после запрета на «популяризацию» средств обхода блокировок, Роскомнадзор отчитался о блокировке 700 материалов про обход блокировок, а также 150 VPN-сервисов. В течение года эта цифра только увеличивалась. В феврале 2025, спустя год после вступления в силу запрета на «популяризацию» VPN Роскомнадзор отчитался о том, что заблокировал уже более 6,3 тыс. страниц в интернете с информацией об обходе блокировок. Штрафов за это время выписали на 19 млн рублей.

В течение прошлого года были заблокированы сайты Amnezia VPN, Lantern, Outline, ProtonVPN, Red Shield, Express VPN, VPN Generator, сайт браузерного расширения Censor Tracker, маркетплейс VPNpay.

Цензура коснулась, в том числе, и исследовательских проектов, причем задолго до того, как в силу вступил официальный запрет на распространение научно-технической информацию о VPN и способах обхода блокировок. В августе 2024 года был заблокирован проект по мониторингу блокировок VPN-протоколов DPIdetector, в сентябре - проект OONI Explorer, предоставляющий открытые данные об интернет-цензуре по всему миру.

Эксперты отмечают, что количество ресурсов, подвергшихся цензуре, может быть в разы больше: в реестр запрещенных сайтов не попадают страницы и сайты, которые сами удалили информацию о VPN и других способах обхода блокировок после соответствующих уведомлений Роскомнадзора. Или же они поставили геоблокировку на конкретные ссылки, сделав их недоступными для пользователей из России. Однако факт цензуры в этих случаях всё равно был.

Удаления антицензурных приложений из AppStore

В 2024 году Роскомнадзор начал прибегать к помощи BigTech-корпораций для осуществления цензуры в российском сегменте интернета.

К Opera, Google и Mozilla были направлены требования удалить из их магазинов расширений плагины для обхода блокировок. Opera такое требование выполнила, удалив в июле 2024 года плагин Censor Tracker. У Mozilla цензоры потребовали удалить, в числе прочих, PlanetVPN, FastProxy и Runet Censorship Bypass, однако компания лишь на непродолжительное время установила геоблокировку на расширения, чтобы оценить собственные риски. Mozilla вернула расширения в магазин, за что позднее была оштрафована российским судом на 3,5 млн рублей за несоблюдение российского законодательства.

Что касается компании Google, то она до сих пор не была замечена в удалении из Google Play сервисов VPN по запросу российских властей. Хотя в марте 2025 года журналисты нашли базу с зарегистрированными требованиями на удаление. Позже эксперты проекта GreatFire, который занимается изучением интернет-цензуры, посчитали, что что за период с 12 марта по 1 апреля 2025 года Россия в лице Роскомнадзора направила в Google Play 214 запросов, нацеленных на 212 VPN-приложений. Кроме приложений требования также включают удаление более 80 тысяч URL-адресов из поиска Google. Но корпорация не последовала за цензорами.

Напротив, корпорация Apple в 2024 отметилась самым тесным сотрудничеством с российскими властями. В июле стало известно, что из российского AppStore было удалено как минимум четыре VPN-приложения - Proton VPN, Red Shield VPN, NordVPN и Le VPN. Позже эксперты насчитали уже около сотни удалённых VPN. Сам Роскомнадзор сообщал о блокировке 197 VPN-сервисов, вероятно, подразумевая и сайты самих VPN.

Одно из самых показательных удалений случилось с приложением Amnezia VPN: в полночь команда получила уведомление от Apple с требованием от Роскомнадзора удаления средства обхода блокировок, а через три часа приложение уже было недоступно в российском AppStore. Корпорация Apple выполняет цезурные требования российских госорганов за считанные часы, без промедлений и без возможности оспорить решение. На призывы к открытости и соблюдению прав человека, исходящие от правозащитников и активистов, корпорация не реагирует.

По требованию Роскомнадзора Apple также удаляла приложения независимых медиа, попавших в России под цензурный каток. В октябре и ноябре 2024 года из выдачи для России пропали приложение «Свобода» с контентом Русской службы Радио Свобода, проектов «Сибирь.Реалии» и «Север.Реалии», приложение Кыргызской службы Радио Свобода, приложение «Настоящее Время». Apple также скрыла ряд подкастов - «The Insider», «Эхо Москвы» и «Что это было?» от BBC Russian Service.

Корпорация Apple сотрудничает с Роскомнадзором, ограничивая для россиян доступ к разным неугодным российским властям приложениям, но одновременно с этим участвует и в антироссийских санкциях. Так приложение RuTube было безвозвратно удалено из AppStore, несмотря на просьбы о восстановлении.

Блокировки VPN-протоколов

Роскомнадзор активно применяет оборудование DPI (Deep Packet Inspection - глубокая проверка пакетов) для анализа трафика и блокировки VPN-протоколов. DPI позволяет анализировать содержимое пакетов данных, которые передаются по сети и фильтровать интернет-трафик на глубоком уровне. Такое оборудование установлено у провайдеров и является частью ТСПУ.

В 2021 году произошли первые случаи блокировок VPN-сервисов. С 2023 началось массовое тестирование VPN-протоколов через ТСПУ. Сначала взялись за протокол Wireguard: его недоступность наблюдалась в Москве и еще нескольких регионах у провайдеров Билайн и МТС. Пользователи также жаловались на недоступность OpenVPN и IKeV2, при этом IP-адреса VPN-серверов не блокировались. Исследователи из аризонского и мичиганского университетов, в 2024 году выпустили исследование, согласно которому блокировка OpenVPN у провайдеров вообще не вызывает затруднений, а для обнаружения подключения затрачивается около 8 секунд с точностью до 85%.

В 2024 году блокировки VPN ужесточились. На протяжении года ограничивалась работа как минимум протоколов ShadowSocks и Wireguard у мобильных операторов. В апреле-мае 2024 года были замечены попытки блокировок прокси-протоколов, таких, как VMess и Shadowsocks (и, следовательно, использующего его Outline).

В протоколах VMess и Shadowsocks передаваемые данные зашифрованы. Как минимум один из шаблонов блокировки на цензурирующем оборудовании для всех неопознанных протоколов выглядит так:

1. Клиент отсылает три пакета, каждый из которых содержит 411+ случайных байт.
2. Сервер отсылает произвольное количество любых байт чаще, чем клиент отправляет свои пакеты.

При выполнении этих условий подключение блокируется. Также есть предположение, что блокировки осуществляются по размеру пакетов или по соотношению размера отправляемого к принимаемому.

Были зафиксированы сообщения о сбоях в Outline, а также о проблемах в работе SSTP, Cloak (если там стоял «дефолтный»SNI под маскировку: googletagmanager.com или yahoo.com). При этом проблемы с Cloak могли быть из-за того, что не все фингерпринты были своевременно обновлены.

