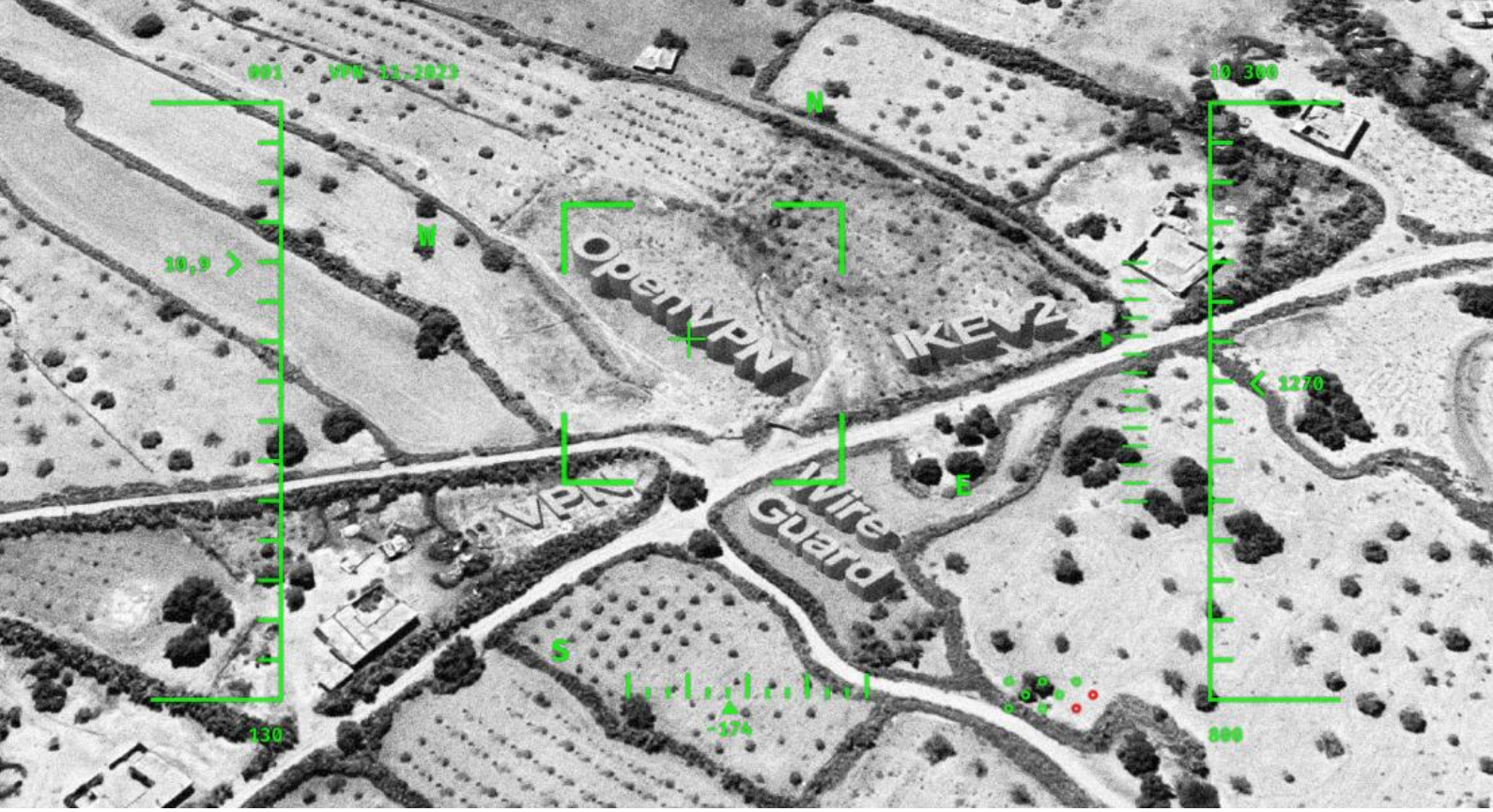

Обзорное исследование

VPN в России: от блокировки сервисов к блокировке протоколов

НАСТОЯЩИЙ МАТЕРИАЛ (ИНФОРМАЦИЯ) ПРОИЗВЕДЕН И (ИЛИ) РАСПРОСТРАНЕН ИНОСТРАННЫМ АГЕНТОМ «РОСКОМСВОБОДА» ЛИБО КАСАЕТСЯ ДЕЯТЕЛЬНОСТИ ИНОСТРАННОГО АГЕНТА «РОСКОМСВОБОДА». 18+

Роскомсвобода

Октябрь 2023

Введение

Интернет-цензура в России активно развивается с каждым годом. С 2011 года по 2023 год Россия стабильно поднималась на несколько позиций в год в индексе свободы интернета, где максимальное значение (100) — несвободный интернет. Такая динамика была обеспечена с одной стороны регулярными изменениями в законодательстве, создающими нормативную базу для усиления цензуры, с другой стороны увеличением количества и разнообразия блокируемых ресурсов.

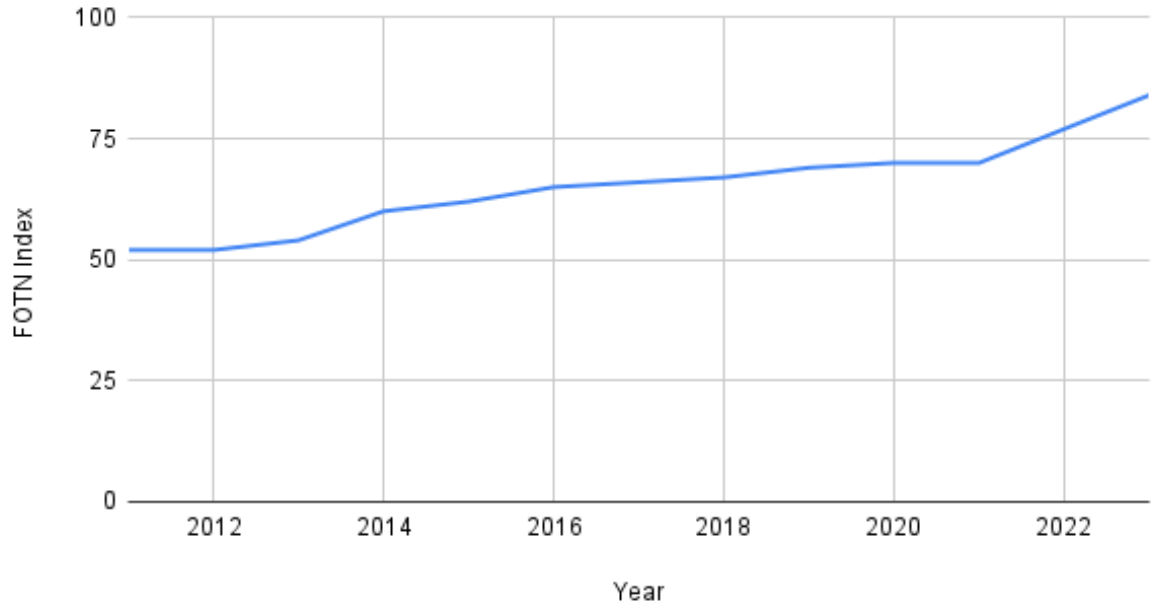

График: Индекс свободы интернета России с 2011 по 2023 год.

Сервисы обхода блокировок подвергаются активной цензуре в России с 2017 года, когда появилось законодательство запрещающее VPN-сервисам предоставлять доступ к сайтам, которые заблокированы в России. По данным базы Lumen, с 2017 года Google получили более 2000 запросов от Роскомнадзора, связанных с удалением ссылок ведущих на скачивание VPN-сервисов или информацию, описывающую их использование. Некоторые из таких запросов включают тысячи отдельных ссылок, поэтому суммарный объем контента, к которому российские пользователи не могут получить доступ, может превышать сотни тысяч ресурсов.

