Исследование

Хроники цензуры

Систематическое давление на независимые медиа в России

09.12.2024

Около трех лет назад, когда Россия начала военную операцию в Украине, она также инициировала параллельную кампанию: цензурную войну против независимых новостных СМИ внутри страны.

Уже через неделю после начала конфликта интернет-провайдеры в России начали блокировать доступ к нескольким иностранным новостным сайтам (таким как BBC и Deutsche Welle) и независимым российским новостным сайтам (таким как Meduza и New Times). В течение первого года цензура независимых новостных СМИ в России стала повсеместной. В нашем предыдущем отчете мы подтвердили блокировку 139 доменов новостных СМИ в России.

Этот отчет – совместное исследование RKS Global и Open Observatory of Network Interference (OONI). Мы приводим данные OONI о блокировке сайтов новостных СМИ в России за последний год, а также информацию о том, как эти блокировки повлияли на независимые российские новостные медиаорганизации.

Авторы:
RKS Global, Elizaveta Yachmeneva (OONI), Maria Xynou (OONI), Mehul Gulati (OONI), Arturo Filastò (OONI).

RKS Global

OONI

Содержание

Основные выводы

Наш анализ сетевых измерений OONI, собранных в России за последний год (с 1 сентября 2023 года по 1 сентября 2024 года), показывает:

- Блокировку не менее 279 доменов новостных СМИ. Основываясь на известных нам отпечатках, мы автоматически подтвердили блокировку 279 доменов новостных СМИ (что вдвое больше, чем в исследовании 2023 года, когда мы подтвердили блокировку 139 доменов). Заблокированные домены включают как иностранные, так и независимые российские новостные сайты, причем большинство из них заблокированы более чем на 10 различных сетях в России. В таких случаях провайдеры, по-видимому, осуществляют блокировку на основе DNS децентрализованным способом (например, возвращая 188.186.146.208 как часть DNS-разрешения).

- Большинство блокировок новостных СМИ в России осуществляется с помощью TLS-вмешательства. Большинство измерений OONI из многочисленных сетей в России показывают, что блокировки в основном реализуются с помощью TLS-вмешательства. В одних случаях данные OONI показывают обрыв TLS-сессии, в других – вброс RST-пакета сразу после сообщения ClientHello во время TLS-рукопожатия.

- Централизованное управление блокировками, но децентрализованное развертывание DPI. Подтверждая выводы Censored Planet, данные OONI показывают на широкое использование ТСПУ (российской системы DPI), поскольку блокировки, по-видимому, осуществляются на уровне SNI, и одни и те же домены блокируются в большинстве сетей в одно и то же время. Это позволяет предположить, что, хотя развертывание ТСПУ децентрализовано (поскольку каждый провайдер обязан установить ТСПУ в своей сети), но блокировки, скорее всего, централизованы и управляются Роскомнадзором.

- Цензурная борьба между Россией и ЕС. После решения Совета Европы от 2022 года многие страны ЕС продолжают блокировать доступ к Sputnik и Russia Today (RT). После того как в мае 2024 года Совет Европы принял решение о приостановке вещания еще 4 связанных с Россией СМИ, в июне 2024 года Министерство иностранных дел России объявило об ограничении

доступа к 81 СМИ стран-членов ЕС (включая несколько сайтов общеевропейских СМИ) на территории России. По данным OONI, доступ к сайтам этих новостных СМИ ЕС блокируется в России со 2 августа 2024 года.

В ходе интервью с представителями 15 независимых российских новостных СМИ респонденты рассказали, что основными проблемами, с которыми они сталкиваются, являются:

- Финансовые сложности. В последние годы российские власти включили большинство независимых медиа в список «иностранных агентов» или «нежелательных организаций», что привело к ограничениям на рекламные предложения, партнерские коллаборации и общему сокращению финансовой поддержки таких организаций в стране. Это усугубилось санкциями и блокировкой платежных систем, которые еще больше увеличили финансовую нагрузку на независимые российские медиа в последние годы. В результате многие СМИ были вынуждены искать альтернативные источники финансирования (например, краудфандинг или международные гранты), и многим из них еще предстоит найти устойчивую модель финансирования.

- Закрытие медиа проектов. В результате финансовых трудностей и усиления цензуры некоторые российские издания были вынуждены закрыться в 2024 году. Например, приостановили свою деятельность следующие СМИ: Якутская газета «Туймаада», экологическое издание «Кедр» (часть коллектива основала новое издание «Смола»), радио «Эхо Кавказа» (приостановило вещание в связи со статусом «нежелательной организации»), СМИ «Курьер.Среда», „Астра“ (временно закрылась из-за отсутствия финансирования, но вскоре возобновила работу благодаря краудфандингу), „Служба поддержки“ (из-за финансовых проблем после неполучения поддержки международных доноров), It’s My City (лишилась лицензии за освещение антивоенных протестов).

- Проблемы безопасности. Возросшие риски слежки и ограничения в распространении информации о VPN создали как цифровые, так и юридические риски для сотрудников СМИ, работающих с конфиденциальной информацией. Присутствие медиапроектов в российских социальных сетях стало небезопасным, поскольку взаимодействие с материалами «нежелательных организаций» легко

отслеживается и может привести к уголовному преследованию читателей. Чтобы минимизировать угрозы для своей аудитории, многие СМИ закрыли свои аккаунты на российских платформах и перешли на зарубежные сервисы с усиленной защитой данных. Однако большинство зарубежных сервисов по-прежнему заблокированы в России, и смена платформ привела к частичной потере российской аудитории.

- Частичная потеря российской аудитории. В результате блокировки сайтов, включения в список «иностранных агентов», «экстремистских» или «нежелательных организаций» (статусы создающие риски для читателей, взаимодействующих с материалами таких организаций) многие независимые СМИ потеряли часть аудитории в России. Эти статусы также сделали невозможным использование платного продвижения через платформы, сервисы и сотрудничество с блогерами, что лишило СМИ важных каналов вовлечения аудитории. Когда блокировки вынуждали медиаорганизации менять платформы, это также приводило к частичной потере аудитории.

- Растущая самоцензура. Правовые статусы «нежелательной организации», «экстремиста» и «иностранного агента», присвоенные российскими властями многим независимым медиапроектам, затрудняют работу с авторами и респондентами, поиск и привлечение новых авторов, респондентов и экспертов, поскольку любое сотрудничество со СМИ становится рискованным и может повлечь за собой уголовную ответственность участников. Такие статусы усиливают самоцензуру и приводят к уходу из профессии отдельных журналистов и закрытию медиаорганизаций.

- Снижение возможностей для освещения событий в России. Трудности эмиграции, низкие зарплаты и постоянный стресс приводят к выгоранию сотрудников, особенно руководителей СМИ. Статус «иностранного агента» или «нежелательной организации» заставляет многих авторов и респондентов неохотно сотрудничать с медиа, что ограничивает возможности СМИ освещать события в России. Независимые медиа сталкиваются с рядом проблем, включая трудности с поиском авторов, доступом к информации, работой с респондентами, находящимися в России, и адаптацией к быстро меняющейся цифровой среде. Все это

требует высокой степени гибкости и способности быстро реагировать на новые угрозы.

Несмотря на все вышеперечисленные трудности, независимые российские медиаорганизации сохраняют стойкость. Усилившиеся угрозы свободе прессы в России привели к укреплению солидарности и сотрудничества между СМИ, которые делятся решениями и предупреждениями о новых технологиях, используемых цензорами. Многие независимые российские СМИ продемонстрировали высокий уровень адаптации, используя зеркала, VPN и альтернативные платформы (например, Telegram) для обхода блокировок и коммуникации со своей аудиторией. Тем не менее, для усиления борьбы за свободу прессы в России все еще необходима существенная международная поддержка.

Введение

24 февраля 2022 года – в тот самый день, когда началась полномасштабная война в Украине, – Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) опубликовал заявление, в котором утверждается, что СМИ обязаны «использовать только информацию и данные, полученные из официальных российских источников».

Неделю спустя Роскомнадзор начал блокировать доступ к нескольким иностранным и независимым российским новостным сайтам по причине «распространения ложной информации». В тот же день в России был принят законопроект с поправками в Уголовный кодекс РФ, предусматривающий ужесточение наказания вплоть до лишения свободы на срок до 15 лет для лиц, осужденных за распространение ложной информации о российских военных операциях, дискредитацию Вооруженных сил РФ и призывы к антироссийским санкциям. В течение года по данным OONI был заблокирован доступ как минимум к 139 доменам новостных СМИ, что свидетельствует об усилении повсеместной цензуры новостных СМИ в России.

В рамках нашего партнерства OONI и RKS Global провели исследование масштабов и влияния цензуры независимых новостных СМИ в России за последний год. Наша цель – задокументировать и повысить осведомленность общественности о продолжающейся блокировке сайтов независимых российских новостных СМИ в России на фоне продолжающихся боевых действий в Украине, а также рассказать о том, как эти блокировки повлияли на некоторые из этих медиаорганизаций.

В частности, основные вопросы, которыми руководствовалось данное исследование, включают:

- Какие сайты независимых российских новостных СМИ заблокированы в России?
- Какие методы используют интернет-провайдеры в России для осуществления блокировок? Как различаются блокировки у разных интернет-провайдеров в России?
- Как эти блокировки влияют на независимые российские новостные СМИ?

Чтобы ответить на первые два вопроса, мы проанализировали данные измерений Web Connectivity теста OONI, собранные в России за последний год, с 1 сентября 2023 года по 1 сентября 2024 года. Для изучения третьего вопроса мы провели исследование открытых источников и опросили 15 независимых российских новостных СМИ.

Основываясь на нашем предыдущем исследовании, посвященном цензуре в интернете в России, мы начали это исследование с нескольких предположений:

- Повсеместная цензура новостных СМИ. В феврале 2023 года наш анализ данных OONI подтвердил блокировку (по меньшей мере) 139 доменов новостных СМИ в России.
- Децентрализованная цензура. Каждый интернет-провайдер в России отвечает за осуществление блокировок по требованию правительства самостоятельно. В результате данные OONI свидетельствуют о том, что в разных сетях страны блокировки осуществляются по-разному. Некоторые провайдеры осуществляют блокировку с помощью нескольких методов одновременно, что затрудняет их обход.
- Различные методы цензуры. Данные OONI показали, что для блокировки сайтов российские интернет-провайдеры используют следующие методы цензуры:
    - 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

Поскольку данное исследование включает в себя анализ более поздних измерений OONI (с сентября 2023 года по сентябрь 2024 года), мы изучаем, изменилась ли и в какой степени блокировка независимых новостных СМИ в России. Что еще более важно, мы изучаем, как эти продолжающиеся блокировки повлияли на способность независимых российских новостных организаций свободно сообщать о событиях для аудитории в России в условиях продолжающейся войны в Украине.

Методы

В рамках данного исследования мы поставили перед собой цель изучить, какие независимые российские новостные сайты были заблокированы в России за последний год, а также влияние этих блокировок на независимые российские новостные медиа-организации.

Для этого мы использовали смешанный исследовательский метод, сочетая количественные и качественные методы. Количественные методы включали анализ данных OONI, а качественные – интервью, исследование открытых источников, анализ законодательства и обновление списка сайтов Citizen Lab для России (в него входят URL-адреса, проверенные на наличие цензуры в стране).

В частности, чтобы выяснить, какие сайты независимых российских новостных СМИ блокируются в России и какие методы цензуры применяют интернет-провайдеры, мы проанализировали данные сетевых измерений OONI, собранные в России за последний год (с 1 сентября 2023 года по 1 сентября 2024 года). Чтобы изучить влияние этих блокировок, мы опросили 15 независимых российских новостных СМИ. Мы также проанализировали список сайтов Citizen Lab для России и обновили его, включив в него дополнительные сайты независимых российских новостных СМИ для тестирования OONI Probe. Более подробная информация представлена ниже.