В ноябре 2024 года были описаны своеобразные кейсы блокировки SSH-протокола на ТСПУ:

- Провайдер блокирует SSH-доступ к серверам, если на них ранее были замечены детектируемые ТСПУ VPN-протоколы (например, Shadowsocks и OpenVPN).
- Блокировка применяется только при попытке авторизации по SSH-ключу. При этом смена ключей или их типа не решает проблему. Авторизация по паролю остается доступной и стабильной.
- DPI на уровне ТСПУ полностью блокирует пакеты после определенного пакета в соединении, что вызывает тайм-ауты и разрывы. Вмешательств в сам трафик (вставка "левых" пакетов) не наблюдается.
- Подключение по SSH через VPN остается успешным, поскольку DPI не видит непосредственно SSH-протокола внутри шифрованного туннеля.
- Блокировка осуществляется на основе анализа трафика и«подозрительности» IP, что подтверждается отсутствием проблем с серверами без VPN-протоколов.

Наряду с VPN-протоколами Роскомнадзор также занимался блокировкой Snowflake, который используется в Tor для обфускации соединения для обхода блокировки. Сама блокировка, вероятно, осуществлялась с помощью ограничения прямого доступа к мостам или с помощью отличительных

признаков DTLS-фингепринтов у Snowflake. В ноябре 2024 в России был зафиксирован резкий спад пользователей Snowflake, однако тогда тестирование не выявило применение DTLS-фингерпринтинга, ранее использованного для блокировок.

Измерения блокировок VPN-протоколов

Выявлять блокировки VPN-протоколов можно, в частности, через инструмент для исследования интернет-цензуры DPIdetector. Он позволяет в режиме реального времени отслеживать блокировки VPN-протоколов и фиксировать их продолжительность с указанием конкретных регионов и операторов. Инструмент анализирует доступность VPN-протоколов Cloak, OpenVPN, OpenVPN+TLScrypt, WireGuard, Amnezia WireGuard, Shadowsocks в разных регионах России, где на момент тестирования есть пользовательские ноды. В настоящее время проект насчитывает более 100 держателей узлов (нод) с разными операторами связи более, чем в 30 регионах России. В анализе учитываются разные операторы мобильного и домашнего интернета, а также анализируется трафик как внутри РФ, так и «за рубеж». Автоматическая проверка происходит каждые 10 минут.

> Чтобы устройство стало «нодой» и могло участвовать в мониторинге, на нем должно быть установлено специальное ПО, которое пользователи (волонтеры) скачивают с GitHub, настраивают и поддерживают постоянный доступ в интернет для

бесперебойной работы. Есть технические требования - устройство с ОС Linux, актуальная версия Docker и плагины «buildx» и «compose» (v2) к ней или устройство на Windows с установленным WSL.

Как показывают графики данных с DPIdetector, протокол Wireguard блокировался в России у мобильных операторов с середины августа по конец ноября 2024 года. В последних числах декабря 2024 Wireguard снова начал подвергаться блокировкам на мобильном интернете. На домашнем интернете Wireguard не блокировался повсеместно, но локальные проблемы с подключением могли оставаться в ряде регионов.

Shawodsocks был недоступен на мобильном интернете с 15 октября по конец декабря 2024 года. Протокол оставался заблокированным на мобильном интернете до конца 2024 года, а на домашнем интернете - работал без каких-либо проблем.

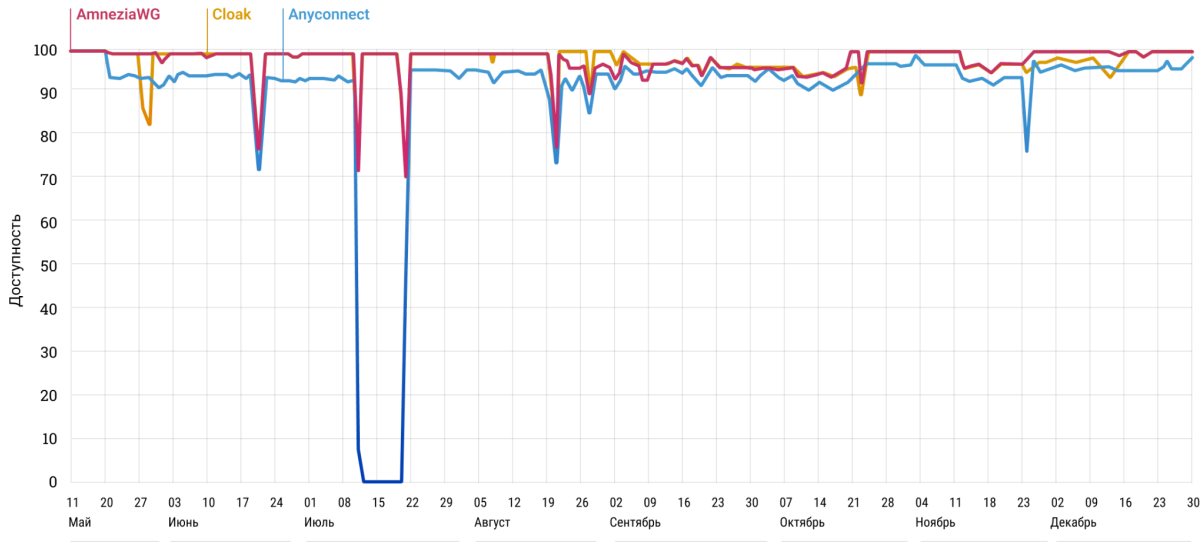
На провайдерах стационарного домашнего интернета с 21 августа по конец ноября 2024 года блокировке подвергался протокол Wireguard, а Shadowsocks - с 23 ноября по начало декабря 2024 года.

Кроме этого в течение года наблюдались блокировки других протоколов:

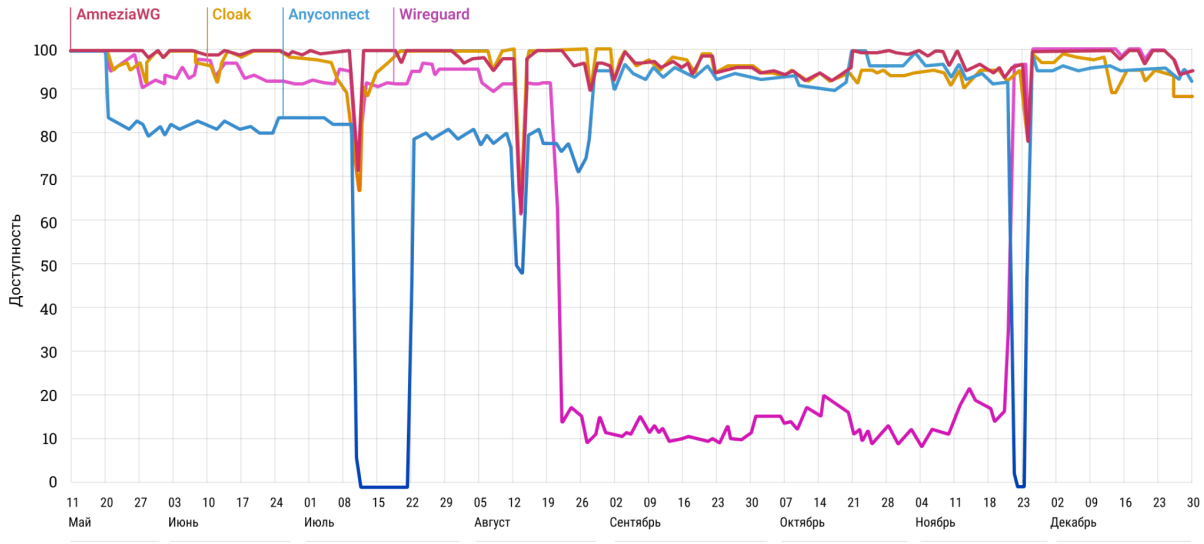
- в мае-июне блокировке на мобильных устройствах подвергался OpenVPN;
- с мая по август в ряде регионов фиксировались попытки блокировок Cisco Anyconnect как на домашнем, так и на мобильном интернете;
- также в некоторых регионах наблюдались непродолжительные блокировки протоколов Cloak и OpenVPN на домашнем интернете.