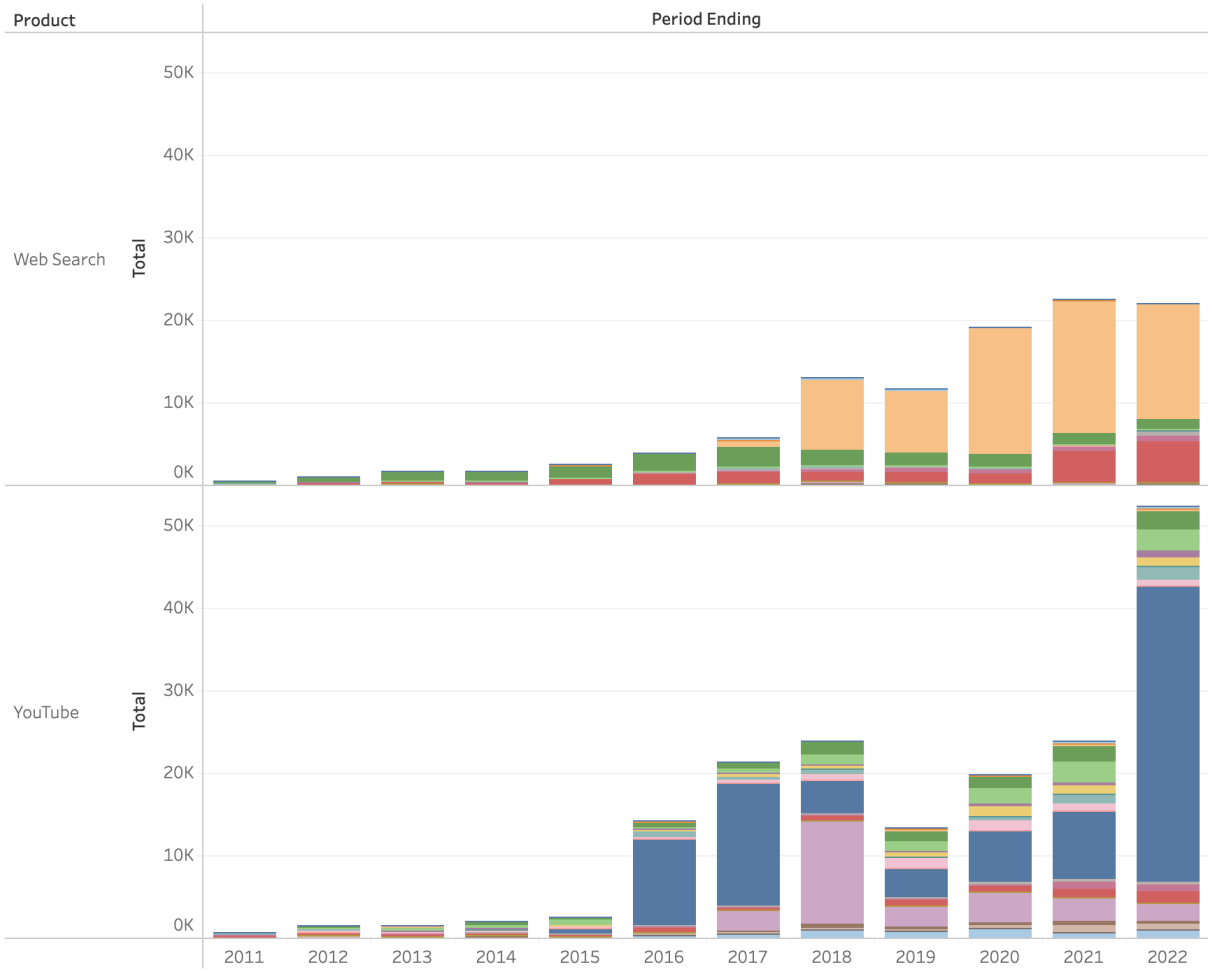

График: количество обращений на удаление контента полученных компанией Google от Роскомнадзора с 2011 по 2022 год. Синий — причина запроса «национальная безопасность», красный — «приватность и безопасность», оранжевый — «копирайт». Полный список тегов.

В 2023 году Министерство цифрового развития предложило новый законопроект, который должен позволить Роскомнадзору целенаправленно блокировать «информацию о способах, методах обеспечения доступа к информационным ресурсам и (или) информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации».

В этом исследовании мы попытались понять как россияне пользуются инструментами обхода блокировок, какие сервисы наиболее популярны, как пользователи реагируют на блокировки сервисов и как интернет-цензура в целом влияет на потребление контента и доступ к источникам информации для россиян.

Методология

Исследование проводилось на основании источников с открытыми данными, опроса, проведенного Роскомсвободой, и коротких интервью с независимыми российскими медиа. У каждого из источников есть свои ограничения, однако в данном исследовании при ответах на все вопросы мы постарались использовать более одного источника, чтобы иметь возможность сравнить результаты и подтвердить гипотезы, или акцентировать внимание на несоответствиях.

Для определения списка наиболее популярных в регионе сервисов были использованы данные Google Play, Apple Store, Google Trends, Яндекс Поиска. В то время как данные каждого отдельного сервиса могут быть нерепрезентативны в силу ограниченной аудитории и их динамичности (в разное время на маркетплейсах разные приложения могут занимать топ выдачи), совокупность данных из всех четырех источников и проведенного опроса, может дать нам общий контекст того, какие сервисы наиболее популярны среди россиян.

Для определения доступности и динамики использования vpn мы использовали три источника, данные поисковых сервисов (Google Trends, Яндекс Поиск), данные Tor Metrics, данные Proton и Psiphon VPN, данные собранные технологическим сообществом в России через отзывы о доступности сервисов по обходу блокировок.

В контексте блокировок мы в том числ использовали данные Open Observatory of Network Interference (OONI), чтобы определить доступность сайтов и сервисов. Данные OONI имеют ограничения по количеству тестируемых сайтов, поэтому для данного исследования мы обновляли списки тестируемых сайтов, чтобы посмотреть на доступность сайтов различных инструментов по обходу блокировок. Это исследование основано на большом количестве источников, которые дают достаточно возможностей, чтобы проанализировать контекст использования сервисов по обходу блокировок в России, однако его нельзя считать исчерпывающим без собственных данных сервисов по обходу

блокировок, которые бы достоверно показали эффективность или неэффективность работы этих сервисов в различных условиях.

Часть 1. Обзор технологий

Востребованность VPN-сервисов и других инструментов по обходу блокировок резко выросла с началом военной операции, достигнув пиковых значений к середине марта 2022 года. По данным Atlas VPN, количество скачиваний различных VPN сервисов выросло в России примерно в три раза по сравнению с 2021 годом,
с 12 585 576 скачиваний в 2021 до 33 540 600 скачиваний в 2022.
В 2023 году спрос резко упал, и за первую половину 2023 года российские пользователи скачали VPN только 3 366 919 раза.

Похожий тренд показывает и статистика отдельных VPN-сервисов, например количество скачиваний Proton VPN резко выросло в марте 2022 года, и уже к апрелю вернулось почти к изначальным значениям. Количество запросов на скачивание отдельных VPN-сервисов показывают похожую статистику.