Обновление списка тестируемых сайтов

Мы начали с изучения списка сайтов Citizen Lab для России, который включает URL-адреса, тестируемые на предмет цензуры пользователями OONI Probe в России. По умолчанию пользователи OONI Probe проверяют URL, включенные в два тестовых списка: (а) глобальный список (в него входят актуальные для всего мира ссылки) и (б) список для конкретной страны (в него входят только ссылки, относящиеся к конкретной стране). В России пользователи OONI Probe обычно проверяют ссылки, включенные как в глобальный, так и в российский тестовые списки.

Учитывая, что целью нашего исследования является изучение блокировки сайтов независимых российских новостных СМИ, на первом этапе мы проанализировали ссылки в российском списке для тестирования и составили список отсутствующих сайтов независимых российских новостных СМИ. Проект RKS Global провел полное

обновление списка, удалив URL-адреса, утратившие актуальность, и добавив 196 дополнительных URL-адресов новостных СМИ для тестирования. Процесс обновления тестового списка был ограничен ссылками, отнесенными к категории «Новостные СМИ (NEWS)» в соответствии с категориями Citizen Lab. Как только эти обновления тестового списка были одобрены, вновь добавленные URL автоматически получили приоритет для тестирования OONI Probe в России. Это позволило обеспечить стабильное покрытие измерениями вновь добавленные URL в период с 29 марта 2024 года (когда был объединен запрос) до 1 сентября 2024 года (конец периода анализа данных OONI для данного исследования).

Анализ данных OONI

В рамках этого исследования Open Observatory of Network Interference (OONI) проанализировала данные сетевых измерений OONI, собранные в России в период с 1 сентября 2023 года по 1 сентября 2024 года. В ходе этого анализа OONI стремилась выяснить, блокировались ли сайты новостных СМИ (включенные в глобальный и российский тестовые списки Citizen Lab) в течение анализируемого периода, и различалась ли реализация таких блокировок в разных сетях в России.

С 2012 года OONI разрабатывает бесплатное программное обеспечение с открытым исходным кодом OONI Probe), предназначенное для измерения различных форм интернет-цензуры, включая блокировку сайтов и приложений. Каждый месяц OONI Probe регулярно запускается добровольцами примерно в 170 странах, включая Россию, где из всех стран пользователи OONI Probe собирают второй по величине объем измерений (после США, которые собирают больше всех измерений в мире). По умолчанию сетевые измерения, собранные пользователями OONI Probe, автоматически публикуются как открытые данные в режиме реального времени.

OONI Probe включает в себя эксперимент Web Connectivity, который предназначен для измерения блокировки сайтов (включенных в публичные, созданные сообществом списки Citizen Lab). В частности, тест OONI Web Connectivity предназначен для измерения доступности URL-адресов путем выполнения следующих действий:

- Идентификация DNS-реестра
- Поиск DNS
- TCP-соединение с возвращенными IP-адресами
- TLS-рукопожатие с возвращенными IP-адресами

- HTTP(s) GET запрос после перенаправления

Вышеописанные действия выполняются автоматически как из сети пользователя, так и из контрольной точки. Если результаты из обеих сетей одинаковые, проверенная ссылка аннотируется как доступная. Если результаты отличаются, проверенная ссылка аннотируется как аномальная, а тип аномалии дополнительно характеризуется в зависимости от причины, вызвавшей сбой (например, если TCP-соединение не произошло, измерение аннотируется как TCP/IP аномалия).

Аномальные измерения могут свидетельствовать о блокировке, однако возможны и ложные срабатывания. Поэтому мы считаем, что вероятность блокировки выше, если общий объем аномальных измерений высок по сравнению с общим количеством измерений (сравнение на уровне сети в одном и том же диапазоне дат для каждого типа эксперимента OONI Probe).

Каждое измерение веб-соединения предоставляет сетевую информацию (например, информацию о TLS-рукопожатиях), которая помогает оценить, есть ли в аномальном измерении признаки блокировки. Поэтому мы дезагрегируем данные по причинам, вызвавшим аномалию (например, сброс соединения во время TLS-рукопожатия), и если они совпадают, то мы интерпретируем это как более сильный сигнал блокировки.

Основываясь на эвристике OONI, мы можем автоматически подтвердить блокировку сайтов по отпечаткам, если вместо сайта показывается заблокированная страница или если DNS-реестр возвращает IP, уже известный нам как связанный с цензурой. Хотя этот метод позволяет нам автоматически подтверждать блокировку сайтов в России и многих других странах (таких как Италия, Казахстан, Иран и Индонезия), мы проанализировали аномальные измерения OONI (с помощью нашей методологии анализа данных OONI), чтобы обнаружить более тонкие и продвинутые методы цензуры.

В рамках данного исследования мы проанализировали данные сетевых измерений OONI, собранные в России в период с 1 сентября 2023 года по 1 сентября 2024 года. Нас в первую очередь интересовал анализ блокировки сайтов медиа, поэтому мы ограничили наш анализ только измерениями собранными с помощью теста Web Connectivity. Из всех измерений веб-соединения, собранных в России за последний год, мы проанализировали домены (включенные в глобальный и российский списки тестирования Citizen Lab), которые категоризованы как “News Media (NEWS)” в списках тестирования Citizen Lab. Это позволило нам изучить блокировку сайтов новостных СМИ, не анализируя все протестированные в России сайты (которые включают широкий спектр самых разных и не имеющих отношения к нашему исследовательскому вопросу сайтов).

Мы агрегировали аномальные измерения, собранные в России, по типам сбоев («dns», «tcp_ip», «http-failure», «http-diff»), чтобы оценить, присутствуют ли они постоянно (или типы сбоев меняются), поскольку более последовательный тип сбоя, наблюдаемый в большом объеме измерений, дает более сильный сигнал блокировки. Далее мы проанализировали эти сбои для выявления специфических ошибок (таких как «connection_reset_error» или «generic_timeout_error»), которые позволили бы нам охарактеризовать потенциальную блокировку, и объединили ошибки для изучения того, совпадают ли они и в какой степени по всем (соответствующим) измерениям на каждой протестированной сети.

В том числе, мы проанализировали информацию из данных о TLS-рукопожатии в этих измерениях, чтобы понять, были ли ошибки результатом цензуры в рамках TLS-рукопожатия. Например, измерение может показать, что DNS-разрешение возвращает правильные IP-адреса, с которыми можно установить соединение, но сессия TLS-рукопожатия завершается после первого сообщения ClientHello (которое является незашифрованным), что приводит к стандартной ошибке «generic_timeout_error». Хотя мы считаем, что такое измерение показывает признаки потенциального вмешательства на основе TLS, мы не будем делать выводы только на основании одного измерения.

Поэтому мы агрегировали ошибки, чтобы определить, является ли большой процент аномальных измерений для тестируемой ссылки одинаковой ошибкой (например, «tls_timeout_error») по сравнению с общим объемом измерений в конкретной сети в определенном диапазоне дат. Чем выше соотношение одинаковых ошибок (от аномальных измерений) по сравнению с общим количеством измерений, тем сильнее сигнал (и тем выше наша уверенность), что доступ к тестируемому домену (а) заблокирован, и (б) заблокирован определенным образом (например, в рамках TLS-рукопожатия).

В рамках нашего анализа мы исключили случаи, которые показывали слабый сигнал блокировки. К ним относились случаи с небольшим/ограниченным охватом измерений (по сравнению с общим охватом измерений в тестируемой ASN за период анализа), низким процентом аномалий (по сравнению с общим объемом измерений для тестируемого сайта), относительно большой долей непоследовательных типов ошибок, а также случаи, которые были определены как ложные срабатывания на основе известных нам ошибок или других проблем (например, глобальные показатели ошибок в результате того, что тестируемые сервисы размещены на ненадежных серверах или измерения собраны в нестабильных сетях).

Как только мы увидели сильные сигналы блокировок в различных российских сетях, мы начали рассматривать измерения с различными ошибками как более

слабые сигналы (считая их вероятными ложными срабатываниями). Далее мы ограничили наш анализ ASN, которые получили наибольший охват измерений и самые сильные сигналы о блокировках. В итоге результаты данного исследования ограничиваются измерениями, которые мы считали более сильными сигналами на основе наших методов анализа.

Интервью

В качественной части исследования мы поставили своей целью проанализировать и задокументировать последствия блокировок и других форм цензуры на деятельность независимых СМИ в России в 2023-2024 году. В рамках качественного исследования мы постарались рассмотреть не только технические аспекты блокировки независимых медиа, но и другие методы цензуры, применяемые в России. Мы проанализировали не только сами блокировки, но и эволюцию правоприменительных практик, в том числе, рост числа проектов со статусами «иностранного агента», «нежелательной» или «экстремистской» организации. Кроме того, мы пытались понять, как сами медиа воспринимают развитие цензуры, какое влияние это оказывает на их деятельность и какие технические решения они используют, чтобы сохранить доступ к своей аудитории в России.

В рамках качественного исследования мы определили следующие цели:

1. Исследовать цифровые стратегии независимых СМИ в условиях повсеместной цензуры: Разобраться в использовании различных каналов и тактик, которые независимые медиа применяют для сохранения доступа к информации (например, VPN и социальные сети).

2. Задокументировать влияние BigTech на доступ к независимой информации: проанализировать роль платформ (например, YouTube, Telegram, Twitter) и влияние их алгоритмов на доступ к независимым новостям в России.

3. Проанализировать влияние санкций и блокировок на способность медиа эффективно распространять информацию и взаимодействовать с российской аудиторией.

4. Анализ влияния статуса «иностранного агента» и «нежелательной организации» на финансовую стабильность СМИ, а также на эффективность их работы и способность взаимодействовать с их аудиторией.

Чтобы ответить на поставленные исследовательские вопросы, мы проанализировали данные из открытых источников и провели серию интервью с представителями 15 СМИ и медиа-проектов.

Выборка респондентов включает медиа разных масштабов и форматов — от крупных изданий с многомиллионной аудиторией до небольших проектов, с аудиторией в несколько тысяч человек. Некоторые из проектов, с которыми мы говорили, не имеют публичных платформ как таковых и общаются с аудиторией через мессенджеры, в то время как другие используют весь доступный арсенал: сайты, социальные сети, мобильные приложения. Многие из опрошенных медиа имеют специальные статусы, такие как «иностранный агент», «нежелательная организация» или «экстремистская организация».

Мы надеемся, что такое разнообразие респондентов дало нам возможность понять, какие аспекты цензуры затрагивают весь сектор независимых СМИ, а какие пока касаются только отдельных проектов. Разнообразие выборки позволило нам изучить как общие тенденции, так и конкретные последствия ужесточения цензуры.

Каждому из респондентов интервью мы задавали следующие вопросы:

1. Что изменилось по вашим наблюдениям в блокировках за последний год на ваших ресурсах или ресурсов партнеров?
2. Какая у вас сейчас стратегия доступа к аудитории? Перешли ли вы на зеркала и другие инструменты, обеспечивающие доступ к контенту без использования VPN? Какая основная платформа для вас сейчас? Меняли ли вы основную платформу для публикаций?
3. Как у вас меняются охваты в соцсетях? Продолжается ли рост аудитории на разных платформах несмотря на блокировки?
4. Поменялась ли у вас география пользователей? Понимаете ли вы географию пользователей, можете ли вы отделить пользователей VPN сервисов от пользователей, которые подключаются к вашим ресурсам не из России?
5. Повлияло ли на вашу работу наличие специального ограничительного статуса (при наличии)? Было ли ограничение со стороны крупных технологических компаний или последствия от санкционного давления?