Эти блокировки носили непродолжительный характер и наблюдались точечно у разных операторов.

Во всех случаях ограничение возможности подключения касается только зарубежного трафика и только ситуаций, когда пользователь пытается подключиться к VPN с серверами за пределами России.



Домашний трафик. Источник DPIdetector



Мобильный трафик. Источник DPIdetector

Active Probing

В феврале 2024 года в российском сегменте интернета произошёл глобальный сбой - вероятно из-за тестирования Active Probing. По наблюдениям экспертов, на тот момент технология Active Probing уже около месяца точечно работала в России. Масштабное падение интернета могло произойти из-за попытки запустить технологию в автоматическом режиме на весь Рунет.

Active Probing — это метод, при котором система сама отправляет запросы на подозрительные IP-адреса или домены, чтобы проверить, не используется ли там запрещённый способ обхода блокировок, например VPN, Tor или прокси.

Эксперты зафиксировали активность с IP-адреса из группы AS61280, принадлежащего государственному учреждению “Главный радиочастотный центр” (ФГУП ГЧРЦ). Проводилось сканирование 443 порта у многих серверов (которые могли быть пустые или на них мог быть установлен VPN).

На примере VPN-сервиса Windscribe, эксперт ValdikSS описал как работает такое сканирование и последующие блокировки.

Это происходит следующим образом.

При обращении по HTTPS со SNI (api|checkip|assets).windscribe.com и других доменов сервиса Windscribe на порт 443 или по TCP SYN на один из известных IP-адресов VPN-серверов сервиса и порт 443, 587, 21, 22, 80, 123, 143, 3306, 8080, 54783, 1194 (например, 149.88.108.1)

или по UDP к VPN-протоколу OpenVPN или WireGuard на эти же порты происходит блокировка на 5 минут:

SNI по regexp (api|checkip|assets)\.[0-9a-f]{40}\.com, но при условии, что в имени зоны содержится хотя бы 5 цифр и 4 буквы. Т.е. https://api.abcdef0123456789abcdef012345678900000000.com заблокируется, но https://api.abc000012345678922222201234567890000000.com — нет”.

Возможно, метод с триггерами используется, в том числе для выявления новых VPN-серверов: если пользователь обратился на (api|checkip|assets).windscribe.com или на regexp-домен после его блокировки, а затем в течение 5 минут подключается по OpenVPN или WireGuard к какому-то неизвестному IP-адресу, то это, скорее всего, сервер Windscribe. Если это и происходит, то не в автоматическом режиме.

В 2024 году российские цензоры заметно нарастили использование Active Probing для поиска и блокировки VPN-сервисов. В течение года регистрировались проблемы с сервисом Outline, а именно с его админкой, которую можно найти и заблокировать.

STP, SoftEther и OpenConnect без обновлений/патчей сильно подвержены блокировке из-за их особенности ответа на запросы с payload:

- SoftEtherVPN в ответ на GET-запрос с путем /vpnsvc/connect.cgi, типом application/octet-stream и пэйлоадом 'VPNCONNECT' выдаст в ответ 200 код и предсказуемый бинарный блоб с рассказом о том, что он из себя представляет.
- В случае с MS SSTP цензоры, желая выяснить, чем занимается пользователь, просто сделают запрос на его сервер с URL /sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/ с HTTP-методом SSTP_DUPLEX_POST, как это описано в стандарте протокола, и

сервер сам подтвердит в ответ, что он - да, действительно, MS SSTP VPN.

- AnyConnect/OpenConnect при обращении по / или по /auth ответят очень характерной XML'кой. И это невозможно откорректировать - эти особенности определены в протоколах, и именно по этой логике работают VPN-клиенты.

Источник habr.com

Уже сейчас ясно, что в скором будущем почти не останется протоколов, которые невозможно вычислить Active Probing - все самые популярные протоколы уже обнаружены и блокируются. Антицензурные сервисы приходят к необходимости искать альтернативы, типа XRay и других инструментов, которые могут маскироваться под веб-трафик, а также имеют защиту от Active Probing.

Блокировка Encrypted Client Hello (ECH)

В сентябре 2023 года Cloudflare подключил протокол Encrypted Client Hello (ECH) для всех сайтов, использующих их сервера. Эта технология скрывает всю информацию, вплоть до метаданных, при защищенном (то есть https, а не http) TLS-подключении. ECH шифрует сообщение ClientHello в рамках TLS-рукопожатия. Задача этого протокола заключается в улучшении конфиденциальности пользователей, которые в противном случае передавали бы имя хоста посещаемого сайта сетевому провайдеру.

Побочным эффектом ECH является то, что он затрудняет работу DPI, которая обычно позволяет просматривать и фильтровать определенные поля в сообщении TLS-рукопожатия ClientHello. В результате этого сайты, размещенные на Cloudflare, которые ранее были недоступны из-за блокировок через DPI, оказались доступны внутри страны без использования каких-либо специальных технологий обхода цензуры.

В ноябре 2024 года появились сообщения, что Роскомнадзор начал блокировать в России доступ к ECH на Cloudflare. В результате этого недоступными оказались сотни тысяч сайтов по всей стране, в том числе сайт Якутской государственной сельскохозяйственной академии.

Использование ECH компанией Cloudflare было названо «нарушением российского законодательства», и цензоры рекомендовали владельцам российских сайтов отказаться от использования ECH и использовать отечественные CDN-сервисы, которые «обеспечивают надежное и безопасное функционирование ресурсов и защиту от компьютерных атак».

> Блокировка осуществлялась, если в пакете ClientHello установлен SNI = cloudflare-ech.com и есть ECH extension.
>
> Только лишь SNI = cloudflare-ech.com без ECH extension не блокировался, как и ECH grease без SNI = cloudflare-ech.com.
>
> Фильтр применяется к HTTP2 (TCP) и HTTP3 (QUIC)-соединениям.
>
> ТСПУ «замораживает» соединение сразу после получения ClientHello, а не разрывает его на уровне TCP или каким-то более подходящим образом. Из-за этого браузер понимает, что соединение сломано, только спустя примерно минуту.
>
> Источник ntc.party

Использование ECH, таким образом, не является полноценным способом обхода цензуры в России. Кроме того, регулярные сообщения РКН о необходимости перехода на отечественные хостинг-провайдеры и сбор IP-адресов, могут говорить о предпосылках к новым блокировкам.

Проблемы с DNS

В экспертных сообществах в течение всего 2024 года обсуждались проблемы с DNS от популярных сервисов, типа Cloudflare, Google, AdGuard, ControlD и др. Эти проблемы наблюдались в разные промежутки времени и с разной длительностью.

