УДК 004.7.056

ТЕХНИЧЕСКИЕ МЕХАНИЗМЫ ОГРАНИЧЕНИЯ ДОСТУПА В РОССИИ: МОДЕЛЬ БЕЛЫХ СПИСКОВ И КЛАССЫ ТЕХНОЛОГИЙ СОХРАНЕНИЯ ДОСТУПА К ОТКРЫТОМУ ИНТЕРНЕТУ

Попов З.А. [1)]

1) АНПОО КИПО, город Краснодар, Россия; zaharpopov516@gmail.com

Аннотация. В работе выполнен системный анализ механизмов интернет-блокировок в РФ по состоянию на 2026 год. Рассматриваются многоуровневые ограничения: DNS, IP/маршрутизация, TLS/SNI, HTTP/HTTPS, QUIC/HTTP/3, платформенный уровень и логика самих приложений. Отдельное внимание уделено модели «белых списков» (allowlist), при которой доступ сохраняется только к заранее разрешённым ресурсам. Показаны практические последствия такой модели для пользователей, разработчиков, бизнеса и хостинга. Предложена типология классов технологий сохранения доступа-от классических VPN и прокси до обфускации, CDN/fronting, ECH/MASQUE, браузерных relay-сетей и P2P/оверлейных сетей. На основе данных OONI, Censored Planet, Cloudflare, операторских документов и сигналов из публичных сообществ (Net4People и др.) сформулированы выводы об устойчивости различных подходов в условиях allowlist-режима. Отмечается, что шифрование не делает трафик невидимым, а решения, работающие сегодня, могут быстро потерять эффективность при изменении сигнатур DPI, магазинных ограничений или политики облачных провайдеров.

Ключевые слова: интернет-блокировки, белые списки, allowlist, DPI, ТСПУ, SNI-фильтрация, обфускация, технологии сохранения доступа, OONI, censorship.

TECHNICAL INTERNET RESTRICTION MECHANISMS IN RUSSIA: ALLOWLIST MODEL AND ACCESS PRESERVATION TECHNOLOGY CLASSES

Popov Z.A. [1)]

1) ANPOO KIPO; Krasnodar; Russia; zaharpopov516@gmail.com

Annotation. This paper provides a systematic analysis of Internet blocking mechanisms in the Russian Federation as of 2026. It examines multi-layer restrictions: DNS, IP/routing, TLS/SNI, HTTP/HTTPS, QUIC/HTTP/3, platform/store-level blocks, and application-level logic. Special attention is given to the allowlist model, where access is preserved only to explicitly permitted resources. Practical consequences of this model for users, developers, businesses, and hosting providers are shown. A typology of access preservation technology classes is proposed-from classic VPNs and proxies to obfuscation, CDN/fronting,

ECH/MASQUE, browser-based relays, and P2P/overlay networks. Based on data from OONI, Censored Planet, Cloudflare, operator documents, and signals from public communities (Net4People, etc.), the study formulates conclusions about the resilience of different approaches under allowlist regimes. It is noted that encryption does not make traffic invisible, and solutions that work today may quickly lose effectiveness as DPI signatures, store-level restrictions, or cloud provider policies change.

Keywords: Internet blocking, allowlists, whitelists, DPI, TSPU, SNI filtering, obfuscation, access preservation technologies, OONI, censorship.

1. Актуальность

К 2026 году система ограничения доступа к сети Интернет в Российской Федерации перестала сводиться к какому-либо одному техническому механизму. Как показывают данные международных наблюдателей [1–4] и операторские документы [6, 9], блокировки реализуются на нескольких взаимодополняющих уровнях: реестровом, DNS, IP/маршрутизации, TLS/SNI, HTTP/HTTPS, QUIC/HTTP/3, а также на уровне магазинов приложений и логики самих приложений. Ключевым трендом последних лет является переход от точечной блокировки отдельных ресурсов (blacklist-модель) к построению инфраструктуры, в которой доступ по умолчанию ограничен, а разрешённые сервисы составляют «белый список» (allowlist) [9, 10]. Это принципиально меняет задачи для технологий сохранения доступа и требует системного анализа как самих механизмов фильтрации, так и устойчивости различных методов обхода.