Для обеспечения безопасности наших респондентов, мы приведем в этом исследовании только обобщенные и обезличенные результаты, исключив собранную информацию об успешных стратегиях и тактиках по восстановлению доступа аудитории к информации СМИ.

Мы благодарим всех участников интервью, и все проекты, согласившиеся поговорить с нами о том, как они переживали цензуру в течение последнего года.

Методологические ограничения

Результаты данного исследования имеют ряд ограничений, в том числе:

- **Диапазон дат анализа.** Результаты исследования ограничены данными измерений сети OONI, собранными в России в период с 1 сентября 2023 года по 1 сентября 2024 года. Таким образом, результаты измерений, проведенных в другие периоды, исключены из данного исследования.

- **Тип измерений.** Проанализированные данные в основном касаются измерений OONI Web Connectivity, связанных с тестированием сайтов на цензуру. Поэтому результаты других экспериментов OONI Probe (особенно тех, которые не измеряют блокировку сайтов и приложений) исключены из данного исследования.

- **Тестируемые сайты.** Тестирование в основном ограничивается URL-адресами, включенными в два тестовых списка Citizen Lab: глобальный список (включающий URL-адреса, имеющие отношение к международной тематике) и российский список (включающий URL-адреса, имеющие отношение только к России). Поскольку эти списки тестируются пользователями OONI Probe и имеют ограничения по пропускной способности, они обычно ограничиваются примерно 1 000 ссылок. Кроме того, в рамках этих списков, мы ограничили наш анализ ссылками из категории Citizen Lab «News Media (NEWS)». В результате в списки сайтов, которые мы тестировали, могли не попасть другие сайты, заблокированные в России, и результаты исследования ограничиваются только проверкой URL-адресов, включенных в категорию «News Media (NEWS)» существующих списков. Кроме того, 196 сайтов новостных СМИ были включены в российский тестовый список только 29 марта 2024 года, что означает, что эти URL-адреса тестировались в течение более короткого периода времени по сравнению с другими URL-адресами, которые уже были в списке. Учитывая, что тестовые списки Citizen Lab составляются сообществом, мы признаем предвзятость при выборе сайтов, добавляемых в списки, а также риск неправильной категоризации этих сайтов.

- **Охват веб-сайтов при тестировании.** Не все URL-адреса, включенные в тестовые списки, измеряются одинаково по всей России с течением времени. Наличие данных OONI для конкретного сайта зависит от того, тестировали ли их пользователи OONI Probe в России, в каких сетях и когда. В результате тестируемые сайты получали различный охват тестирования в течение всего анализируемого периода, что влияет на результаты.

- **Тестируемые сети.** Хотя тесты OONI Probe регулярно проводятся на нескольких сетях в России, не все сети тестируются одинаково. Скорее, доступность измерений зависит от того, к каким сетям были подключены пользователи OONI Probe во время проведения тестов. В результате охват измерений в разных сетях в течение анализируемого периода различается, что влияет на результаты. Более того, мы ограничили результаты данного исследования сетями, которые получили наибольший охват измерений и которые представили самые сильные сигналы блокировки в рамках анализируемого периода.

- **Сигналы блокировки**. В рамках анализа данных мы ограничили наши выводы сигналами, которые, по нашему мнению, были более надежными и указывали на цензуру, осуществляемую правительством, исключив при этом случаи, которые считались слабыми сигналами (как обсуждалось выше в разделе «Методы»). В результате мы признаем риск того, что в наших выводах могут быть пропущены некоторые случаи блокировок (если эти случаи были аннотированы как слабые сигналы в рамках нашего анализа данных).

- **Интервью**. В попытке изучить влияние цензуры на новостные СМИ в России мы провели интервью с 15 независимыми российскими новостными СМИ. С помощью этих интервью мы стремились дополнить анализ измерений сети OONI качественными данными. Однако мы признаем, что результаты этих интервью не дают полное представление о влиянии цензуры на (большинство) новостных СМИ в России, поскольку они отражают мнение ограниченного числа опрошенных организаций. Мы призываем исследователей проводить более подробные исследования на эту тему (с большей выборкой интервью).

Общий контекст

В последние годы российский сегмент интернета — Рунет — переживает систематическое и растущее давление со стороны властей. Это давление затронуло не только традиционные формы блокировок, но и значительно расширилось в технологическом и правовом отношении. На практике интернет-цензура появилась в России задолго до событий 2022 года: усилия по контролю Рунета уходят корнями в 2012 год, когда российские власти начали впервые блокировать сайты по IP-адресам. Но первый опыт показал, что такие меры легко обходятся пользователями.

В последние годы подход к блокировкам изменился — и технически, и юридически, и по интенсивности и масштабу воздействия. 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: Deep Packet Inspection Technology (DPI) устройства подконтрольные Роскомнадзору и установленные на сетях всех провайдерах. С тех пор ограничительные законы стали все более жесткими, категории запрещенной информации все чаще стали включать в себя политически-мотивированный контент, а локальные отключения интернета в зонах массового скопления людей, стали распространенной практикой. Блокировке и запросам удаление контента подверглись социальные сети, мессенджеры, защищенные почтовые сервисы, биткоин-сервисы, VPN и иные инструменты обхода блокировок, а с 2022-2023 года началась реализация блокировки самих VPN-протоколов. И если раньше цензура была направлена на блокирование доступа к запрещенной информации, то к 2024 году основной фокус сместился на борьбу со средствами обхода блокировок (таких как VPN и Tor).

В 2024 году на обновление системы блокировки интернет-ресурсов и сервисов в Рунете до 2030 года было выделено почти 59 миллиардов рублей, а с 1 марта 2024 года в России вступил в силу запрет на публикации «информации о способах обхода установленных в России блокировок ресурсов», что существенно ограничивает правое поле и возможности распространения информации о противодействии цензуре. Более того, сервисы по мониторингу доступности ресурсов и измерению цензуры также стали блокироваться, включая OONI Explorer.

Рунет также подвергся серьёзной перестройке в части платформ и крупных компаний:

- С одной стороны, власти вытесняют западные компании, заменяя их российскими аналогами, отличающимися усиленным контролем и возможностью отслеживания действий пользователей. Этот процесс коснулся крупнейших игроков, таких как «Яндекс», где после ухода основателя Аркадия Воложа управление было передано структурам, близким к правительству. Схожие изменения произошли с Тинькофф Банком, который с 2022 года полностью перешёл под новое руководство. Иностранные IT-гиганты, включая Alphabet и Apple, также испытали давление — им пришлось либо удалять контент, либо ограничивать доступ к своим сервисам по требованию российских государственных органов.
- С другой стороны, санкции и уход международных сервисов и платёжных систем вынудили пользователей либо отказаться от них, либо искать альтернативы, которые зачастую оказываются менее надёжными и безопасными.

В результате по ряду этих причин Рунет и глобальный интернет теперь представляет собой в некотором смысле два параллельных пространства, которые пока ещё существуют в одном браузере, но связность между ними постепенно угасает.

Цензура медиа в России

Россия занимает 162-е место из 180 в рейтинге свободы прессы за 2024 год, составляемом международной организацией «Репортёры без границ». Цензура независимых СМИ в российском интернет-пространстве к 2024 году демонстрирует значительное увеличение объёмов блокировок и усиление механизмов контроля над информацией. Процесс обострился в 2022 году, когда с началом полномасштабного конфликта с Украиной были сначала массово, а затем последовательно заблокированы сайты всех независимых СМИ, публиковавших антивоенные материалы. С тех пор число заблокированных ресурсов продолжает расти, что связано с попытками регулирования общественного восприятия военных событий.

Процедура блокировки СМИ становится все менее прозрачной: в реестре запрещённых сайтов часто не указывается орган, инициировавший блокировку. Уведомления о блокировках ограничиваются требованиями удалить контент, при этом причины не разъясняются. Особенно это касается материалов, критикующих военные действия или освещающие их с альтернативной точки зрения.

Правовые меры, такие как включение СМИ в списки «иностранных агентов» или «нежелательных организаций», создают дополнительные препятствия для их работы. Статус «иностранного агента» требует строгой маркировки контента и отчётности, что значительно увеличивает административную нагрузку на редакции, ограничивает доступ к рекламодателям и усложняет сотрудничество с партнёрами. Эти ограничения также способствуют росту самоцензуры среди журналистов.

Журналисты независимых изданий сталкиваются с угрозами, преследованиями и обысками, которые сопровождаются изъятием оборудования и данных. Такие действия способны парализовать деятельность редакций. Давление со стороны правоохранительных органов создаёт атмосферу страха и неуверенности, что негативно сказывается на свободе слова и качестве журналистских расследований.

Выводы OONI

Наш анализ данных OONI, собранных в России за последний год (с 1 сентября 2023 года по 1 сентября 2024 года), показывает, что цензура новостных СМИ в России остается повсеместной. Мы автоматически подтвердили блокировку 279 доменов новостных медиа), что вдвое больше, чем в предыдущем исследовании 2023 года (139 доменов). Среди заблокированных сайтов СМИ есть как иностранные, так и независимые российские новостные сайты, большинство этих сайтов были заблокированы в течение всего периода анализа данного исследования. Наш анализ также показывает, что, хотя интернет-провайдеры в России продолжают осуществлять блокировку независимо друг от друга децентрализованным способом (некоторые провайдеры продолжают блокировать домены с помощью DNS), преобладающим методом цензуры остается TLS-вмешательство.

Подтвержденные блокировки новостных сайтов в России

В рамках анализа данных OONI, собранных в России за последний год (с 1 сентября 2023 года по 1 сентября 2024 года), мы подтвердили блокировку 279 доменов, относящихся к категории «News Media (NEWS)» на основе категоризации тестового списка Citizen Lab. Эти домены относятся к широкому спектру новостных СМИ, включая как иностранные (такие, как BBC, Deutsche Welle и Voice of America), так и независимые российские новостные сайты (например, Meduza). Среди них есть

также несколько украинских новостных сайтов, «Кавказ-центр» (чеченское новостное интернет-агентство, которое также заблокировано в Казахстане) и сайт журналистских расследований Bellingcat – все они уже много лет заблокированы в России.

Полный список из 279 доменов новостных СМИ, блокировку которых мы подтвердили, доступен в этом CSV). В этом CSV также указаны конкретные сети, где блокировка этих доменов была автоматически подтверждена на основании отпечатков, присутствующих в базе данных OONI. Как видно из CSV, блокировка подавляющего большинства этих доменов была подтверждена более чем на 10 различных сетях в России.

Однако эти домены были автоматически подтверждены заблокированными на относительно небольшом количестве сетей по сравнению с общим количеством тестируемых сетей, на которых они были проверены в течение анализируемого периода. Вероятно, это связано с тем, что провайдеры в России осуществляют блокировку, используя разные методы цензуры, помимо тех, которые мы можем автоматически обнаружить и подтвердить на основе существующих отпечатков. Например, блокировка www.bbc.com была автоматически обнаружена на основании IP-адреса 188.186.146.208 (включенного в нашу базу существующих отпечатков), который был получен в результате DNS-разрешения. Однако в других случаях российские интернет-провайдеры блокируют доступ к BBC, используя иные методы, например, с помощью TLS-вмешательства.