Чаще всего проблемы наблюдались именно с Cloudflare из-за того, что их DNS использовался в бесплатном VPN WARP. Из-за блокировок DNS использование WARP для обхода блокировок было затруднено, однако он получил второй

шанс после появления инструкций по его «оживлению» с помощью протокола AmneziaWG (обфускация с помощью AWG позволяла обойти блокировку чистого WARP, который работает на WG).

Ещё в 2020-м года стало известно, что Роскомнадзор заблокировал все три DNS-сервера облачного сервиса DigitalOcean: ns1, ns2 и ns3, однако блокировка не была стабильной и периодически сервисы оказывались доступными.

DNS (Domain Name System) — это иерархически организованная система доменных имён, обеспечивающая преобразование привычных адресов (например, google.com) в числовые IP-адреса, используемые для маршрутизации трафика в сетях. В России манипуляции с DNS, такие, как подмена ответов или блокировка запросов, применяются для интернет-цензуры и ограничения доступа к информации.

Еще в 2019 году со вступлением в силу закона о «суверенизации» Рунета было предусмотрено создание российской системы доменных имен (DNS) в качестве альтернативы глобальной DNS, поддерживаемой Корпорацией по управлению доменными именами и IP-адресами (ICANN). Национальная система доменных имен (НДСИ) начала функционировать в России с 2021 года, тогда же Роскомнадзор обязал провайдеров и владельцев автономных систем подключиться к ней, и в том же году начались первые штрафы за неподключение.

В 2024 НСДИ активно применялась для перенаправления DNS-запросов и реализации блокировок на сетевом уровне. В сентябре 2024 года Роскомнадзор заблокировал доступ к платформе OONI Explorer, которая предоставляет данные об интернет-цензуре.

> На некоторых сетях в России DNS-запросы к explorer.ooni.org возвращали IP-адреса, с заглушками от самого Роскомнадзора или страницами блокировки, например, 188.186.154.88 — “Доступ к информационному ресурсу ограничен на основании ФЗ от 27.07.2006 г. №149-ФЗ "Об информации, информационных

технологиях и о защите информации". В других случаях DNS-запросы возвращали ошибку, указывая на то, что домен не существует. Эти методы подтверждают использование подмены DNS-ответов для блокировки доступа к ресурсам.

Аналогичным образом, по данным исследования OONI, в России по состоянию на сентябрь 2024 году ограничивается доступ как минимум к 279 доменам новостных СМИ, как независимых, так и иностранных. В этих случаях блокировка на основе DNS осуществляется децентрализованным способом и возвращает пользователю адрес 188.186.146.208 как часть DNS-разрешения.

В декабре 2024 года Роскомнадзор провёл учения по изоляции российского сегмента интернета от глобальной сети. Тогда от мирового интернета были временно отключены три региона: Чечня, Дагестан и Ингушетия. Функционирование внутренних ресурсов в условиях изоляции как раз обеспечивал НСДИ.

Также 2024 году российские власти значительно усилили меры по блокировке защищённых DNS-протоколов, таких, как DNS-over-HTTPS (DoH) и DNS-over-TLS (DoT), рассматривая их, как угрозу государственной цензуре. Эти протоколы шифруют DNS-запросы, затрудняя их перехват и подмену. Для блокировки применялись системы DPI, способные анализировать сетевой трафик в реальном времени, выявляя характерные признаки DoH и DoT, такие, как специфические порты, заголовки и шаблоны трафика.

Цензура в отношении хостинг-провайдеров

Еще в мае 2022 года, пользователи в России сообщили о проблемах при попытке получить доступ к сетям Cloudflare и DigitalOcean через отдельные порты. Пользователям не удавалось установить TCP-соединение через порт 443, и все пакеты сбрасывались. Однако через другие порты (не 443) - всё работало. Такое явление наблюдалось во многих кабельных и мобильных сетях, включая принадлежащие «Билайну», «Ростелекому», «Дом.Ru» и другим. TCP-порт 443 используется протоколом HTTPS, видимо атака была на него.

В апреле 2024 года о проблеме блокировки хостинг-провайдеров заговорили снова - Роскомнадзор заблокировал сайты тех, кто не выполнил требования закона о «приземлении».

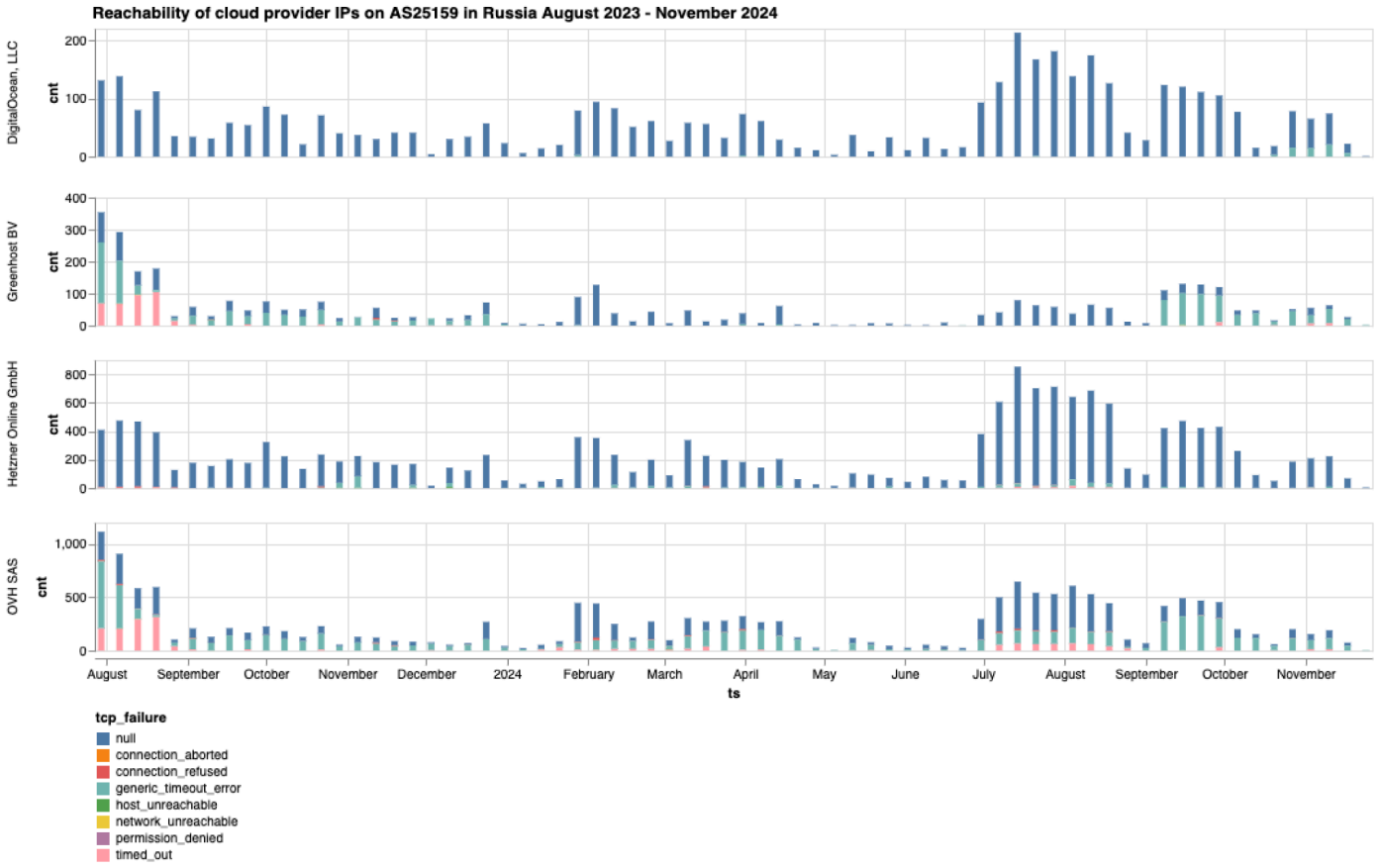
Через три месяца пользователи в России сообщили о блокировке HTTP/HTTPS-трафика на портах 80 и 443 при попытке подключения к IP-адресам Linode, OVH, Fastly, Digital Ocean и Scaleway. В результате некоторые сайты, такие как Nmap и Reddit, были временно недоступны.