2. Цель и задачи исследования

Цель работы-систематизировать технические механизмы ограничения доступа к интернету в РФ на 2026 год, проанализировать последствия модели белых списков и предложить классификацию технологий сохранения доступа с оценкой их устойчивости.

Задачи.

1. Выделить основные уровни фильтрации трафика (DNS, IP/маршрутизация, TLS/SNI, HTTP/HTTPS, QUIC, платформенный и прикладной).
2. Описать проявления allowlist-модели в операторской практике и её последствия для разных групп пользователей.
3. Классифицировать классы технологий сохранения доступа (VPN, прокси, обфускация, CDN-fronting, браузерные relay-сети, P2P-оверлейные сети).
4. Сформулировать выводы об устойчивости каждого подхода в условиях allowlist и динамического DPI.

3. Многоуровневые механизмы ограничения доступа.

3.1. Реестровый и адресный уровень.

Публичные реестры запрещённых доменов, URL и IP-адресов остаются стартовой точкой для блокировок. Однако, как отмечается в [3],

значительная часть ограничений не отображается в официальных реестрах, а применяется операторами самостоятельно на основе технических сигнатур.

3.2. DNS-уровень.

DNS по-прежнему используется как точка вмешательства. Инструмент OONI Probe [2] фиксирует в РФ DNS-манипуляции и перенаправления на страницы блокировки. В то же время измерения показывают, что многие блокировки срабатывают уже после успешного резолвинга имени [1], то есть на более высоких уровнях.

3.3. Уровень HTTP/HTTPS и TLS/SNI.

Одна из главных линий фильтрации проходит на уровне TLS и HTTP. Согласно измерениям OONI [1, 4], применяются следующие методы: HTTP MITM, TLS MITM, инъекции TCP RST после ClientHello, принудительные таймауты и немедленное закрытие соединения. Исследование Censored Planet [5] связывает эти паттерны с работой «Технических средств противодействия угрозам» (ТСПУ) и указывает на анализ SNI и QUIC-триггеров, а также на stateful-поведение устройств фильтрации.

3.4. IP-, CDN- и маршрутизационный уровень.

Существует также класс ограничений, при которых соединение формально не запрещено, но использовать его практически невозможно. В июне 2025 года Cloudflare сообщила, что при доступе к сайтам под её защитой из РФ часто загружались только первые 16 КБ ресурса [7]. Пользовательский опыт при этом оказывается сходным с полной блокировкой, хотя формально соединение не разрывается.

3.5. Протокольный уровень: QUIC и HTTP/3.

Современная фильтрация анализирует не только адреса и домены, но и класс протокола. Censored Planet [5] прямо относит QUIC к числу триггеров для ТСПУ, а Cloudflare [7, 8] фиксировала деградацию как для HTTP/3/QUIC, так и для обычного HTTPS поверх TCP. Таким образом, использование новых транспортных протоколов не гарантирует обхода: на одних участках сети они могут помочь, а на других-сами стать заметным признаком для блокировки.

3.6. Платформенный и store-level уровень.

К 2026 году ограничения вышли за пределы самой сети. OONI фиксирует удаление приложений и расширений из App Store и ограничения в каталогах расширений браузеров [3]. Это означает, что даже если некоторая сетевая технология теоретически жизнеспособна, пользователь может просто не получить или не обновить соответствующий клиент.

3.7. Уровень самого приложения.

Согласно исследованию RKS Global [3], значительная часть популярных Android-приложений определяет наличие активного VPN и передаёт этот факт на сервер. Поведение сервиса может меняться в зависимости от того, как приложение видит режим подключения у клиента. Это уже не чисто сетевая блокировка, а логика на стороне приложения.

4. Модель белых списков (allowlist).

4.1. Принципиальное отличие от blacklist-модели.