Блокировка сайтов независимых российских СМИ

В нашем предыдущем исследовании мы уже выяснили, что многие интернет-провайдеры в России осуществляют блокировки преимущественно с помощью TLS-вмешательства. На данный момент мы не можем автоматически определять такие блокировки, поэтому мы провели более подробный анализ измерений, цензуру в которых мы не можем автоматически обнаружить и подтвердить по существующим отпечаткам. Для более детального анализа мы попросили RKS Global проанализировать список из 279 подтвержденных заблокированных доменов новостных СМИ) и выбрать из этого списка домены российских независимых новостных сайтов для более глубокого анализа.

В результате, мы проанализировали следующие 23 домена:

dossier.center

gubernia.media

ichkeria.info

mbk.news

novayagazeta.eu

semnasem.org

skat.media

thebell.io

theins.ru

thetruestory.news

tjournal.ru

cherta.media

doxa.team

glasnaya.media

helpdesk.media

tayga.info

verstka.media

www.proekt.media

www.svoboda.org

meduza.io

ovdinfo.org

zona.media

tvrain.tv

Результаты нашего анализа по каждому из вышеперечисленных доменов представлены на следующих шести диаграммах, которые объединяют результаты тестирований OONI в нескольких сетях в России в период с 1 сентября 2023 года по 1 сентября 2024 года.

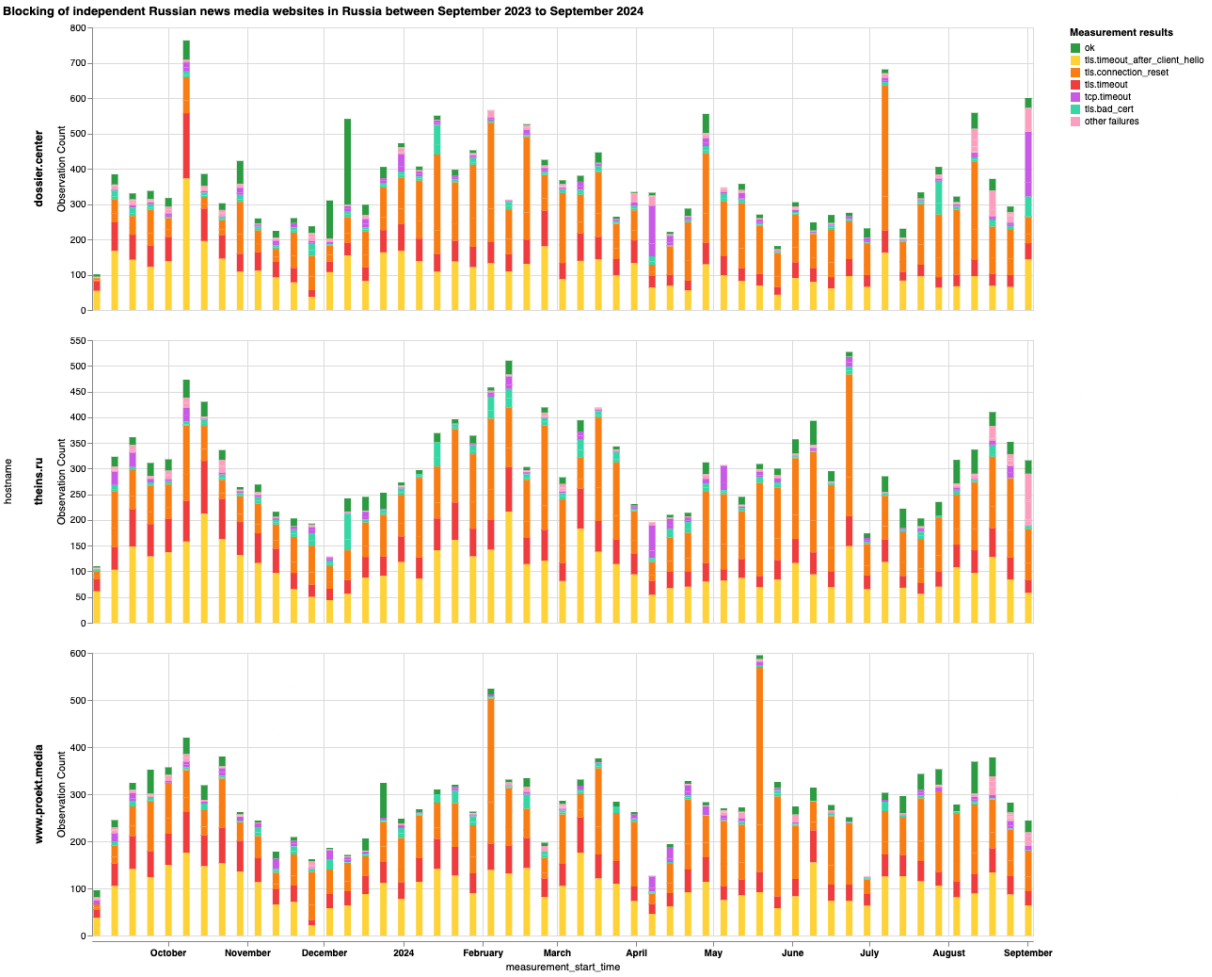

График: Результаты тестирования доменов dossier.center, theins.ru и www.proekt.media с помощью OONI Probe в нескольких сетях в России в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

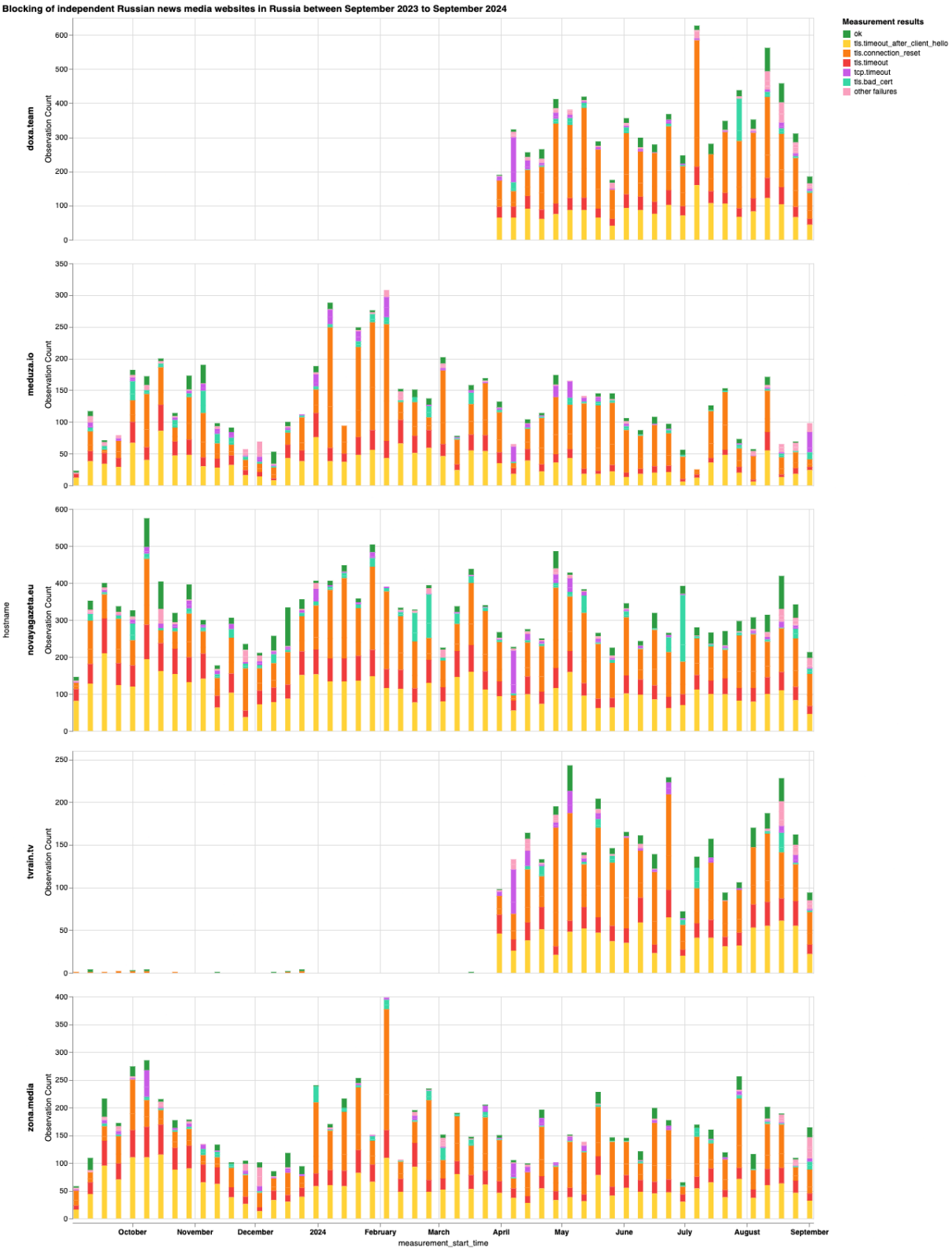

График: Результаты тестирования доменов doxa.team, meduza.io, novayagazeta.eu, tvrain.tv и zona.media с помощью OONI Probe в нескольких сетях в России в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

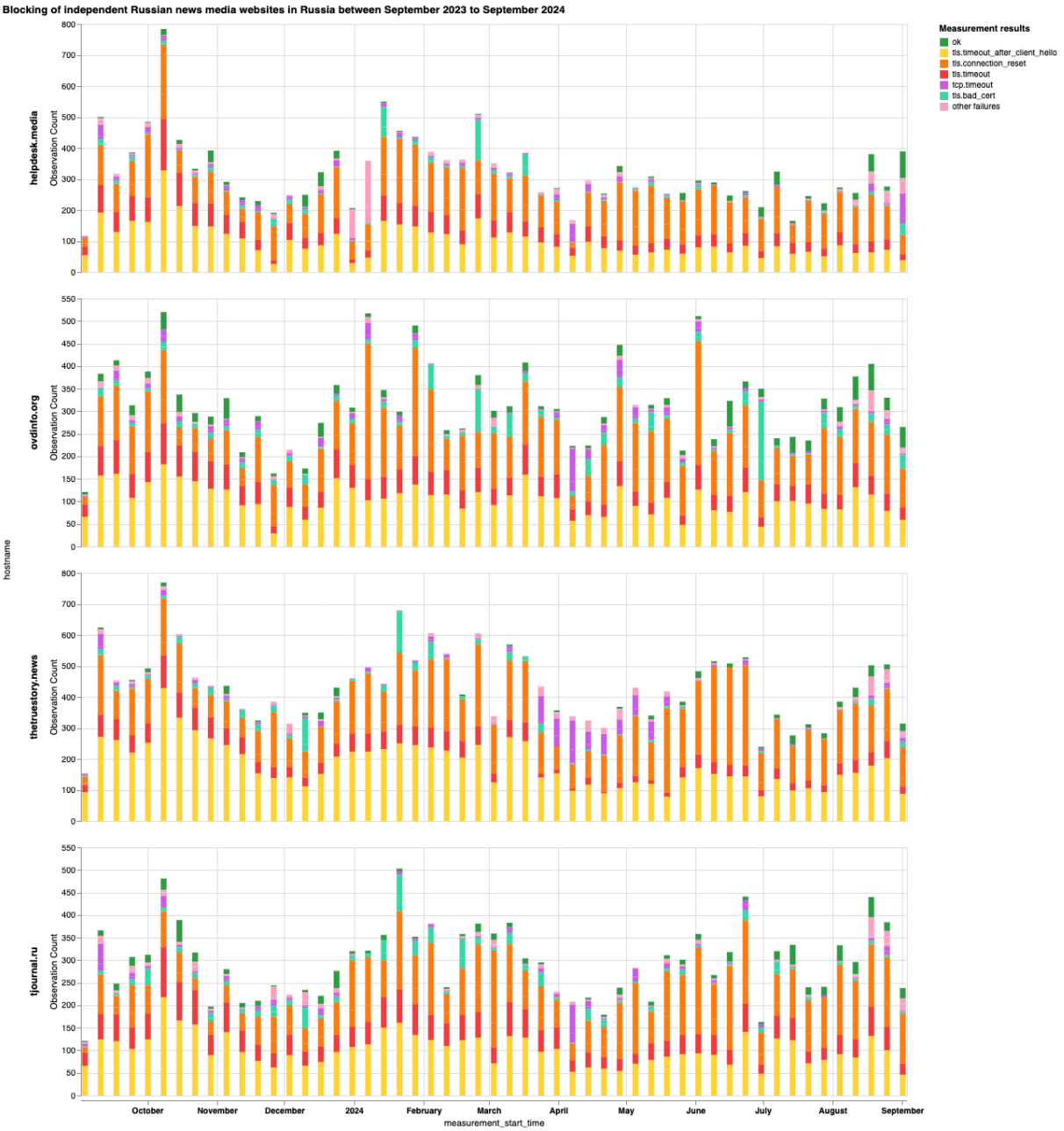

График: Результаты тестирования доменов helpdesk.media, ovdinfo.org, thetruestory.news и tjournal.ru с помощью OONI Probe в нескольких сетях в России в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