Как минимум были заблокированы диапазоны:
51.68.188.0/22
51.38.124.0/22
50.116.0.0/18
151.101.0.0/16
206.189.65.0/24
51.15.0.0/17

В ноябре появились сообщения о проблемах с сайтами, которые расположены на площадках Greenhost, Cloudflare, Hetzner, OVH, Aeza. Из-за проблем с этими площадками пострадали такие ресурсы, как 2ip, сайт Notepad++, archlinux, filezilla и др. Скорее всего Роскомнадзор так пытался бороться с VPN-сервисами, которые имеют подсети IP-адресов у этих хостинг-провайдеров.

> При попытке открыть http-версию сайта в ответ приходили TCP Retransmission или повторная передача TCP-пакета, что также свидетельствует об искусственном вмешательстве в трафик. Это приводит к «вечной загрузке» страницы или ошибке «время ожидания истекло».

Эти сообщения пользователей подтверждаются данными OONI, которые показывают всплеск таймаут-ошибок при тестировании IP-адресов облачных провайдеров на сети AS25159 (ПАО «Мегафон») в России в период с сентября 2024 года по октябрь 2024 года.



Доступность IP-адресов облачных провайдеров на AS25159 в России с августа 2023 по ноябрь 2024. Источник ooni.org

Позже Роскомнадзор официально допустил, что может ограничить возможность пользоваться зарубежными сервисами, оказывающими услуги хостинга. По заявлению государственного ведомства, работа таких компаний, как GoDaddy, Kamatera, Network Solutions, Ionos, HostGator, DigitalOcean, Amazon Web Services и Hetzner Online GmbH, подвергает рискам ресурсы российских организаций. Ссылается ведомство, как и в других случаях, на нарушение законодательства, в частности, на не включение в реестр провайдеров хостинга.

В течение всего 2024 года активно блокируются подсети хостинг-провайдеров, так как они - по мнению цензоров - могут использоваться для разворачивания VPN. При этом сопутствующие потери в виде блокировок многих непричастных сайтов, которые хостятся рядом, не являются значимыми по мнению властей.

И это очень похоже на «иранизацию» российской цензуры (в Иране практически все диапазоны IP-адресов крупных хостинг-провайдеров заблокированы). Это дорога к «белым спискам» разрешённых сайтов, когда всё заблокировано, запрещено и не работает, кроме небольшого количества того, что разрешено цензорами.

Проблемы с зеркалами сайтов на CDN

В феврале 2024 года известный CDN-сервер Fastly отключил возможность использования Domain Fronting на своем сервисе, что поставило под угрозу работоспособность многих средств обхода блокировок, которые использовали данный метод (meek, VLESS и другие). Крупнейшие CDN-провайдеры Google и Amazon запретили Domain Fronting ещё в 2018 году для предотвращения хакерских атак.

Инструменты Domain Fronting используют не только хакеры, но и разработчики сервисов VPN и проектировщики зеркал для заблокированных сайтов. Это один из методов маскировки реального адреса ресурса за счет манипулирования запросами сети доставки контента (CDN, Content Delivery Network).

Заблокированные сайты запускают свои копии - зеркала - которые прячут, используя Domain Fronting, внутри большого серверного пространства провайдеров CDN. Это позволяет им избежать блокировки согласно стратегии Collateral freedom. Вмешательства в работу CDN приводит к тому, что рушатся важные средства обхода цензуры.

Независимые российские СМИ, которые находятся под цензурной блокировкой и вынуждены содержать сложную систему зеркал и антицензурных инструментов, позволяющих читателям заходить на них, рассказывали исследователям о том, что блокировки CDN и

хостинг-провайдеров повлияли на их работу. В частности, эти блокировки снижают скорость загрузки контента, увеличивая расходы на инфраструктуру и делая инфраструктуру медиа более уязвимой для кибер-атак, что особенно критично для независимых изданий, работающих под политическим давлением.

Помимо Domain Fronting российские СМИ используют также сокращатели ссылок, чтобы прятать зеркала. И хотя эти инструменты всё ещё работают (в т.ч. Bitly, vk.cc и др), блокировка их возможна.

Сбои у провайдеров при тестировании суверенного рунета

В середине октября 2024 пользователи провайдера Skynet сообщали о невозможности получить доступ к различным сайтам - от Википедии до банков. Сам провайдер объявил, что с их стороны не осуществляется никаких препятствий для работы интернет-ресурсов.

Пользователи обсуждали версию, что сбой связан с тем, что оборудование ТСПУ, получило какие-то новые настройки. Это могло произойти при тестировании «белых списков», такой модели работы внутреннего интернета, когда запрещены все сайты, кроме тех, что внесены в список разрешённых. Сбои связи в таких ситуациях происходят довольно часто, что бывает вызвано как человеческим фактором и неаккуратно проведённым обновлением, так и несовершенством аппаратуры.

1 ноября аналогичный массовый сбой наблюдался ещё как минимум у четырёх провайдеров - МГТС, МТС, Ростелеком, Дом.ру.