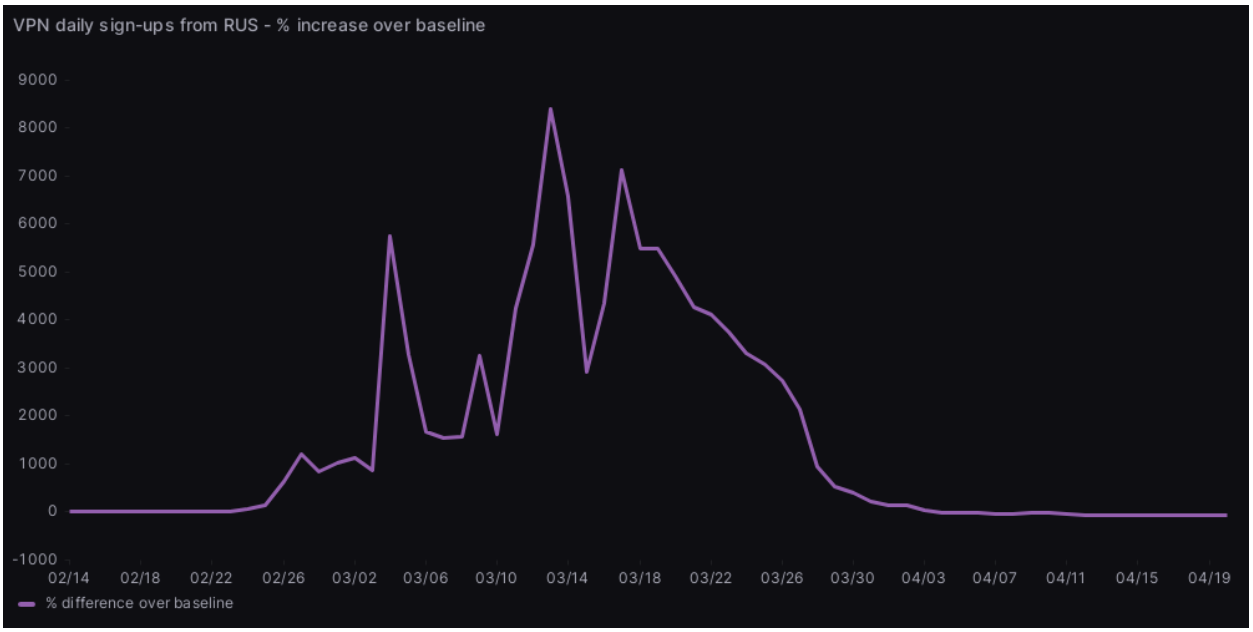

График: Количество ежедневных скачиваний Proton VPN с 14 февраля 2022 по 19 апреля 2022.

После марта небольшие пики пришлись на периоды с 29 мая по 4 июня 2022 года, и с 6 по 12 августа 2023 года. Эти периоды совпадают с датами сообщения о блокировках популярных в России VPN-сервисов, например, сообщения о блокировках Nord VPN и Proton VPN начали поступать 1-го и 2-го июня 2022 года соответственно.

Пик 6-12 августа также коррелирует со временем блокировки протоколов Wireguard и OpenVPN, доступ к которым восстановился 8-го августа 2023.

График: Количество запросов по теме VPN-сервисов в Google Search с начала 2022 года до конца августа 2023 года

Данные Яндекс Поиска показывают похожую статистику, с первым пиком в середине марта и вторым в начале июня 2022 года.

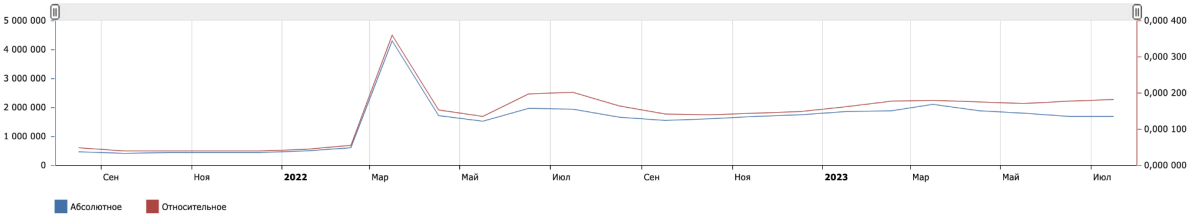

График: Количество запросов по теме VPN-сервисов в Яндекс поиске с начала 2022 года до конца июля 2023 года

Похожую динамику можно наблюдать и в отношении запросов на поиск сервисов Tor browser, пик популярности пришелся на 6-12 марта, с последующим пиком 29 мая — 4 июня и 25 июня — 1 июля 2023 года.

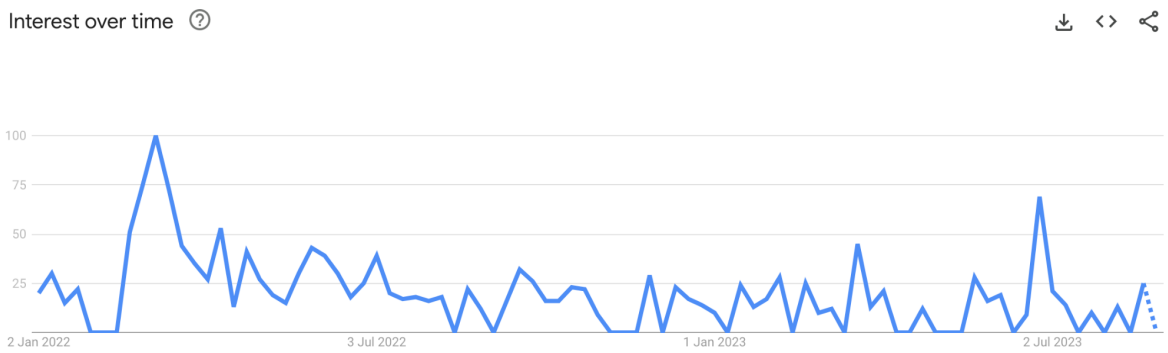

График: Количество запросов на тему Tor в Google Search с начала 2022 года до конца августа 2023 года

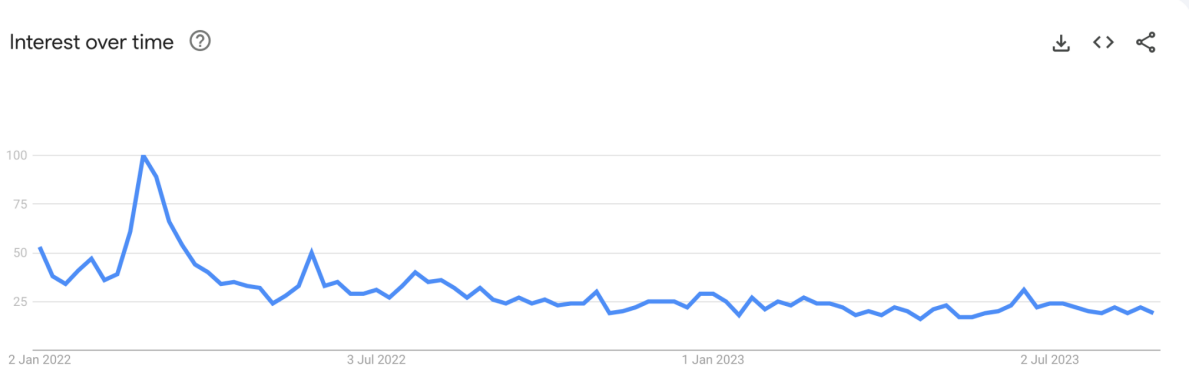

График: Количество запросов на тему Tor browser в Google Search с начала 2022 года до конца августа 2023 года

Метрики Tor также подтверждают несколько пиков подключений за последние два года. В декабре 2021 года количество пользователей сети Tor в России резко уменьшилось в связи с блокировкой Tor 8-го декабря 2021 года.

Количество подключений к сети продолжало падать до пика в марте 2022 года, в связи с массовыми блокировками различных сайтов и сервисов. Следующий пик приходится на сентябрь 2022 года, скорее всего он связан с разблокировкой сайта Tor в России и началом частичной мобилизации. Последний пик произошел в августе 2023, вероятнее всего он связан с блокировкой VPN-сервисов в начале августа.