В blacklist-модели сеть по умолчанию открыта, а ограничения накладываются на заранее перечисленные ресурсы или сигнатуры. В allowlist-модели логика обратная: доступ сохраняется только к явно разрешённым назначениям, приложениям или протоколам. Для инженеров это означает необходимость не расширять список запрещённого, а поддерживать в актуальном состоянии карту всего допустимого трафика.

4.2. Проявления allowlist в РФ в 2025–2026 годах.

В операторских документах 2025–2026 годов белые списки описываются как перечни сервисов, доступных при ограничениях мобильного интернета [9]. Эти перечни формируются совместно с профильным ведомством, а сеть настраивается так, чтобы указанные сервисы продолжали работать. Показательно, что один из операторов прямо указывает: для доступа к ресурсам из белого списка VPN должен быть отключён [9]. Это хорошо демонстрирует внутренний конфликт между туннелированием и логикой «разрешены только известные назначения».

4.3. Практические последствия для разных групп.

Для обычных пользователей allowlist-режим означает частично работающий интернет, в котором даже формально доступные сервисы могут ломаться из-за неучтённых внешних зависимостей (сторонние API, внешние логины, статические ресурсы, обновления приложений, медиаконтент, аналитика, push-механизмы) [7, 9].

Для разработчиков возникает необходимость жёстко контролировать внешние зависимости, сторонние SDK, CDN и вход через внешние платформы.

Для бизнеса и хостинга проблема в том, что allowlist плохо сочетается с мультиарендными облаками, shared IP и anycast/CDN-моделями, поэтому коллатеральный ущерб становится почти неизбежным.

Мобильные приложения зависят сразу от двух слоёв: наличия в магазине приложений и сетевой достижимости их реальных backend-зависимостей.

5. Классы технологий сохранения доступа и их устойчивость

На основе проведённого анализа можно выделить следующие классы технологий сохранения доступа (от менее устойчивых к более устойчивым в условиях allowlist):

1. Классические VPN и прокси (OpenVPN, WireGuard, Shadowsocks без обфускации). Уязвимы к DPI по характерным сигнатурам (например, WireGuard легко идентифицируется по длинам пакетов и handshake). В allowlist-режиме операторы могут просто блокировать все неизвестные IP или протоколы, не входящие в белый список.

2. Обфусцированные туннели (Shadowsocks с плагинами, V2Ray, XRay, Hysteria).

Более устойчивы, но DPI-системы постоянно обновляют сигнатуры. Как показывают данные [5, 6], изменение одного параметра (например, имитация HTTP/3) может сделать протокол заметным за считанные часы.

3. CDN-фронтинг (domain fronting) и ECH/MASQUE. Используют разрешённые CDN (Cloudflare, Akamai и др.) для маскировки реального назначения. Однако политика облачных провайдеров может меняться [7, 8], а ECH (Encrypted Client Hello) ещё недостаточно распространён и может блокироваться по признаку неизвестного расширения TLS.

4. Браузерные relay-сети (Snowflake, Tor с meek/webtunnel). Работают через временные relay, предоставляемые добровольцами. Устойчивы к IP-блокировкам, но уязвимы к ограничениям на уровне магазинов расширений и к анализу трафика на предмет WebRTC или WebSocket.

5. P2P-оверлейные сети (I2P, ZeroNet, некоторые реализации Tor). Не имеют единых точек входа, что затрудняет их тотальную блокировку. Однако высокая задержка и сложность настройки ограничивают их применение для обычных пользователей, а DPI может распознавать специфические handshake-паттерны.

Общий вывод по классам: шифрование само по себе перестало быть достаточным средством обхода. DPI-системы успешно анализируют метаданные TLS (SNI, длины сообщений, тайминги), а также работают с QUIC и HTTP/3 [5, 6]. Наиболее устойчивыми в allowlist-режиме остаются те подходы, которые либо полностью выводят соединение за пределы национальной сети (браузерные relay, P2P), либо имитируют разрешённый трафик до уровня полной неотличимости (что технически очень сложно).