В декабре прошли учения по «суверенизации Рунета», особенно это ощутили на себе жители Дагестана, где 6-7 декабря 2024 не работало

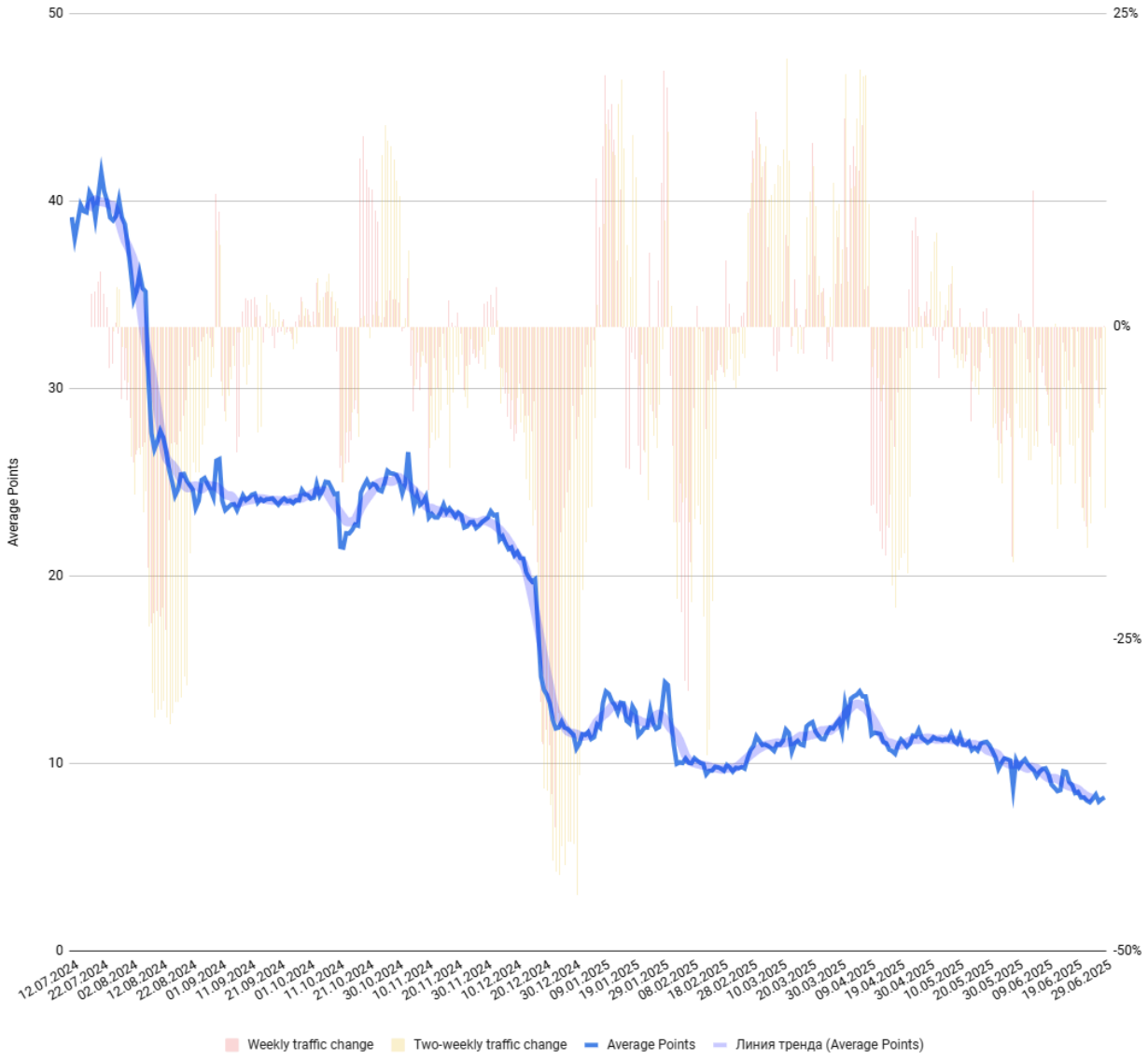
большинство зарубежных ресурсов (Github, GPT, WhatsApp, Telegram и пр.) - попытки подключиться к зарубежным VPN также выдавали ошибки.

Замедление Youtube и VPN-протоколов

В 2024 году в России также наблюдалось замедление сервисов и инструментов. Самый резонансный и показательный случай - это замедление YouTube, которое началось в июле 2024 года.

Сначала власти официально списывали неполадки в работе видео-сервиса на деградацию оборудования Google, которое американская корпорация якобы должным образом не обслуживает и не обновляет с 2022 года. Но 25 июля 2024 года появились заявления официальных лиц о том, что в России специально начали замедлять YouTube. Потом Роскомнадзор назвал причины, по которым им приняты меры в отношении видеосервиса: многочисленные нарушения законодательства России и «неуважение к нашей стране и гражданам».

Полностью YouTube замедлился с 1 августа, когда его скорость резко упала у всех провайдеров по всей стране. Загрузка самого сайта YouTube и приложений осуществлялась без проблем, но видеоролики не воспроизводились совсем или их загрузка была очень медленной.
За первые две недели блокировки трафик YouTube в России упал более чем на 20%.



Среднесуточный трафик на YouTube, Россия. Источник ЗаТелеком

В этот момент в России зафиксирован скачок интереса пользователей к средствам обхода цензуры и массовая установка VPN. Операторы связи отметили повышение общего объема трафика на 5-10%. В сетях региональных операторов - до 20%. Последних это привело к дополнительным тратам на приобретение трафика у магистральных операторов.

Помимо YouTube в 2024 году замедлялись также VPN-протоколы: OpenVPN, WireGuard, AmneziaWG, Cloak. Некоторые пользователи рапортовали также о трудностях с менее популярными протоколами SoftEther и OpenVPN XOR. При подключении на 443 порт скорость замедлялась, а на любом другом порту

приходила в норму. Проблема наблюдалась на домашнем интернете, при переходе на мобильный все работало корректно.

Замедление происходило на разных VPS-провайдерах, то есть не зависело от локации или принадлежности к хостеру. Чаще всего замедление было временным и заканчивалось спустя полчаса или пару часов. Смена настроек обфускации, например, у AmneziaWG или Cloak позволяло решить проблему.

Эпоха замедления (троттлинга) сервисов началась в России в 2021 году, когда российские власти стали применять эту технологию к Twitter. Замедлять социальную сеть стали из-за того, что, по словам властей, она не удаляла материалы с запрещённой информацией. Таким образом санкции в виде замедления должны были побудить Twitter к сотрудничеству.

> Тогда эксперты провели полноценные исследования новой цензурной технологии. Они выяснили, что тротлинг инициируется доменами Twitter в расширении TLS SNI, и он ограничивает как восходящий, так и нисходящий трафик до значения от 130 кбит/с до 150 кбит/с, отбрасывая пакеты, которые превышают эту скорость. Также было обнаружено, что устройства, которые используются для замедления, по-видимому, расположены близко к конечным пользователям, и что замедление является одинаковым у разных интернет-провайдеров, что предполагает их централизованную координацию.

Начало использования технологии замедления в России стало следствием отхода от ранее открытой модели цензуры в пользу более централизованной, дающей больше полномочий цензорам вводить ограничения в одностороннем порядке. Старая система была основана на блокировках IP-адресов, список которых публикуется Роскомнадзором. Полномасштабное внедрение ТСПУ сделало цензуру более хитрой и искусной. Именно ТСПУ