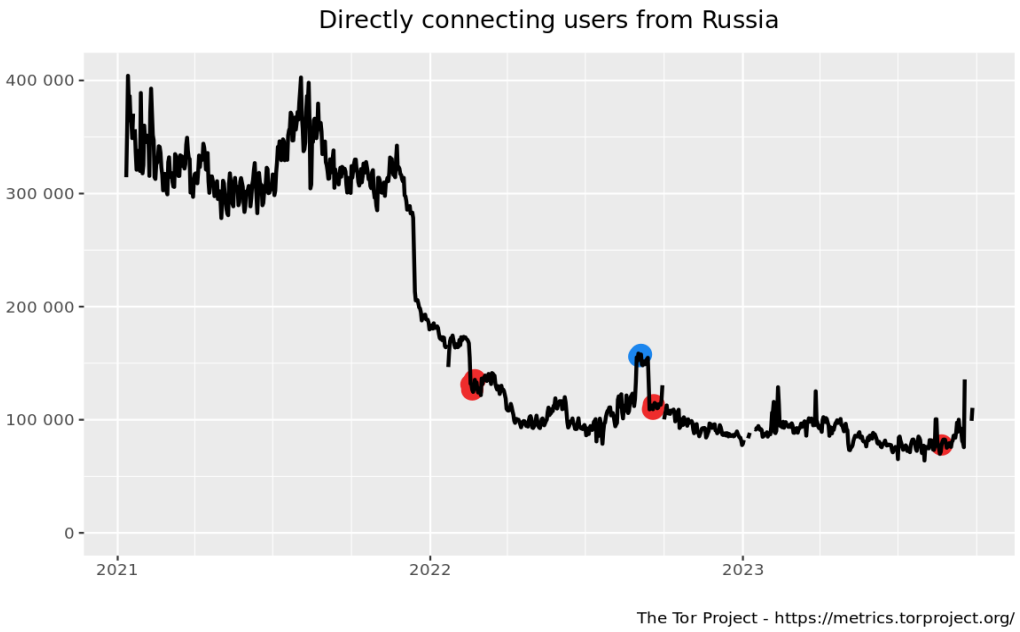

График: Статистика пользовательских подключений к сети Tor из России с 2021 года по конец сентября 2023 года.

Сервисы Tor примерно в 10 раз менее популярны, чем VPN-сервисы в целом — по сравнению с 2,1 млн запросов в месяц, относящихся к VPN-сервисам, лишь 200 тысяч поисковых запросов приходятся на сервисы Tor, по данным Яндекс Wordstat.

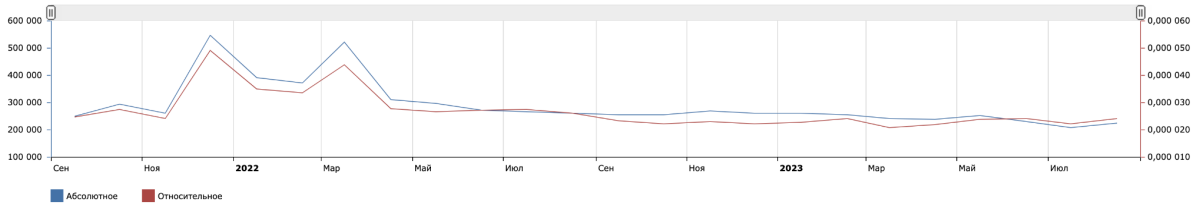

График: Количество запросов на тему Tor в Яндекс Поиске с конца 2021 года до августа 2023 года

В то же время, среди пользователей, опрошенных Роскомсвободой, сервисы Tor (Tor Browser, Orbot) оказались первыми по популярности среди других инструментов обхода блокировок, и чуть меньше половины респондентов

пользовались сервисами Tor хотя бы один раз за последний год, поэтому далее в исследовании мы включили данные о доступности Tor.

Помимо VPN-сервисов и сервисов Tor, мы включили в исследование несколько инструментов, которые помогают обходить блокировки, но не являются классическими VPN-сервисами, например, Lantern, Censor Tracker и АнтиЗапрет.

VPN-сервисы

Самыми популярными в России VPN-сервисами сейчас можно считать:

- AdGuard VPN
- Express VPN
- Proton VPN
- Turbo VPN
- VPN Planet
- VPN Proxy Speed
- VPN Master

Эти сервисы находятся в топе приложений Google Play, AppStore, являются одними из самых распространенных запросов к поисковым сервисам Google и Яндекс, и являются лидерами по количеству скачиваний в стране.

Чуть менее популярными сервисами можно считать Hola VPN, Nord VPN, Secure VPN, Tomato VPN, VPN — fast, secure, no limits, VPN Super Unlimited Proxy — это сервисы, популярные среди пользователей как минимум одного из поисковиков и одного из маркетплейсов.

Из 13 наиболее популярных в России VPN, 9 присутствуют в рейтинге VPN Overview, и только 4 из этих 9 считаются достаточно безопасными и эффективными (AdGuard VPN, Express VPN, Proton VPN, Nord VPN).

Четыре VPN, не включенные в рейтинг VPN Overview, часто не имеют даже сайта, где можно было бы найти информацию о сервисе, например сайт 'VPN Proxy Speed — Super VPN' в Google Play — https://www.supershell.me/, выдает пустую страницу. У 'VPN — fast, secure, no limits' нет ссылки на сайт, и единственные доступные документы — Privacy Policy и Terms of Service.

Из 13 наиболее популярных в маркетплейсах и поисковиках VPN-сервисов, только 4 можно считать условно безопасными, и только три из этих четырех сервисов прошли формальный внешний аудит: Express VPN, Proton VPN, Nord VPN.

По результата опроса, проведенного Роскомсвободой, самыми популярными сервисами оказались AdGuard VPN, Proton VPN, Express VPN, Amnezia VPN, Planet VPN, Lantern VPN, Psiphon VPN, Outline VPN, Turbo VPN.

Этот список частично совпадает со статистикой поисковых запросов и скачиваний приложений, отличия со статистикой запросов в поисковые сервисы может быть связано со спецификой аудитории, которая проходила опрос.

На основе наиболее популярных сервисов по количеству поисковых запросов, и по результатам опроса, мы составили следующий список из 15 популярных сервисов, которые в дальнейшем использовали для анализа:

1. AdGuard VPN
2. Express VPN
3. Proton VPN

4  Turbo VPN

5  VPN Planet

6  VPN Proxy Master

7  Amnezia VPN

8  Lantern VPN

9  Psiphon VPN

10  Outline VPN

11  Secure VPN

12  Nord VPN

13  RedShield

14  Hola VPN

15  AntiZapret

Чтобы определить доступность базовой информации о сервисах, упомянутых респондентами, мы проверили доступность сайтов этих сервисов на территории России.

По данным OONI, домены 8 из 15 самых популярных сервисов уже блокируются на территории РФ.

AdGuard VPN, AntiZapret, Hola, NordVPN, Psiphon, RedShield, TurboVPN и VPN Proxy Master либо недоступны для российских пользователей, либо доступны только на определенных сетях.