6. Выводы

1. Система ограничения доступа в России к 2026 году представляет собой многоуровневый, динамически настраиваемый комплекс технических мер, включающий фильтрацию на уровнях DNS, IP/маршрутизации, TLS/SNI, HTTP/HTTPS, QUIC, а также на платформенном и прикладном уровнях [1–8].

2. Ключевой тренд-эволюция от blacklist-модели к allowlist-модели («белые списки»), при которой доступ по умолчанию ограничен, а разрешены только заранее определённые сервисы [9, 10]. Это подтверждается операторскими документами и сообщениями СМИ.

3. Allowlist-режим меняет задачу для технологий сохранения доступа: недостаточно скрыть факт обращения к запрещённому ресурсу-необходимо либо имитировать разрешённый трафик, либо полностью выводить соединение за пределы контролируемой сети.

4. Шифрование без обфускации не является эффективным средством обхода, так как DPI-системы анализируют метаданные протоколов (SNI, длины пакетов, тайминги, handshake-паттерны) [5, 6].

5. Наиболее устойчивыми классами технологий в условиях allowlist являются: обфусцированные туннели с динамической сигнатурой, CDN-фронтинг (где позволяет политика облачного провайдера), браузерные relay-сети (Snowflake) и P2P-оверлейные сети (I2P). Однако каждый из этих подходов имеет уязвимости: магазинные ограничения блокируют

распространение клиентов [3], коллизии с белыми списками операторов делают многие VPN-протоколы заметными [9], а изменение сигнатур DPI может деактивировать обфускацию за часы.

6. Решения, работающие сегодня, могут быстро потерять эффективность при изменении сигнатур DPI, политики магазинов приложений или облачных провайдеров. Поэтому необходимы постоянный мониторинг (например, с помощью OONI [1, 2]) и развитие адаптивных, многоуровневых методов сохранения доступа.

Список использованной литературы

1. OONI Explorer : платформа для мониторинга интернет-цензуры [Электронный ресурс] // OONI. – Режим доступа: https://explorer.ooni.org
2. OONI Probe : инструмент с открытым исходным кодом для измерения интернет-цензуры [Электронный ресурс] // OONI. – Режим доступа: https://ooni.org/install
3. OONI (2024). Хроники цензуры: систематическое давление на независимые медиа в России [Электронный ресурс] / OONI, RKS Global. – 2024. – Режим доступа: https://ooni.org/documents/censorship-chronicles-russia-2024
4. OONI (2024, December 13). Russia blocked Viber [Электронный ресурс] // OONI Explorer Measurements. – 2024. – Режим доступа: https://explorer.ooni.org/measurement/?input=viber.com
5. Xue D., Mixon-Baca B., ValdikSS et al. TSPU: Russia's Decentralized Censorship System [Текст] / D. Xue, B. Mixon-Baca, ValdikSS, ... // Proceedings of the 2022 ACM Internet Measurement Conference (IMC '22). – New York : ACM, 2022. – P. 1–15.
6. Servercore Documentation. TSPU Impact Diagnosis [Электронный ресурс] // Servercore. – Режим доступа: https://servercore.com/docs/tspu-diagnosis
7. Cloudflare (2025, June 26). Russian Internet users are unable to access the open Internet [Электронный ресурс] // Cloudflare Blog. – 2025. – Режим доступа: https://blog.cloudflare.com/russian-internet-users-unable-to-access-open-internet-2025
8. Cloudflare Support (2025, June 30). Potential disruption of services for Russian users [Электронный ресурс] // Cloudflare Status. – 2025. – Режим доступа: https://www.cloudflarestatus.com/incidents/russia-20250630
9. CNews (2025, November 27). «Белым спискам» нужен отбеливатель [Электронный ресурс] // CNews. – 2025. – Режим доступа: https://www.cnews.ru/articles/2025-11-27_belym_spiskam_nuzhen_otelivatel