График: Результаты тестирования доменов mbk.news, semnasem.org, thebell.io и www.svoboda.org с помощью OONI Probe в нескольких сетях в России в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

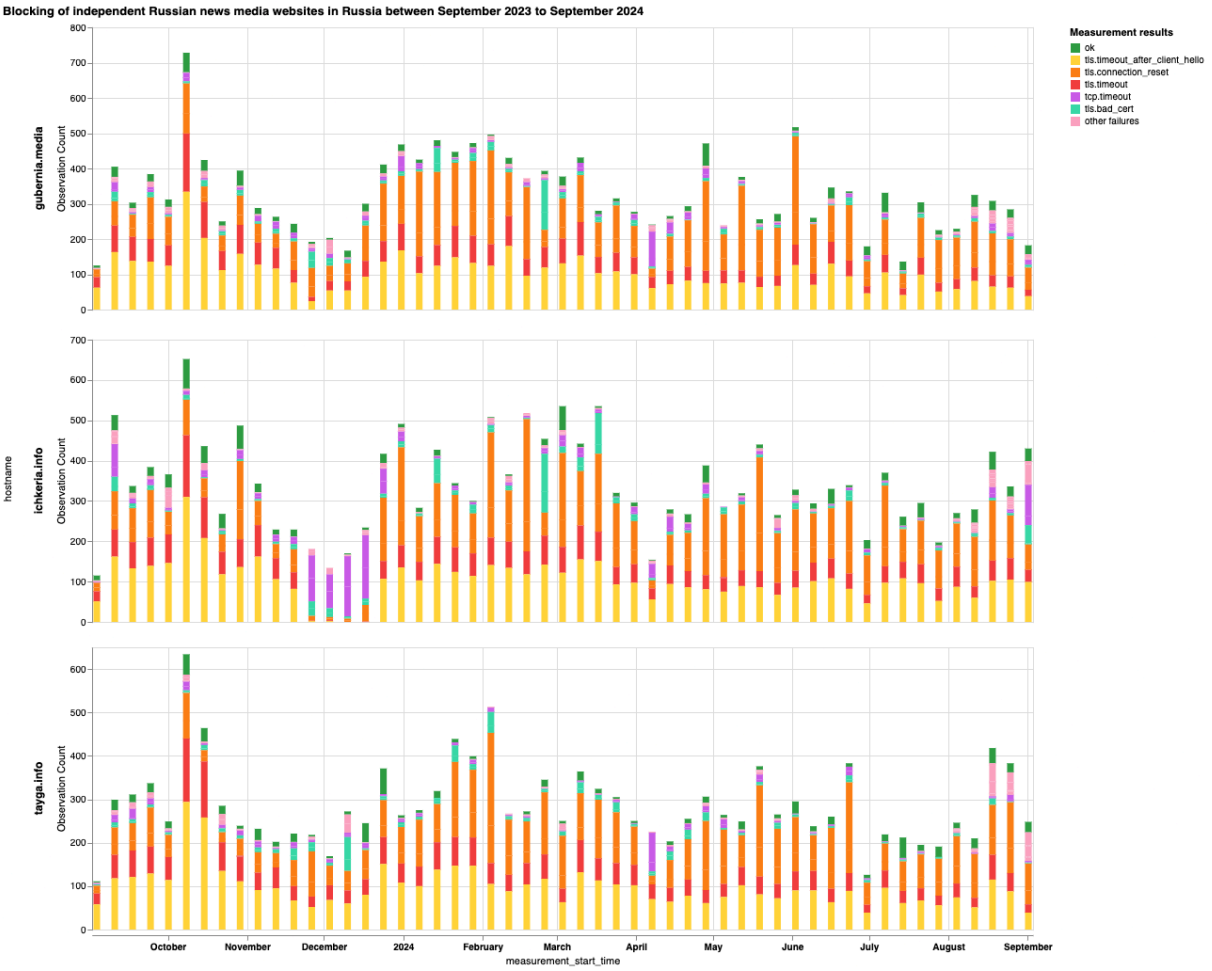

График: Результаты тестирования доменов gubernia.media, ichkeria.info и tayga.info с помощью OONI Probe в нескольких сетях в России в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

График: Результаты тестирования доменов cherta.media, glasnaya.media, skat.media и verstka.media с помощью OONI Probe в нескольких сетях в России в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

Из приведенных выше шести графиков видно, что большинство доменов стабильно тестировались пользователями OONI Probe в России в течение всего анализируемого периода, и лишь несколько доменов (doxa.team и tvrain.tv) начали получать измерения только в течение анализируемого периода. Это важно, так как чем больше измерений мы смогли собрать, тем больше наша уверенность в результатах. Стоит также отметить, что охват измерений, представленный на графиках выше, агрегирован по нескольким сетям в России, что еще больше повышает надежность результатов.

Как видно на графиках, подавляющее большинство попыток подключения к доменам привело к TLS-ошибкам, это является сильным сигналом цензуры на основе TLS. Мы видим такой паттерн при тестировании почти всех доменов, представленных на графиках выше, единственным исключением стал домен glasnaya.media. В отличие от других доменов, тестирование OONI Probe домена glasnaya.media показывает, что он в основном был доступен в протестированных сетях и начал демонстрировать всплеск аномалий только после 6 июля 2024 года. Интересно, что это полностью совпадает с датой (6 июля 2024 года), когда Роскомнадзор добавил glasnaya.media в свой реестр блокировок, что позволяет предположить, что интернет-провайдеры в России немедленно осуществляют блокировку, как только домены добавляются в реестр. После блокировки тестирование glasnaya.media стало показывать признаки вмешательства на основе TLS, как и тестирование всех остальных доменов на приведенных выше графиках.

Для всех 23 медиа, мы наблюдали две основные ошибки, связанные с TLS:

- Отключение сессии после Client Hello во время TLS-рукопожатия (отмечены как tls.timeout_after_client_hello, желтый цвет на графиках)
- Отправка RST-пакета после Client Hello во время TLS-рукопожатия (отмечены как tls.connection_reset, оранжевый цвет на графиках)

Перед тем как соединение TLS становится защищенным и зашифрованным, пользователь отправляет начальное сообщение, называемое «Client Hello», которое не зашифровано. Это (незашифрованное) сообщение включает (помимо прочего) указание имени сервера (Server Name Indication, SNI), которое определяет доменное имя сайта, к которому пользователь пытается получить доступ. Это означает, что цензор видит это незашифрованное сообщение с информацией о сервисе, к которому подключается пользователь, и может прервать соединение еще до того, как оно будет зашифровано. Чтение SNI и блокировка сервисов с использованием информации из этого поля требует использования технологии Deep Packet Inspection (DPI).

Именно это мы наблюдаем в данных OONI для 23 доменов новостных СМИ, представленных на графиках выше. В частности, данные OONI показывают, что в то время как разрешение DNS возвращало согласованные IP-адреса и можно было установить соединение с разрешенными IP-адресами, TLS-соединение сразу же обрывалось. В некоторых случаях данные OONI показывают обрыв TLS-сессии, в других – отправку RST-пакета сразу после Client Hello во время TLS-рукопожатия. Поскольку мы наблюдаем одну и ту же картину в подавляющем большинстве измерений, собранных из нескольких сетей за один и тот же период времени, данные OONI позволяют предположить, что многие интернет-провайдеры в России

блокировали доступ к этим новостным доменам с помощью TLS-вмешательства. Этот метод блокировки также совпадает с предыдущими техниками цензуры, которые мы зафиксировали в России в рамках предыдущих исследований.

Учитывая, что данные OONI показывают, что эти 23 новостных медиа-домена заблокированы почти во всех протестированных сетях в России (при этом некоторые домены, например cherta.media были проверены на более чем 400 сетях в течение анализируемого периода), и что они блокируются одинаково (через TLS-вмешательство), вероятно, что эти блокировки централизованно управляются Роскомнадзором с помощью ТСПУ – системы DPI, которую интернет-провайдеры в России обязаны установить с момента подписания закона «о Суверенном Рунете» в мае 2019 года. Ранее Censored Planet выяснили, что ТСПУ может реагировать на разные типы трафика, например, на траффик, использующий SNI. Это согласуется с тем, что мы наблюдаем в данных OONI, где большинство блокировок, по-видимому, вызвано полем SNI, поскольку мы видим, что TLS-соединение разрывается или сбрасывается сразу после сообщения ClientHello. Таким образом, хотя развертывание ТСПУ децентрализовано (каждый интернет-провайдер обязан установить эти устройства в своей сети), цензура, похоже, управляется централизованно Роскомнадзором. На централизованное управление устройствами ТСПУ Роскомнадзором указывает и документация производителя, в которой указано, что в таком «оборудовании (EcoFilter) реализовано автоматическое обновление и загрузка данных из реестра Роскомнадзора».

О децентрализованном развертывании устройств TSPU говорит и тот факт, что конкретные ошибки TLS отличаются от сети к сети. Это иллюстрирует, например, следующий график тестирования cherta.media на трех сетях с наибольшим охватом измерений OONI в России за анализируемый период.