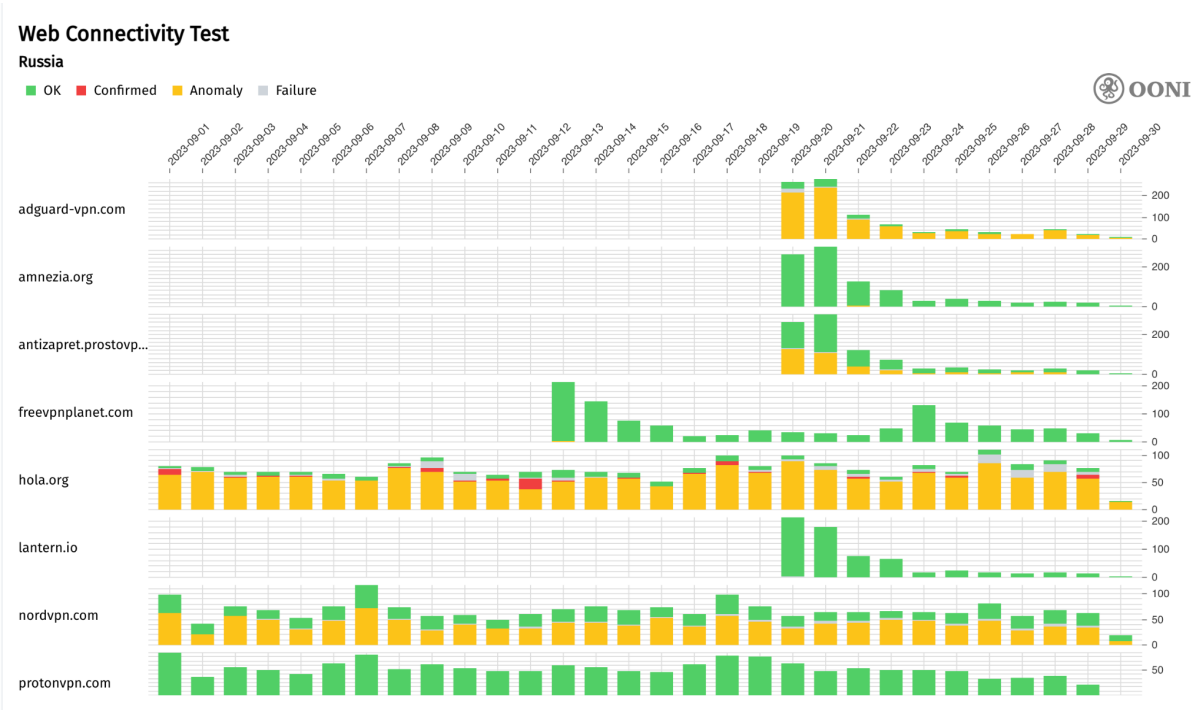

График: Измерения OONI, собранные на территории Российской Федерации с 1-го сентября 2023 года до 30-го сентября 2023 года

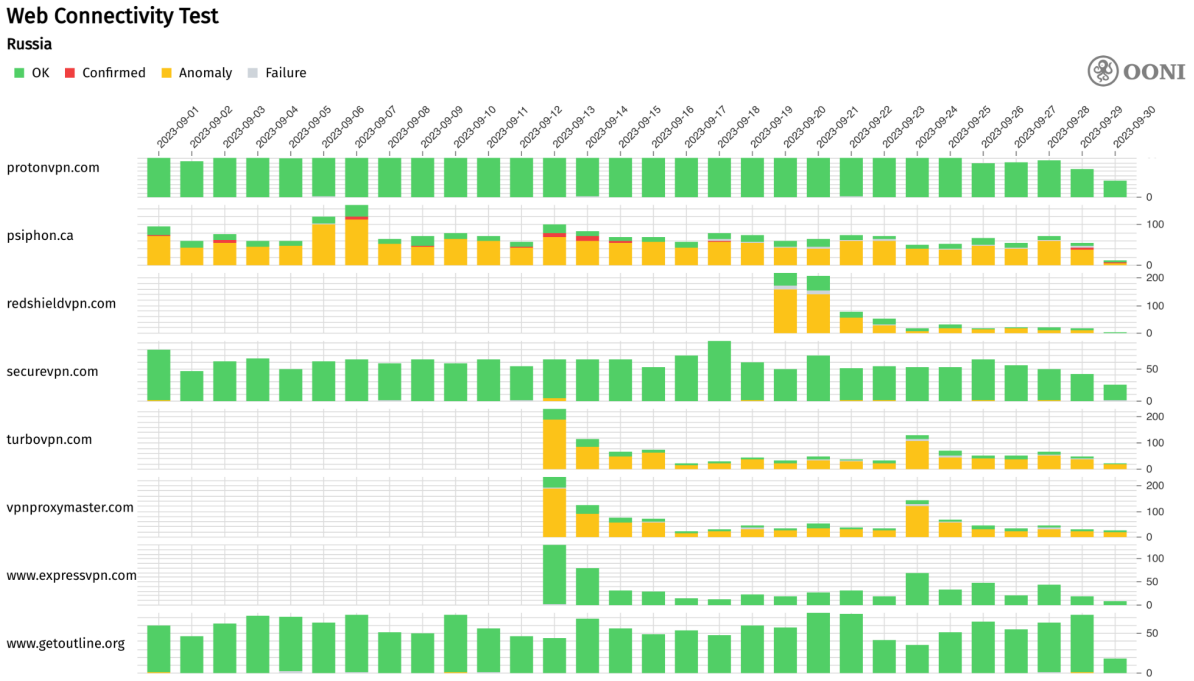

График: Измерения OONI, собранные на территории Российской Федерации с 1-го сентября 2023 года до 30-го сентября 2023 года

Таким образом, несмотря на популярность этих сервисов, количество их пользователей в ближайшее время может меняться, и возможно перераспределяться между другими сервисами, которые пока не подверглись блокировке.

Для новых пользователей, пока не пользующихся сервисами обхода блокировок, может быть сложнее найти информацию о сервисах, чьи сайты уже недоступны на территории РФ.

Среди тестов, относящихся к сайтам других сервисов из списка, также были обнаружены несколько заблокированных доменов, тема масштабирования блокировок сервисов по обходу блокировок может стать темой отдельного отчета в будущем.

Роскомсвобода ведет собственный рейтинг VPN Love, составленный экспертами в сфере инфобезопасности и цифровыми правозащитниками.

Это список надежных vpn, которые отвечают требованиям безопасности, анонимности, и при этом являются еще и доступными по цене. Эксперты ведут наблюдение за рынком vpn-сервисов, анализируют их характеристики, политики безопасности, отслеживают инциденты, проводят анализ репутации основателей. Реализована функция безопасной оплаты сервисов по обходу блокировок с российских карт и криптовалютой на VPNPay.

VPN-протоколы

Основные протоколы, используемые 15 сервисами, которые мы выделили в предыдущей части, это:

- OpenVPN,
- Wireguard,
- Shadowsocks,
- IKEv2,
- V2Ray.

Из 15 сервисов четыре используют только протокол OpenVPN, либо собственный протокол, созданный на основе OpenVPN, еще два сервиса используют Wireguard в дополнение к OpenVPN. Только два сервиса из пятнадцати используют протокол Shadowsocks: Amnezia VPN и Outline VPN.

OpenVPN считается одним из самых уязвимых для блокировки протоколов. В исследовании 2022 года CensoredPlanet в рамках эксперимента смогли идентифицировать 85 % трафика идущего через OpenVPN. [1]

Этому протоколу также отдают предпочтение российские банки и коммерческие компании, использующие VPN.

В то же время, только шесть из пятнадцати сервисов имеют встроенную возможность использовать обфускаторы, ExpressVPN предлагает использовать Camouflage, разработанный Surfshark, Proton VPN предлагает обфускатор собственной разработки (Proton VPN Stealth), Nord VPN использует обфускатор, разработанный Tor (obfsproxy), Amnezia предлагает использовать cloak.

В том же исследовании Censored Planet исследователи продемонстрировали, что один из самых популярных обфускаторов, патч XOR, также легко идентифицируется и был обнаружен в 90 % случаев.[1] Такие же результаты были достигнуты и в случае обфускации с помощью TLS, SSL, obfs2/3. Чуть лучше работает обфускация TCP, в этом случае использование OpenVPN смогли обнаружить только в 34 случаях из 49 (примерно в 70 % случаев).

Только пять сервисов предлагают встроенные инструменты обеспечения анонимности: AdGuard VPN предлагает SOCKS5 proxy, Nord VPN и АнтиЗапрет предлагают Onion прокси, Nord VPN и RedShield предлагают возможность подключения через Double VPN.

Таким образом, когда в августе 2023 года начали блокировать протоколы OpenVPN и Wireguard, как минимум 6 из 15 сервисов начали испытывать

---

[1] Xue, Diwen, Reethika Ramesh, Arham Jain, Michalis Kallitsis, J Alex Halderman, Jedidiah R Crandall, and Roya Ensafi. 'OpenVPN Is Open to VPN Fingerprinting', n.d.