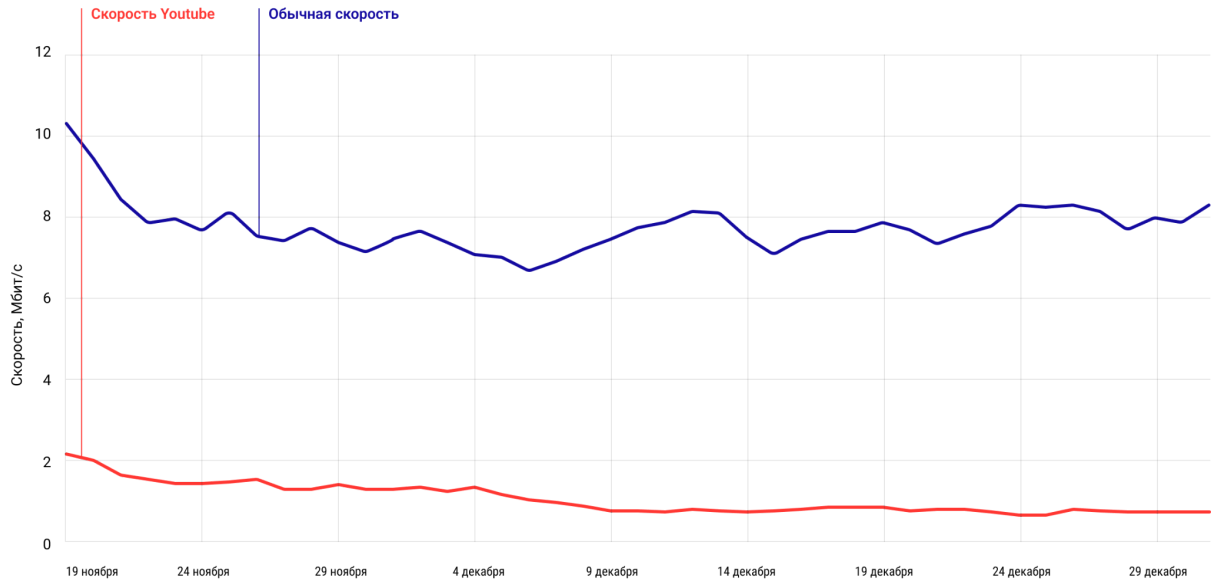
позволило властям использовать технологию троттлинга, фингерпринтов, блокировки по SNI, по протоколам и пр.

Измерение замедления YouTube

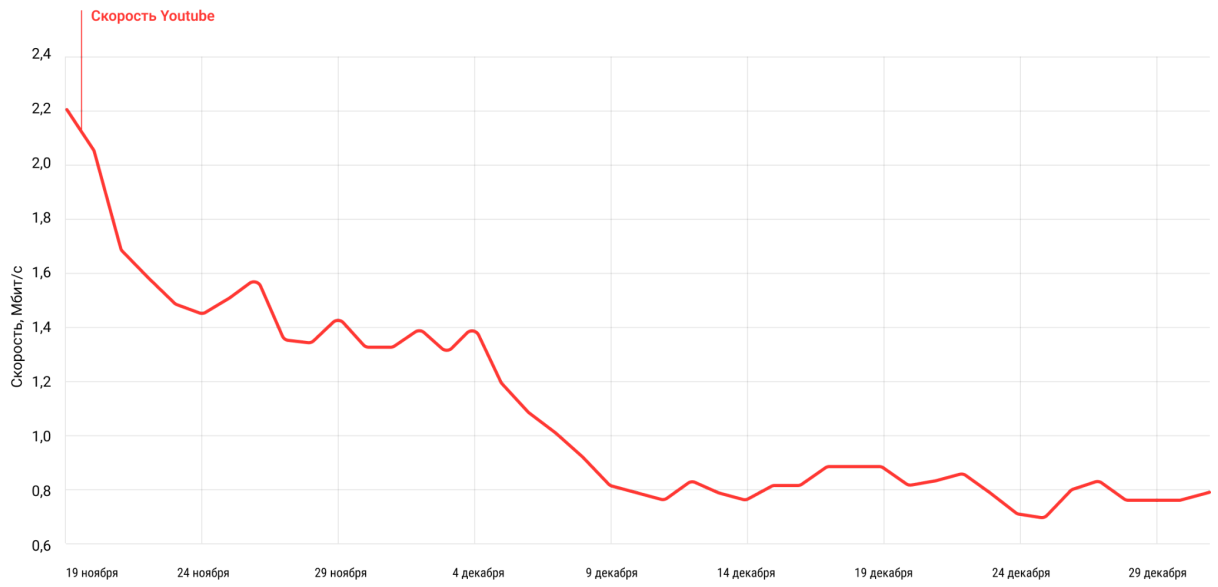
С ноября 2024 года DPIdetector начал замерять замедление YouTube. Данные основываются на разнице между обычной загрузкой интернета и скоростью загрузки YouTube.

С серверов для тестирования скорости скачиваются первые 400 килобайт тестировочного файла, замеряется время скачивания и экстраполируется до "мегабитов в секунду". Скачивание происходит два раза: в "обычном" режиме и в режиме подмены имени сервера на принадлежащие YouTube. Синий график показывает замеры в "обычном" режиме, красный — с подменой на YouTube.

На графике видно, что с 19 ноября 2024 года уже и так низкая скорость загрузки YouTube продолжилась снижаться, достигнув минимума в 0,8 мбит/сек к концу года.



Источник DPIdetector



Источник DPIdetector

Антицензурные средства в России

В России постепенно сокращается число работающих средств обхода цензуры. То, что было доступно для пользователей в начале года - к концу года может уже не работать, а эффективные инструменты требуют, зачастую, более тонкой настройки и не всегда подходят для «непродвинутых» пользователей.

После массированной блокировки VPN-протоколов стало намного сложнее подобрать стабильно работающий VPN-сервис. Удаление приложений из AppStore добавило трудностей для пользователей, которым теперь, чтобы установить приложение, нужно проводить специальные манипуляции по смене региона. Отдельный квест - оплата VPN, так как только небольшое количество провайдеров успешно работают с российскими картами.

В то же время - особенно после блокировки YouTube - расцвела продажа VPN-однодневок. Чаще всего это могут быть малоизвестные Telegram-боты, продающие ключи для Outline. Неизвестные люди также собирают VPN-сервисы на базе бесплатного self-hosted решения Amnezia VPN или

Outline и продают к нему ключи доступа, которые через непродолжительное время перестают работать. Ситуации, когда пользователи остаются с неработающим сервисом за которые они отдали деньги (часто и не один раз), подрывают их доверие к VPN-технологиям, они часто перестают искать работающие варианты и выходы в свободный интернет. Что только способствует цели российских властей - оставить всех внутри суверенного рунета.

Тем не менее мы можем выделить несколько сервисов, хорошо зарекомендовавших себя в 2024 году в России, вопреки всем попыткам блокировок и замедлений.

GoodbyeDPI, Zapret, ByeDPI

Бесплатный опенсорсный инструмент, созданный исследователем цензуры ValdikSS долгое и качественно работает в России, помогая обходить блокировки без использования сервера. После начала блокировки YouTube, его разработчики выпустили отдельную инструкцию по настройке приложения и компьютера, которая позволяет разблокировать видео-сервис. Иногда всё же у GoodbyeDPI наблюдались проблемы с подключением, что может быть связано с тем, что системы ТСПУ научилось его искать и блокировать.

Инструмент Zapret имеет похожие функции, хотя сложнее в настройке. На основе него было создано популярное решение для Windows, позволяющее в пару кликов разблокировать YouTube и Discord, а также ByeDPI, который получил реализацию в виде плагина для NekoBox, а также версию для Android от другого автора.