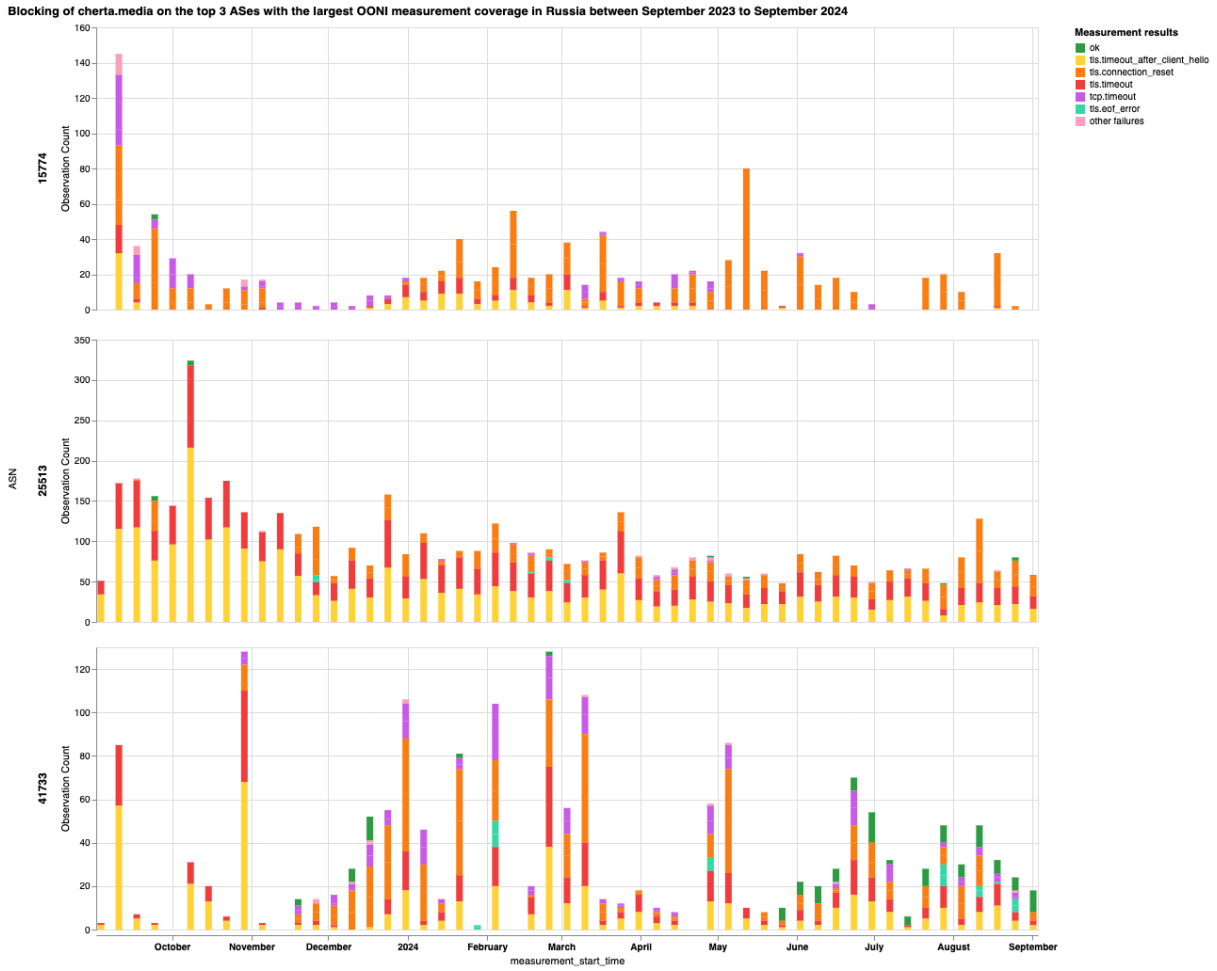

График: Результаты тестирования домена cherta.media с помощью OONI Probe в трех сетях в России с наибольшим количеством измерений в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

Из приведенного выше графика видно, что таймаут TLS-соединения чаще встречается в сети AS25513 по сравнению с AS15774, где чаще встречаются ошибки сброса TLS-соединения. Эта разница нам не совсем понятна, но мы предполагаем, что она может быть связана с различными сценариями реализации блокировки, в которых некоторые провайдеры могут использовать развертывание “on-path” или “in-path”. Например, провайдеры, развертывающие DPI “on-path”, будут вбрасывать RST-пакеты, в то время как провайдеры, развертывающие DPI “in-path”, могут также устанавливать таймаут соединения, поскольку у них есть возможность отбрасывать пакеты.

Что касается блокировок на основе DNS, которые мы можем автоматически обнаружить и подтвердить по существующим отпечаткам (об этом говорилось выше), то эти блокировки, скорее всего, не зависят от ТСПУ-устройств (которые, похоже, не имеют возможности блокировки по DNS). Это подтверждается и тем, что многие блокировки на основе DNS были введены еще до введения требования об использовании устройств ТСПУ.

Гонка медиа-цензуры между Россией и ЕС

Когда в феврале 2022 года в Украине началась полномасштабная война, Россия не была единственной страной, начавшей блокировать сайты новостных медиа.

2 марта 2022 года Совет Европейского союза опубликовал заявление о приостановке вещания Sputnik и Russia Today (RT) на территории ЕС, ссылаясь на стратегию России по дестабилизации соседних стран и ЕС посредством систематической информационной манипуляции и дезинформационной кампании. В ответ многие страны ЕС начали блокировать доступ к Sputnik и Russia Today (RT) – и многие из этих блокировок продолжаются до сих пор. Это первый крупный случай блокировки новостных медиа в ЕС.

На следующем графике представлены европейские страны, в которых в период с 1 июня 2024 года по 1 сентября 2024 года в ходе тестирования OONI Probe сайта Russia Today (www.rt.com) было выявлено наибольшее количество аномалий (признаков блокировки). Во многих из этих стран (таких как Италия, Франция, Германия и Ирландия) блокировка осуществляется с помощью DNS-вмешательства.

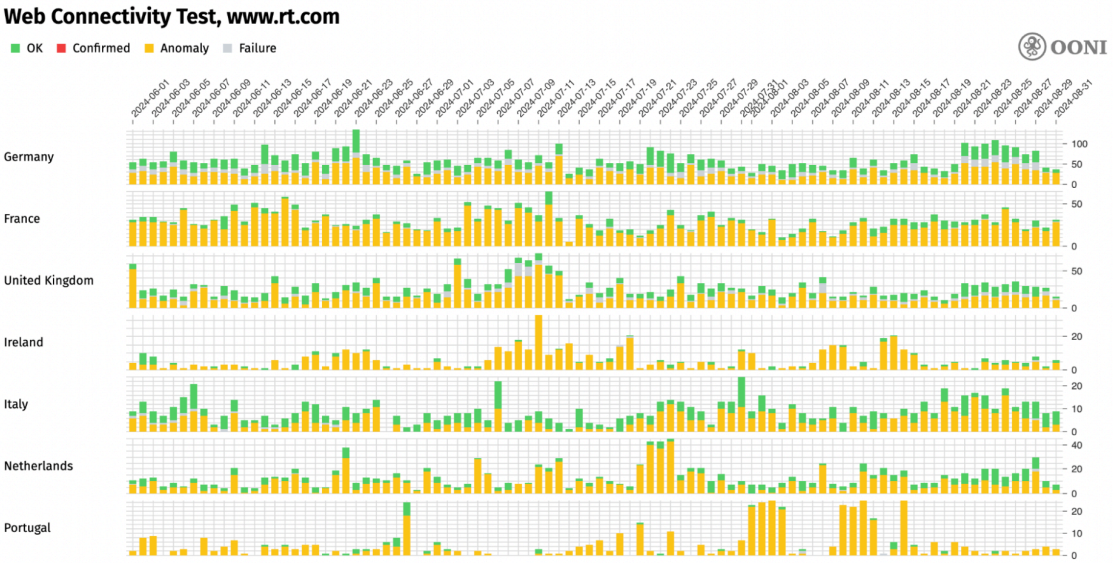

График: Результаты тестирования Russia Today (www.rt.com) с помощью OONI Probe в европейских странах с наибольшим количеством аномальных измерений в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

Точно так же многие европейские страны продолжают блокировать доступ к Sputnik. На следующем графике представлены европейские страны, в которых результаты тестирования сайта sputniknews.com показывает наибольшее количество аномалий в период с 1 июня 2024 года по 1 сентября 2024 года. Эта блокировка также осуществляется с помощью DNS-вмешательства.

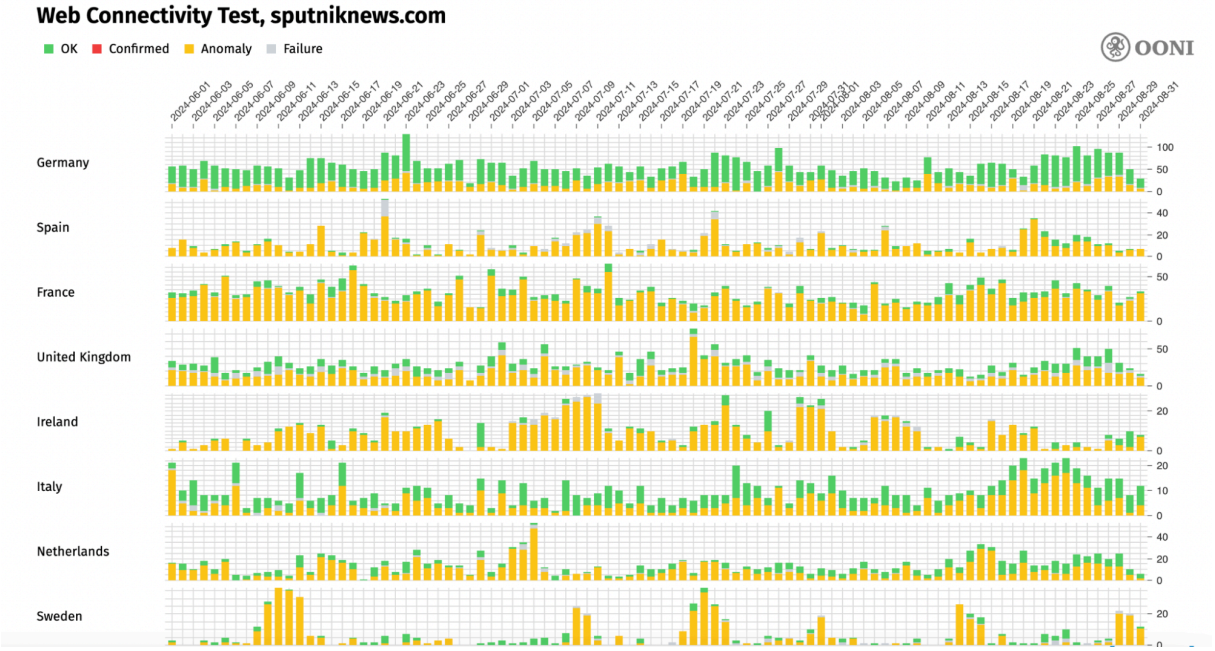

График: Результаты тестирования Sputnik (sputniknews.com) с помощью OONI Probe в европейских странах с наибольшим количеством аномальных измерений в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

Однако с марта 2022 года, когда Совет Европейского Союза объявил о приостановке деятельности вещания Sputnik, Sputnik сменил свой домен на sputnikglobe.com. Сегодня, когда пользователи заходят на сайт sputniknews.com, они перенаправляются на sputnikglobe.com. Сравнивая измерения OONIsputniknews.com (график выше) из тех же европейских стран с измерениями sputnikglobe.com (график ниже), мы видим, что большинство из этих стран не блокируют доступ к новому домену Sputnik.