проблемы с доступом в сеть. В зависимости от эффективности обфускации остальных сервисов и осведомленности пользователей о существовании подобной настройки, еще как минимум три сервиса (Express VPN, Nord VPN, Proton VPN) могли оказаться заблокированы.

Например, по данным OONI видно, что блокировки в августе 2023 частично задели Psiphon, использующий L2TP/IPsec и Shadowsocks протоколы, но для большинства пользователей он остался доступным. То же самое произошло во время волны блокировок в середине сентября.

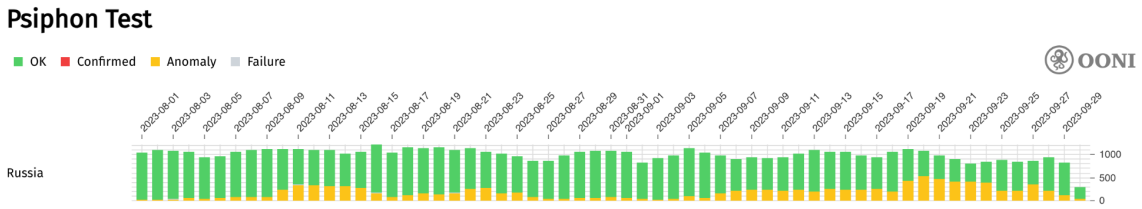

График: Измерения OONI доступности сервисов Psiphon VPN с 1 августа по 30 сентября 2023 года

В октябре 2023 Amnezia VPN анонсировала свой протокол AmneziaWG, предназначенный для стран со строгой цензурой.

Это сделанный на основе стандартного WireGuard форк, который добавляет в пакеты мусора и рандома, не позволяющие DPI-системам привычно блокировать WireGuard. Таким образом удается добиться высокой скорости, как у WireGuard, но быть защищенным от блокировки по протоколу.

Часть 2. Обзор блокировок

Интернет-цензура в России в 2023 году приняла всеобъемлющие масштабы, в середине 2023 года Роскомнадзор отчитался об увеличении числа блокировок на 85 % по сравнению с 2022 годом. При этом еще в 2022 году уже были заблокированы большинство сайтов независимых медиа, активно блокировались зеркала независимых ресурсов, сайты правозащитных проектов и политических организаций. По данным OONI, цензура в России затронула практически все типы контента — от коммерческих бизнесов до экологических и просветительских проектов.

Вместе с объемом блокировок изменилась и процедура — появилось больше ведомств, имеющих возможность требовать блокировку ресурсов в обход судов. Например, в 2022 году Генпрокуратура получила возможность включать ресурсы в реестр Роскомнадзора без судебного решения. Можно заметить, что в 2022 году 34 тысячи ресурсов были внесены в реестр «анонимно» без указания госоргана, ответственного за блокировку.

До 2022 года таких решений о блокировке было всего около трехсот за последние 10 лет. Ни один из ресурсов, внесенных «анонимно» не был разблокирован. Роскомсвобода продолжает отслеживать количество заблокированных ресурсов по причине военной цензуры, сейчас это число уже больше 15 тысяч.

	С января 2022 (01.2022 — 09.2023)		За все время (11.2012 — 09.2023)		Итого на 30.09.23
Ведомство	**Заблокировано**	**Разблокировано**	**Заблокировано**	**Разблокировано**	**Заблокировано сейчас**
Генпрокуратура	21 569	1156	174 199	105 250	**68 949**
Госорган не указан (предположительно Генпрокуратура)	34 028	295	34352	295	**34 057**
МВД	16 074	29 647	81 967	62 516	**19 451**
Минкомсвязь	17 479	1	49 028	11	**49 107**
Минцифры	3 663	0	5 779	0	**5 779**
Минюст	6	0	6	0	**6**
Мосгорсуд	27 455	33 430	211 226	153 028	**58 198**
Росалкорегулироование	2 032	2 998	15 427	12 188	**3 239**
Росздравнадзор	5 564	7 120	24 209	13 909	**10 300**
Роскомнадзоор	23 738	9 319	93 732	49 485	**42 297**
Росмолодежь	266	255	769	375	**394**
Роспотребнадзор	966	555	6 270	4 810	**1 460**
Россельхознадзор	22	84	106	84	**22**
ФНС	50 420	176 830	429 277	265 126	**164 151**
ФСКН	173	154	27 592	27 127	**465**
ЦИК	1	0	1	0	**1**
Суд	28 238	155 021	365 048	306 335	**58 713**
ИТОГО	**231 694**	**416 865**	**1 518 988**	**1 000 539**	**516 589**

Таблица: Количество заблокированных и разблокированных сайтов с начала 2022 до конца сентября 2023 года по данным открытого реестра Роскомсвободы.

В 2022 году был принят ряд законодательных проектов расширяющих полномочия Роскомнадзора и категории контента, подлежащие блокировке, а также усиливающие ответственность провайдеров за успешную реализацию цензуры.

Так, МВД определило механизм блокировки сайтов, содержащих персональные данные лиц, находящихся под госзащитой. Ответственным за внесение таких сайтов в реестр запрещённых был признан Роскомнадзор, который будет обязан в течение суток с момента получения решения о признании информации

запрещенной и постановления об ограничении к ней доступа внести соответствующую запись в реестр.

В марте 2022 года вступил в силу закон о наказаниях до 15 лет лишения свободы за публикацию фейков о российской армии. Сейчас суды начинают выносить первые приговоры с реальными сроками более 5 лет лишения свободы.

В июле 2022 года Путин подписал закон, который вводит штрафы для операторов связи, которые не установили ТСПУ. Власти объясняют необходимость использования этого оборудования для цензуры наличием “информационных угроз для россиян”.

В августе 2022 года Минцифры опубликовало документы, которыми предложило наделить Роскомнадзор полномочиями по блокировке зеркал ранее заблокированных сайтов. Постановление вступило в силу с 1 марта 2023 года и будет действовать в течение 6 лет.

В декабре 2022 года в силу вступил закон о запрете ЛГБТ-пропаганды. Теперь такого рода контент также вносится в реестр запрещенных по решению Роскомнадзора. Были заблокированы сайт «Nuntiare et Recreare», посвященный верующим представителям ЛГБТ различной религиозной и конфессиональной принадлежности, а также сайт музея истории ЛГБТ в России.

В сентябре 2023 года Минцифры выложило на общественное обсуждение проект постановления кабмина, который касается ведения Роскомнадзором реестра запрещенной информации. Документ также расширяет полномочия РКН, позволяя ему блокировать «информацию о способах, методах обеспечения доступа к информационным ресурсам и (или) информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации». Проект — http://regulation.gov.ru/p/141488.

С марта 2024 года маркетплейсы должны будут удалять приложения VPN-сервисов по требованию Роскомнадзора. В следующем году он может начать блокировать VPN-сервисы, которые предоставляют доступ к заблокированным в России сайтам. В первую очередь блокировка коснётся сервисов, размещенных в магазинах приложений.

Ранее, в июле 2023 подписан закон № 406-ФЗ, запрещающий рекламировать способы обхода блокировок, а также разработаны критерии блокировки информации про обход блокировок:

- Наличие описания действий, позволяющих получить доступ к заблокированным ресурсам.
- Наличие информации, дающей представление о способах доступа к заблокированным ресурсам.
- Наличие информации, направленной на убеждение в привлекательности способов обхода блокировок.
- Информация, обосновывающая достоинства обхода блокировок, а также дающая положительную оценку или одобрение обходу блокировок.
- Предложения о приобретении доступа к средствам обхода блокировок.
- Наличие информации, предоставляющей возможность получения доступа к заблокированным ресурсам.

Ограничения не будут работать в отношении научной, научно-технической и статистической информации о способах обхода блокировок.