XRay, Cloak, OpenVPN XOR и другие рабочие решения

Для того, чтобы обойти цензуру, продвинутые пользователи используют XRay-core, в котором есть VLESS, позволяющий маскировать соединение под HTTPS-трафик. VLESS имеет достаточно «обвесов», которые делают его более устойчивым к блокировке. Например, его можно спрятать за CDN, можно пустить через gRPC или WebSocket. Помимо этого разработчики

недавно выпустили XHTTP, который создан на основе SplitHTTP. Он разбивает соединение на части таким образом, что при просмотре потокового видео туннель не остаётся статичным. Вместо этого соединение фрагментируется и пересобирается в виде множества случайных запросов, создавая со стороны видимость активного веб-серфинга.

Помимо XRay все ещё работает Cloak, OpenVPN XOR, а при достаточном количестве технических знаний можно настроить NaiveProxy или PingTunnel.

Tor

Помимо VPN/Proxy-протоколов для обхода цензуры используется Tor, в котором хорошо себя показывает новый транспорт WebTunnel. Он похож на HTTPS из-за чего его сложнее определить и заблокировать, в отличии, от obfs4, считающегося устаревшим и менее устойчивым к современным блокировкам.

Остальные методы обфускации в Tor так или иначе могут блокироваться в РФ. Например, в Tor блокировались мосты obfs4 на мобильных сетях 4G и не только. Проблемы наблюдались с мостами как минимум у Tele2, Beeline и Yota.

Meek-транспорт в Tor работает нестабильно, и его скорость оставляет желать лучшего. Еще одна проблема meek, которую стоило бы упомянуть, - отказ сервисов от предоставления своей инфраструктуры для Domain Fronting, что сильно сокращает возможности настройки и использования meek, использующего этот метод маскировки.

Amnezia

Amnezia VPN работает на собственном протоколе - AmneziaWG. Это форк WireGuard-Go, в который добавили функции для обхода блокировок и снижения вероятности обнаружения. Также Amnezia VPN работает с другими протоколами, позволяющими маскировать трафик - OpenVPN over Cloak, XRay VLESS Reality. Это делает сервис очень устойчивым к

блокировкам, так как его трафик не похож на VPN-трафик, а значит его не смогут найти и заблокировать российские цензоры, которые поставили блокировки протоколов VPN на поток.

Первой разработкой команды стал self-hosted продукт, который пользователи высоко оценили за высокую степень надежности и приватности. В 2022 года Amnezia VPN запустила для России специальную версию Amnezia Free, с помощью которой можно получить доступ к сайтам независимых СМИ, правозащитных организаций, социальных сетей и мессенджеров, заблокированных государственной цензурой. После блокировки в стране YouTube было развёрнуто классическое коммерческое решение на устойчивом к блокировкам протоколе, позволяющее смотреть потоковое видео, без самостоятельной настройки сервиса.

VPNGenerator

VPN Generator - сервис, построенный на коллективном использовании VPN. Это бесплатное и надёжное решение подразумевает, что пользователи объединяются в «бригаду», для которой создается свой собственный мини-VPN. Он обладает уникальным сетевым адресом, который трудно найти и заблокировать. Решение работает на базе Outline, позволяет разблокировать YouTube, Discord и другие потоковые высоконагруженные сервисы.

Сейчас работает также коммерческое решение GenVPN, которое распространяет ключи доступа через телеграм-бота. На его основе создаются решения для крупных русскоязычных СМИ и блогеров.

Paper VPN и другие антицензурные решения от СМИ

Активное развитие в 2024 году получили антицензурные решения от независимых российских медиа, которые развивали собственные инструменты для того, чтобы сохранить аудиторию. Самый крупный пример - Paper VPN от издания «Бумага». Сам VPN был запущен еще в 2022 году, когда сайт «Бумаги» был заблокирован в России, но активно продвигался и наращивал базу пользователей именно в 2024 г.

Независимый телеканал и интернет-издание «Дождь», признанный в России нежелательной организацией, после начала замедления трафика YouTube разработал расширение для браузера «Поток». Оно позволяет «ускорить» загрузку видео и смотреть ролики в высоком качестве. Это бесплатное решение продвигается среди читателей и зрителей «Дождя».

Уже в 2025 году собственные VPN-решения появились у медиа, правозащитных команд и популярных YouTube-блогеров, например, у признанного нежелательным издания The Insider, у правозащитного проекта «Ковчег», у блогера Димы Зицера и др.

Прогнозы

Все описанные выше наблюдения имеют своей целью фиксацию этапов развития цензуры. Проанализировав их эксперты, исследователи, разработчики антицензурных инструментов, а также простые пользователи интернет в России могут спрогнозировать дальнейший ход событий и запланировать свои действия.

Наши прогнозы на ближайшее будущее таковы.

1. Вероятно, в 2025 года мы увидим статистические методы для блокировок. При использовании метода статистических блокировок, будет организована «слежка» за определённым пользователем, группой пользователей или сервером. Трафик будет анализироваться на предмет обращения к различным сервисам, и, если будет обнаружено много трафика на определенный адрес, его проверят на наличие VPN/Proxy. Далее возможна блокировка или продолжение наблюдения.
2. Рунет движется в сторону введения «белых списков» разрешённых сайтов и адресов и «профессионального интернета», когда все внешние ресурсы заблокированы по умолчанию, но по необходимости можно получить

доступ. Например, если квалифицированным разработчикам необходимо использовать иностранный сервис (github), то необходимо будет оформить запрос на разблокировку в ответственном за это ведомстве.

3. Вероятно, мы увидим попытки разработать и внедрить в российское законодательство меры административного или уголовного преследования граждан не только за распространение, но и за использование VPN и других средств обхода блокировок - так называемую «ответственность потребителей». Правоприменение может подразумевать штафы и даже тюремные сроки для нарушителей запретов (как например, это уже сделано в Китае).

4. От Китая Россия также продолжит перенимать модель цензуры в связке с импортозамещением: блокировки больших международных сервисов сопровождаются продвижением отечественных аналогов. Власти не только запрещают что-то, но и предлагают что-то взамен. Мы уже видели беспрецедентные государственные инвестиции в VK и Rutube, целью которых было улучшение сервисов перед блокировкой YouTube в 2024 году. После блокировки часть пользователей YouTube просто перешла на российские сервисы, не имея мотивации разбираться с тем, как обойти блокировки и найти работающий VPN. Со временем отечественные сервисы будут ещё удобнее и привлекательнее для пользователей, несмотря на работающие там цензурные ограничения и слежку, которая включена в сервис по умолчанию.

5. Одним из лучших решений в борьбе с блокировками станет split tunneling (раздельное туннелирование), которое позволит усложнить оборудованию DPI анализ исходящего от пользователей VPN-трафика, так как он станет пропускать через себя только трафик до заблокированных ресурсов или ресурсов с геоблоком, а не весь трафик с устройства.

6. Главным критерием при выборе рабочего инструмента обхода цензуры в России будет его умение притворяться чем-то другим, например, маскироваться под что-то, либо стать ни на что не похожим. Это затруднит для DPI-оборудования обнаружение и блокировку его паттерна, что произошло, например, с Shadowsocks, который при стандартных настройках без маскировки легко обнаруживается и блокируется системами DPI или обычными VPN-протоколами: OpenVPN и WireGuard.