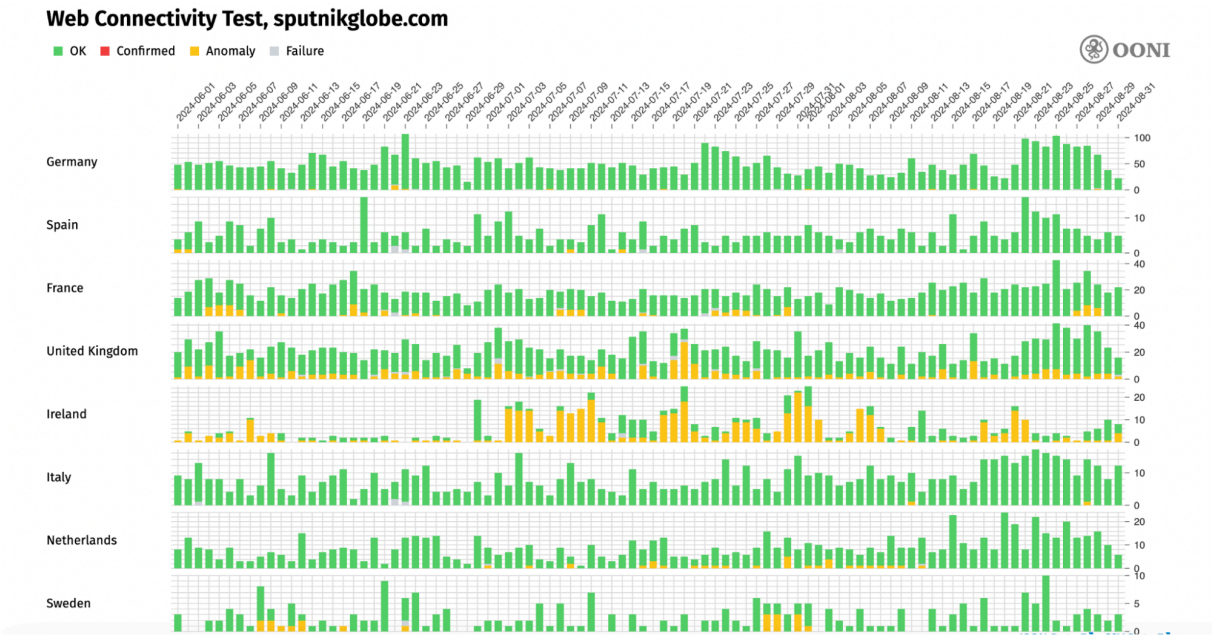

График: Результаты тестирования Sputnik (sputnikglobe.com) с помощью OONI Probe в европейских странах с наибольшим количеством аномальных измерений в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

Сравнение двух приведенных выше графиков позволяет предположить, что доступ к Sputnik в Европе блокируется неэффективно, и что Sputnik смог легко обойти DNS-блокировку в Европе, просто изменив свой домен.

17 мая 2024 года Совет Европейского союза расширил ограничения, приняв решение о приостановке вещания еще 4 связанных с Россией СМИ: Voice of Europe, РИА Новости, «Известия» и «Российская газета». Как и в случае с приостановкой вещания RT и Sputnik, Совет принял это решение для борьбы с российской кампанией дезинформации, которая рассматривается как часть более широкой стратегии по дестабилизации ЕС и увеличению поддержки войны России в Украине.

Из последних 4 запрещенных СМИ в последние месяцы в Европе пользователи OONI Probe тестировали в основном РИА Новости. На следующем графике представлены европейские страны, в которых тестирование OONI Probe РИА Новости (ria.ru) показало наибольшее количество аномалий в период с 1 февраля 2024 года по 1 сентября 2024 года.

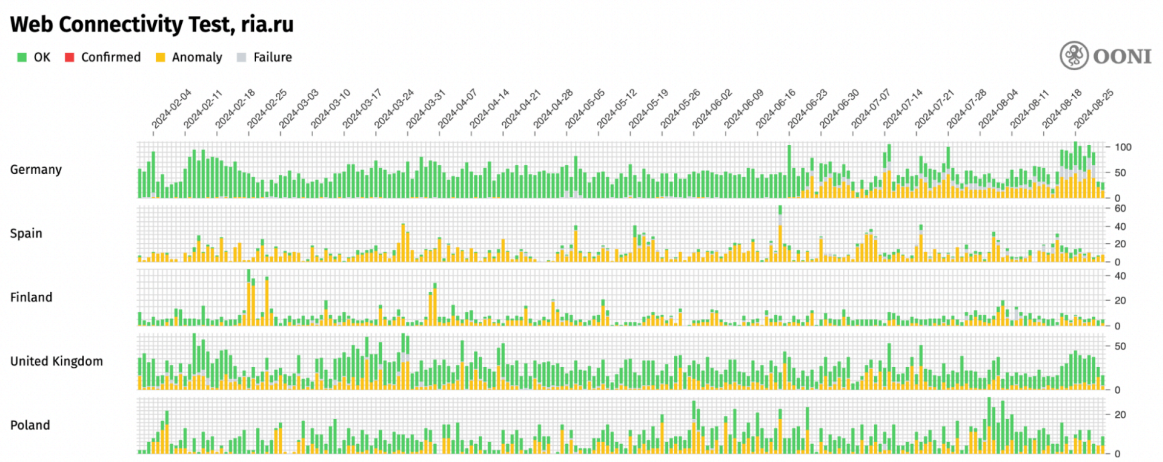

График: Результаты тестирования RIA Novosti (ria.ru) с помощью OONI Probe в европейских странах с наибольшим количеством аномальных измерений в период с 1 сентября 2023 года по 1 сентября 2024 года (источник: данные OONI).

Как видно, сайт ria.ru был недоступен (постоянно присутствуют аномалии) в большинстве европейских стран, показанных на приведенном выше графике, до решения Совета ЕС от 17 мая 2024 года. Из этих стран только Германия начала блокировать доступ к ria.ru после принятия решения, поскольку данные OONI показывают всплеск аномалий с 26 июня 2024 года и далее.

В ответ на решение Совета ЕС, 25 июня 2024 года (в день вступления в силу решения Совета ЕС) Министерство иностранных дел России объявило, что ограничит доступ к 81 СМИ стран-членов ЕС (включая несколько сайтов общеевропейских СМИ) в России. В тот же день мы добавили эти сайты СМИ в список сайтов Citizen Lab для России, чтобы их доступность могли проверить пользователи OONI Probe в России.

На следующем графике представлены обобщенные данные OONI, полученные в результате тестирования некоторых из этих новостных СМИ ЕС в России в период с 1 июня 2024 года по 1 сентября 2024 года.

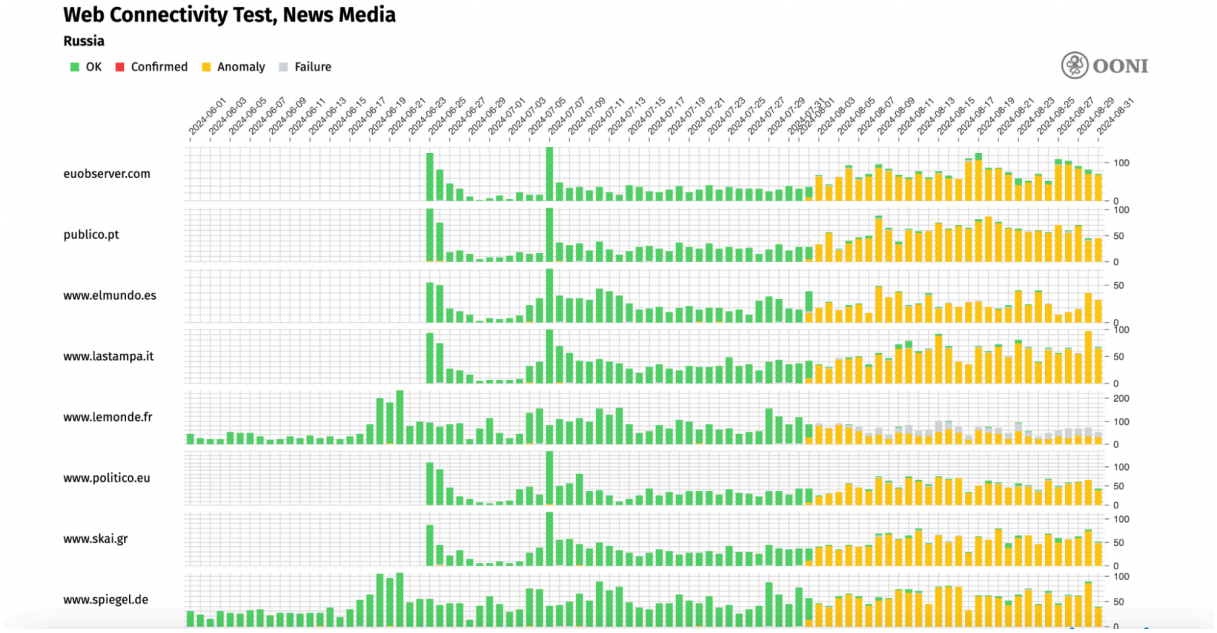

График: Результаты тестирования европейских медиа с помощью OONI Probe в России в период с 1 июня 2024 года по 1 сентября 2024 года (источник: данные OONI).

Как по часам, мы наблюдаем, что доступ ко всем сайтам новостных европейских СМИ (показанным на графике выше) был заблокирован в России 2 августа 2024 года, и остается заблокированным, как минимум, до 1-го сентября. Как и в случае с другими блокировками новостных СМИ, рассмотренными в рамках данного исследования, эти блокировки осуществляются в основном с помощью TLS-вмешательства.

В то время как Россия и ЕС ведут войну, цензурируя СМИ, данные OONI показывают, что Россия применяет блокировки гораздо эффективнее и более сложным методом (который в том числе сложнее обойти). Страны ЕС в основном осуществляли блокировку на уровне DNS, что легко обходится как пользователями Интернета в ЕС (путем смены используемого DNS-регистратора), так и затронутыми российскими СМИ (например, Sputnik сменил домен). В то же время

Россия блокировала доступ к европейским СМИ с помощью TLS-вмешательства, для обхода которых необходимо использовать Tor или VPN-сервисы, распространение информации о которых в России запрещено.

Более того, у России есть большой опыт внедрения цензуры на уровне сети, что означает, что она способна быстро и эффективно осуществлять блокировки (как показано на приведенном выше графике). В ЕС, с другой стороны, каждая отдельная страна должна сама интерпретировать решения Совета ЕС (в которых перечислены только организации, но не их дочерние домены) и решать, какие домены должны быть заблокированы. В результате блокировки осуществляются непоследовательно во разных странах ЕС.

Результаты интервью

Общие выводы

2024 год отметился ожидаемым усилением цензурных ограничений и преследований независимых российских СМИ. Хотя немногие представители медиа указали на появление принципиально новых методов давления, большинство подчеркнули, что работать для российской аудитории становится всё сложнее.

Основные проблемы связаны не столько с самими блокировками, последствия которых многие СМИ смогли преодолеть, сколько с законодательными и административными мерами. Обыски, штрафы, а также присвоение статусов «иностранного агента» и «нежелательной организации» стали ключевыми инструментами контроля и подавления журналистской деятельности. Репрессии затронули как крупные издания, так и региональные медиа. Это привело к усилению самоцензуры в журналистской среде: часть журналистов была вынуждена продолжать работу из-за границы, а некоторые проекты прекратили существование.

Аудитория большинства изданий сегодня распределена между Россией и другими странами, однако из-за широкого использования VPN-сервисов медиа сталкиваются с трудностями при анализе её географического состава.
По косвенным данным, в среднем более 50% аудитории продолжают находиться в России. Несмотря на масштабные блокировки и усиление цензуры, многие медиа отмечают, что значительная часть россиян не использует VPN, ограничиваясь зеркалами или чтением постов в социальных сетях. Оценка трафика на сайты

изданий от пользователей VPN варьируются в пределах 30–40%, а еще часть аудитории продолжает заходить на сайты заблокированных СМИ напрямую (через зеркала или другие средства обхода блокировок предоставляемые самим медиа).

У некоторых медиа наблюдается значительная доля аудитории из числа мигрантов, находящихся за пределами России, которые испытывают серьёзное беспокойство из-за статуса «нежелательной организации», присвоенного изданиям. В таких случаях медиа фиксируют значительный переход читателей с сайтов в Telegram. В целом, многие издания отметили, что блокировка их сайтов, признание медиа «нежелательной организацией» или присвоение статуса «иностранного агента», а также иные общие резонансные новости, приводят к увеличению числа подписчиков в социальных сетях. Отдельного внимания заслуживает тот факт, что российские блокировки затронули не только независимые российские издания, но и ряд кыргызских, таджикских и грузинских медиа. Кроме того, наблюдается рост аудитории из Украины, но определить, из каких именно регионов — оккупированных или других — идет этот трафик, пока затруднительно.