Типы блокировок

Рассматривая тему средств по обходу блокировок, необходимо разобраться с типами блокировок, собственно, сайтов и медиа. Техническая имплементация блокировок в России долго носила ярко-выраженный децентрализованных характер — каждый провайдер был ответственен за реализацию блокировки на своих сетях, и мог использовать любые методы блокировки на свое усмотрение. В результате, в данных проектов по измерению сетей на предмет цензуры, видно, что одни и те же ресурсы блокируются разными способами на разных сетях, а иногда даже в рамках одной сети могут быть использованы различные инструменты блокировок.

Такие инструменты могли включать[2] [3]:

- Фильтрацию по ключевым словам незашифрованных пакетов данных
- Фильтрацию HTTP-пакетов в исходящих и входящих запросах и ответах
- TCP/IP блокировки с завершением сессий со всеми нежелательными хостами или возвращением страницы блокировки
- DNS-манипуляции с возвращением ложных доменных имен или перенаправлением на страницу блокировки
- SNI-фильтрацию зашифрованного трафика с последующим вмешательство в TLS-рукопожатие (закрытие соединения, включение RST-пакета, time out сессии)

После принятия в 2019 году закона 90-ФЗ (о «Суверенном рунете») всем российским операторам пришлось установить ТСПУ (технические средства противодействия угрозам), российскую версию DPI (Deep Packet Inspection). В 2021 году случился первый известный случай применения ТСПУ, когда на многих сетях одновременно началось замедление (троттлинг) работы Twitter. В отличие от предыдущих непоследовательных и разрозненных блокировок, троттлинг был реализован в одно и тоже время на разных сетях различными провайдерами, позднее Роскомнадзор подтвердил, что блокировка реализовывалась с помощью ТСПУ.

В тоже время в 2021 году было известно, что девайсы установлены не у всех провайдеров, и во время троттлинга твиттера был произведен большой сопутствующий ущерб – пользователи сообщали о проблемах с доступом к государственным сайтам, Почте России и другим сервисам. В исследовании 2022 года говорится о том, что в рамках исследования получилось обнаружить более 6000 устройств на более чем 650 сетях.

В этом же исследовании, авторы постарались понять, какие типы трафика может определять ТСПУ, и на какие типы трафика он реагирует, чтобы определить наиболее успешные стратегии обхода блокировок. По итогам ряда экспериментов, исследователи определили, что ТСПУ может реагировать на разные типы трафика, как основанного на SNI, так и на IP, и QUIC. ТСПУ блокирует только попытки соединения идущие с территории РФ, и отслеживает

[2] Xynou, Maria, and Arturo Filastò2022-03-07. ‘New Blocks Emerge in Russia amid War in Ukraine: An OONI Network Measurement Analysis’, 7 March 2022. https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/.

[3] D. Xue, R. Ramesh, ValdikSS, L. Evdokimov, A. Viktorov, A. Jain, E. Wustrow, S. Basso, and R. Ensafi. Throttling twitter: An emerging censorship technique in russia. In Proceedings of the 21st ACM Internet Measurement Conference, IMC ’21, page 435–443, New York, NY, USA, 2021. Association for Computing Machinery.

в основном подключение к информационным ресурсам: блогам, новостным медиа, социальным сетям. Несмотря на то, что часть ресурсов уже включена в реестр Роскомнадзора, ТСПУ все равно продолжает отслеживать подключение к этим ресурсам.

Блокировки с помощью ТСПУ все еще возможно обходить, и авторы статьи предлагают несколько различных решений. Однако на данном этапе не до конца ясно как именно будут дальше развиваться блокировки с помощью ТСПУ, а скорость имплементации всей системы, и масштаб ее воздействия заставляет предполагать пессимистичные сценарии – для сравнения на постройку фаервола в Китае у государства ушли десятилетия, на имплементацию ТСПУ с момента принятия закона ушло менее трех лет.

Отдельно стоит заметить, что блокировки сайтов и сервисов могут иметь большой сопутствующий ущерб не только в контексте доступа к информации, но и в контексте работы независимых медиа в целом. Так, с одной стороны некоторые медиа отмечали, что работа их репортеров напрямую зависит от доступности сайта, так как многие интервьюируемые отказываются общаться с журналистами, если видят, что ресурс подвергается блокировке. С другой стороны, блокировка сайтов медиа ведет к невозможности принимать донаты, поэтому многие медиа начали использовать отдельные краудфандинговые платформы, доступные в России. К сожалению, доступность платформ не гарантирует их доступность для независимых организаций, так платформа Boosty сообщила о закрытии и «пожизненной блокировке» аккаунта Новой газеты. Также цензуре подверглись многие платформы, которыми медиа и блогеры пользовались для создания контента. Например, конструктор для создания сайтов Tilda заблокировал, а потом полностью удалил сайт издания DOXA в марте 2022-го года, а платформа для создателей подкастов Mave заблокировала доступ к проекту «Продолжение следует» в октябре 2023-го года. Таким образом, цензура влияет не только на доступность существующего контента, но и на производство новых материалов ограничивая способность проектов собирать пожертвования и ограничивая доступ к сервисам, которыми проекты пользуются для создания контента.

Важно отметить, что помимо инструментов обхода блокировок, существуют и другие способы получить доступ к заблокированному контенту. Например, многие медиа подстраиваются под пользователей, и перераспределяют контент по разным платформам, которые пока не заблокированы в России – Telegram, YouTube. Также многие независимые издания продолжают публиковать зеркала и создают автоматизированные системы по их публикации, таким образом пока

что опережая усилия Роскомнадзора по автоматизированной блокировке новых зеркал. Большинство опрошенных медиа отметили, что скорость блокировки зеркал менялась на протяжении последних двух лет в зависимости от общей информационной повестки, и в момент обострений (например, похода ЧВК Вагнер) скорость блокировки нового зеркала у самых крупных медиа могла достигать 1.5 минуты.

Такая оперативность реагирования на запуск новых зеркал, и масштабное использование ТСПУ для блокировок зашифрованного соединения и отслеживания использования инструментов по обходу блокировок, заставляет думать, что уровень и масштаб цензуры может увеличиться в ближайшие годы.

Блокировки VPN-сервисов и других средств для обхода блокировок

VPN-сервисы в России блокировались в разном масштабе начиная с 2017 года, когда вступил в силу закон о запрете использования VPN-сервисов и анонимайзеров. В 2019 году Роскомнадзор начал требовать от VPN-сервисов, действующих на территории РФ подключения к Федеральной государственной информационной системе (ФГИС), тогда уведомления были направлены Nord VPN, Hola! VPN, ExpressVPN. В июне 2021 были заблокированы VyprVPN и Opera VPN, в сентябре 2021 Hola! VPN, ExpressVPN, KeepSolid VPN Unlimited, Nord VPN, Speedify VPN и IPVanish VPN.

В 2021 году появлялись первые сообщения о протокольных блокировках, например, в сентябре пользователи Ростелекома и мобильной связи Beeline сообщали о проблемах с подключением с помощью протокола Wireguard. Похоже, что это была попытка реализовать блокировку с помощью ТСПУ, однако не очень удачная, так как пользователи отдельных сетей сообщали о случайной блокировке других сервисов, в том числе Avito, Twitch и другие стриминговые сервисы.

В мае 2022 года пользователи Windscribe сообщали о проблемах в работе сервиса, в июне 2022 года пользователи Proton VPN и NordVPN начали сообщать

о проблемах с доступом к сервисам. Позднее Роскомнадзор подтвердил, что ограничил доступ к Proton VPN, а по данным некоторых медиа также планировалось ограничить доступ к VPN Proxy Master, Browsec VPN, vpn-super unlimited proxy, Melon VPN, Windscribe VPN, VPN RedCat secure unlimited.
В 2022 году предпринимались попытки блокировать сервисы с помощью ТСПУ, через блокировку доменов и IP-адресов, ассоциируемых с VPN-сервисами. Так, например, в случае Proton блокировке подвергся API-хост api.protonvpn.ch, а в случае Windscribe блокировались IP-адреса серверов сервиса. В то же время, пользователи сообщали и о блокировке отдельных протоколов, в регионах Западной Сибири и на юге России протоколы IPsec и IKEv2 оказались недоступны на корпоративных сетях.

В январе 2023 года начали появляться новые сообщения о попытках блокировок протоколов IKEv2 и OpenVPN, так 23-го января в канале Tech Talk сообщали о том, что в восточных регионах России (Алтай, Бийск, Омск, Новосибирск и другие) блокировались именно протоколы, в то время как IP-адреса серверов VPN оставались доступными. 1-го февраля эта волна блокировок распространилась и на другие регионы, в том числе: Пермь, Орск, Новочебоксарск, Тольятти, Якутск, Казань, Елабуга, Уфа, Чебоксары, Нижний Новгород.

Следующая попытка блокировки протоколов началась 30-го мая 2023 года с частичной блокировкой протоколов OpenVPN, IKEv2 и IPSec. Тогда о блокировке сообщали пользователи клиентов МТС (мобильный интернет Москва, домашний интернет Челябинск), «Билайн» (домашний и мобильный интернет в Москве, Казани, Краснодаре, Новосибирске), «Мегафон», «МирТелеком», Yota, Tele2, «Таттелеком», Wifire (Netbynet), «Дом.Ру» и других провайдеров. В течение суток эта волна блокировок закончилась, и вечером 31-го мая все сервисы снова стали доступными.

В начале августа 2023 года пользователи снова начали сообщать о блокировке протоколов OpenVPN и Wireguard. Оба протокола, как мы писали выше, очень популярны, и используются большинством VPN-сервисов для установки соединения. Planet VPN сообщали также о блокировке IKEv2, некоторые пользователи сообщали о блокировке IPSec.

Один из участников форума ntc.party, автор GoodbyeDPI, провел ряд тестов, чтобы понять какие именно действия происходят в момент попытки установки соединения и обнаружил следующее:

«Для всех VPN-протоколов, кроме L2TP, сначала выполняется обнаружение протокола, затем «проверка» протокола (проверка ответа или мониторинг нескольких пакетов в TCP/UDP-сессии), затем происходит разрыв сессии (TCP) или блокировка прохождения трафика по связке srcip-srcport-dstip-dstport (UDP).

Мобильный Теле2 Санкт-Петербург:

- L2TP (UDP 1701, без IPsec): пакеты L2TP Control Message (самые первые пакеты сессии) не доходят до сервера на порт 1701
- IPsec (UDP 500/4500): блокируется прохождение UDP-пакетов после нескольких переданных пакетов во время установления сессии
- PPTP (TCP 1723): разрывается TCP-соединение после отправки сервером ответа Start-Control-Connection-Reply на первый пакет в сессии Start-Control-Connection-Request, до установки GRE-туннеля не доходит
- OpenVPN UDP: блокируется прохождение UDP-пакетов после нескольких переданных пакетов DATA после установки сессии
- OpenVPN TCP: разрывается TCP-соединение после нескольких переданных пакетов DATA после установки сессии
- WireGuard: блокируется прохождение UDP-пакетов после 5 принятых пакетов данных (Transport Data) с сервера

Проводной МТС Кузбасс:

- Блокируется только OpenVPN UDP/TCP, L2TP, WireGuard, но не PPTP и IPsec
- L2TP, в отличие от Теле2, доставляет пакеты на сервер, но ответы сервера блокируются
- WireGuard: блокируется прохождение UDP-пакетов после первого пакета данных (Transport Data) с сервера

Блокировки отличаются от тех, какие применяют для коммерческих VPN-сервисов (вроде ProtonVPN, Windscribe): их фильтруют с самого первого пакета, не позволяя сессии установиться.»

Вечером 8-го августа доступность всех сервисов снова восстановилась. Многие VPN обещали рассмотреть использование других протоколов и найти способы устанавливать соединение несмотря на блокировки.

29-го сентября проект «На связи» отметил, что начали поступать новые сообщения о блокировках, на этот раз пользователи в основном сообщали о неэффективности протокола Wireguard. В этот раз блокировки, судя по всему,

были менее масштабными, и повлияли в основном на центральную часть России, однако охватили пользователей как крупных, так и региональных провайдеров: МТС, «Билайн», «Мегафон», «Теле2», Yota, «Трайтек», Skynet, «Акадо», «Эр-Телеком».

Единственный крупный протокол, который пока что не подвергся массовым блокировкам — Shadowsocks, его сложнее определить, но нельзя гарантировать, что сервисы, использующие Shadowsocks не подвергнутся блокировкам со следующей волной. Также пока не блокируются сервисы обфускации, однако, как мы упомянули выше, большинство сервисов обфускации работают не эффективно и также могут быть обнаружены с помощью DPI.

Так как блокировки с помощью ТСПУ не всегда осуществляются по решению суда или включению ресурса в реестр Роскомнадзора, некоторые сервисы смогли подать иск к Роскомнадзору с требованием отменить блокировку. Пока неизвестно, чем закончится этот процесс, но этот иск может стать хорошим прецедентом в юридической практике.

Заключение

Цензура в России усиливается с каждым годом как по числу, так и по разнообразию блокируемых сервисов. Если раньше блокировки часто были непоследовательными и одни и те же ресурсы могли блокироваться разными способами и в разной степени у разных провайдеров на различных сетях, то в 2021 году в России для блокировки впервые были применены ТСПУ. В 2022 году исследователи показали, что с помощью DPI устройств можно сравнительно легко обнаруживать соединения, осуществляемые с помощью одного из самых распространенных протоколов OpenVPN даже при использовании обфускации. В 2023 году мы видим, как ТСПУ применяется в России для блокировки отдельных VPN-протоколов, и как эти блокировки могут происходить скоординировано в одно и то же время у разных провайдерах в разных регионах. Такая скорость развития механизмов блокировок в совокупности с новым законодательством заставляет опасаться попыток полной блокировки существующих VPN-сервисов на территории Российской Федерации.

Несмотря на то, что большинство российских пользователей пользуются VPN-сервисами и знают о существовании интернет-цензуры и блокировок,

многие из них недостаточно осведомлены о том, как именно работают инструменты обхода блокировок. Такая неосведомленность с одной стороны приводит к тому, что люди выбирают неблагонадежные сервисы предпочитая более дешевые или бесплатные приложения, с другой стороны в случае блокировки отдельных протоколов не имеют достаточных знаний, чтобы настроить используемый сервис и обойти блокировку.

Цензура в России реализуется не только на уровне сети, но также и на уровне отдельных сервисов, в том числе на уровне социальных сетей и поисковых платформ. Такую цензуру намного сложнее отследить, и во многом нам приходится опираться на данные и заявления отдельных сервисов.
Те источники, которые нам удалось найти и проанализировать в рамках этого исследования, показывают, что даже несмотря на доступность таких сервисов как YouTube и Google, мы не можем утверждать, что у их пользователей есть полный доступ к независимым источникам информации.

В рамках этого исследования мы обнаружили несколько лакун, на которые нам бы хотелось обратить внимание правозащитного, технологического и исследовательского сообщества в России.

В первую очередь это исследование работы ТСПУ — на данный момент опубликовано всего несколько академических исследований о том, сколько российских ТСПУ установлено на данный момент и как они фильтруют трафик российских пользователей. Так как ТСПУ являются ключевым элементом российской цензуры, который позволяет усилить ее за счет централизации, мы считаем, что технологическому и исследовательскому сообществу нужно больше взаимодействовать для изучения этой темы.

Вторая тема, которую мы бы хотели обозначить — осведомление пользователей о механизмах работы VPN-сервисов и обфускации, а также об опасностях использования неаудированных и непроверенных сервисов. Текущая пользовательская стратегия перебора VPN-сервисов в поисках рабочего приложения может стать большой уязвимостью при блокировке основных популярных протоколов.

Мы будем и дальше следить за доступностью VPN-сервисов и протоколов, анализировать ситуацию и держать вас в курсе на сайте, в телеграмме и актуализировать рейтинг VPN-Love.