В целом, многие медиа отметили, чтоб блокировка их сайтов и признание их организаций «иностранными агентами», либо «нежелательными организациями» приводит к увеличению числа подписчиков в их социальных сетях (включая телеграм).

Для всех медиа Telegram стал ключевой платформой для публикации в России. Почти все издания активно используют встроенные функции мессенджера, такие как Instant View и сервис сбора пожертвований. Однако многие выражают обеспокоенность безопасностью использования этой платформы так как сих пор неизвестно, имеют ли российские правоохранительные органы доступ к данным о подписках и донатах пользователей. Также вызывает вопросы непрозрачность системы модерации контента в Telegram. Некоторые издания сталкивались с бот-атаками на свои каналы, а процесс верификации (получения галочки) остаётся проблематичным из-за отсутствия оперативного взаимодействия между представителями платформы и владельцами каналов.

Что касается других платформ, у большинства СМИ отмечается снижение активности и падение трафика на Facebook. Это объясняется блокировкой социальной сети в России, теневыми банами и особенностями её модерационной политики. Замедление работы YouTube и его блокировка на отдельных российских сетях, начавшиеся в 2024 году, пока что не привели к значительному снижению охватов и трафика.

На основе интервью, мы выделили основные проблемы, с которыми сталкиваются современные независимые медиа. Они также влияют на способность организаций

противостоять цензуре с точки зрения производства контента, и с точки зрения реализации технических решений для обхода блокировок.

- Финансовые сложности. Финансовая нестабильность является одной из ключевых проблем для независимых СМИ в России. Ограничения на рекламу и партнерства, вызванные правовыми статусами «иноагента» и/или «нежелательной организации», усугубляют эту проблему. Из-за блокировки платежных систем и санкций финансовая поддержка большинства медиа существенно сократилась, и им пришлось перепридумывать свою бизнес-модель. В результате многие СМИ были вынуждены искать альтернативные источники финансирования, такие как краудфандинг или международные гранты, многие медиа до сих пор не нашли устойчивую модель финансирования.

- Недостаток кадров, выгорание и текучка. Иммиграционные проблемы, низкие зарплаты и постоянный стресс приводят к выгоранию среди сотрудников, особенно среди медиаменеджеров. Статусы «иноагента» или «нежелательной организации» приводят к нежеланию многих авторов и респондентов сотрудничать с изданиями, ограничивая возможность медиа освещать события происходящие в России. Независимые СМИ сталкиваются с рядом вызовов, которые включают в себя сложности с поиском авторов, доступом к информации, работой с респондентами, находящимися в России, а также необходимость адаптации к быстро меняющимся условиям цифровой среды. Все это требует от редакций высокой степени гибкости и способности быстро реагировать на новые угрозы.

- Статусы «нежелательной организации», «экстремистов» или «иноагентов». Накладывают ограничения в работе с авторами и респондентами, усложняют поиск и привлечение новых авторов, респондентов и экспертов, поскольку любое сотрудничество с медиа становится рискованным и может привести к уголовной ответственности для участников. Эти статусы также делают невозможным использование платного продвижения через платформы, сервисы и сотрудничество с блогерами, что лишает медиа важного канала для привлечения аудитории. Также это влияет на самоцензуру и уход из профессии отдельных журналистов и закрытие изданий.

В 2024 году список «иностранных агентов» пополнился более чем 102 людьми в персональном качестве и 26 организациями и проектами, из которых треть – журналисты и СМИ. Среди них – «Холод», «BILD на русском, «SOTA», «Republic», интернет-издание «Смола», «T-invariant», правозащитный проект «Первый отдел», телеграм-каналы «ВЧК-ОГПУ» и «Сирена», Газета «Собеседник», ASTRA, «Говорит НеМосква», Незыгарь, BRIEF и др. Реестр «нежелательных организаций» также

пополнился новыми именами журналистов, медиа проектов и СМИ, среди которых «Радио Свобода», Sota Media, The Moscow Times и др. Также продолжилось включение журналистов в список «экстремистов» или «террористов» за отличные от официальной государственной позиции высказывания. За 2024 год некоторые издания были вынуждены закрыться из-за финансовых трудностей и усиления цензуры. Например, закрылись: Якутская газета «Туймаада, экологическое издание «Кедр» (часть команды основала новое издание «Смола»), Радио «Эхо Кавказа», издание “Курьер. Среда”, Astra (вскоре возобновила благодаря поддержке донатчиков и доноров), «Служба поддержки» (закрылась из-за недостаточного финансирования), медиа It’s My City (лишено лицензии из-за освещения антивоенных протестов).

Риски безопасности: Повышенные риски слежки, ограничения в использовании VPN (неудобства, связанные с необходимостью включения и выключения сервиса, поиском стабильно работающего инструмента; невозможность использования VPN из-за вынужденного удаления сервисов с маркетплейса или отсутствия оплаты рублями повышение цензурных требований и др) создают как цифровые, так и юридические риски для сотрудников, работающих с чувствительной информацией. Присутствие на российских платформах стало небезопасным, так как взаимодействие с материалами «нежелательных организаций» легко отслеживается и может привести к уголовному преследованию читателей. Чтобы минимизировать угрозы для аудитории, многие медиа закрыли свои аккаунты на российских платформах и перешли на зарубежные сервисы с усиленной защитой данных. Однако большинство зарубежных сервисов остаются заблокированными в России, и такая смена платформ приводит к потере доступа к российской аудитории.

Системные блокировки, постоянное преследование журналистов, наложение штрафов, а также различные препятствия в распространении материалов независимыми СМИ, создают значительное давление на деятельность независимой прессы в стране и ставят само существование независимых медиа под вопрос. Совокупность этих мер направлена на полную ликвидацию альтернативных источников информации, что в свою очередь угрожает демократическим процессам и свободному выражению мнений. Это также формирует атмосферу страха среди журналистов и авторов, вынуждая их либо покидать страну, либо подвергать себя серьезным рискам.

Методы цензуры

Блокировки и DDoS атаки

В предыдущие годы мы задокументировали блокировку сайтов большинства медиапроектов в России. Как видно из данных OONI за последний год описанных выше, блокировки медиа остаются повсеместными. Однако, большинство медиа продолжали работать с российской аудиторией используя зеркала своих сайтов даже после блокировки своего основного домена.

В 2024 году обходить блокировки с помощью зеркал стало сложнее, многие провайдеры научились автоматизировать блокировку зеркал по мере появления новых ссылок, и у некоторых изданий произошло учащение блокировок вплоть до регулярности раз в несколько минут. В то же время, медиа научились выкатывать новые зеркала с нужной скоростью и, в некоторых случаях, теперь процесс блокировки со стороны провайдеров и реализации нового зеркала со стороны медиа автоматизирован с обеих сторон. Однако остается непонятным, есть ли у всех медиа возможность реализовать и поддерживать такие технические решения как автоматическая реализация новых зеркал, если это будет необходимо, так как этот вопрос напрямую связан с количеством ресурсов издания.

Продолжились и масштабные блокировки сайтов, особенно затрагивающие ресурсы, освещающие протестную активность, правозащитные инициативы и события, антивоенные проекты. Среди заблокированных оказались RusNews и сервис рассылки писем Kit (оба позднее разблокированы), а также такие издания, как «Говорит НеМосква», Sota Project, «Свободные новости», «Полит.ру», «Репортёры без границ», Avtozak LIVE, Compromat.ru, интернет-магазин «Новой газеты» и др.

Помимо блокировок, некоторые издания сталкивались с техническими атаками на свои ресурсы, такими как DDoS-атаки (распределенные атаки отказа в обслуживании). Такие атаки, как правило, направлены на выведение из строя веб-сайтов СМИ, что снижает их доступность для пользователей. Такие атаки могут быть организованы как государственными структурами, так и частными лицами. В зависимости от медиа, и по ответам респондентов во время таких атак, к сайту могли осуществляться сотни тысяч запросов в секунду. В феврале и апреле 2024 года независимое издание Meduza подверглось одним из самых масштабных кибератак за свою историю. Атака включала интенсивные DDoS-атаки, блокирование зеркальных доменов каждые 10-20 минут, попытки взлома аккаунтов

журналистов и разрушения краудфандинговой системы. Хакеры также использовали фишинговые атаки и перегружали журналистов спамом. Атака в апреле 2024 года длилась 48 часов, за это время было осуществлено два миллиарда запросов к сервисам Медузы. В октябре 2024 сайт Новой Газеты Европа также подверглась атаке сравнимого уровня с 12-ю миллионами запросов в минуту.

Большинство медиа, подвергшихся атакам, о которых нам известно, смогли восстановить доступ к своему сайту в течение нескольких часов, однако наша выборка включает только 15 проектов, многие из которых имеют достаточно ресурсов, чтобы противостоять таким атакам.

Блокировки третьих сервисов

Социальные сети и YouTube

После начала полномасштабного военного вторжения в 2022 году, большинство российских медиа начали диверсифицировать платформы для публикации контента. В марте 2022 большинство социальных сетей (Facebook, Instagram, Twitter) оказались заблокированы на большинстве российских сетей. Несмотря на это, многие медиа проекты продолжают использовать Instagram как эффективный канал для работы с аудиторией. Некоторые медиа даже сообщили, что количество их подписчиков в инстаграме растет быстрее, чем на других платформах, которые они использовали на протяжении последних трех лет. Несмотря на блокировку Instagram в России и снижение общего числа пользователей, большинство независимых СМИ продолжают использовать его в качестве одного из основных каналов распространения информации, поскольку их целевая аудитория по-прежнему активна. Напротив, блокировка и ухудшение алгоритмов Facebook негативно сказались на присутствии независимых СМИ на этой платформе, где аудитория и так была относительно небольшой и непопулярной для большинства из них.

После блокировки большей части социальных сетей, даже проекты, которые изначально не занимались видео-контентом, начали использовать YouTube как одну из платформ. С проблемами с доступом к YouTube многие проекты столкнулись еще в начале 2024 года, когда YouTube начал активно внедрять геоблокировку контента по требованию Роскомнадзора. Некоторые медиа и организации также столкнулись с требованиями YouTube удалить видео с платформы.

С июля 2024-го года появились новости о замедлении и блокировке YouTube в России. По последним данным OONI видно, что YouTube в основном доступен на большинстве сетей в России. Пользователи сообщают, что иногда платформа может быть доступна на мобильной сети, но заблокирована на кабельном подключении у одного и того же провайдера. Такую же стратегию озвучивало правительство, объявляя возможную блокировку YouTube.

Медиа, использующие YouTube как основную из платформ для публикации упомянули, что несмотря на сохранение доступа на части сетей, на них так или иначе повлияла блокировка YouTube в России. Это выражается в потенциальном снижении трафика аудитории на 30% процентов (он приходится на долю пользователей, заходящие на ютуб-канал СМИ с домашних устройств и телевизоров), по состоянию на конец 2024 года доля потери трафика у части медиа оценивается в 10%. Гипотеза озвученная медиа, заключается в том, что установить средства обхода блокировок на домашние девайсы (такие как телевизор), намного сложнее, чем на мобильный телефон или компьютер. Поэтому люди, которые привыкли получать доступ к контенту с таких девайсов, оказываются отрезаны от YouTube в случае блокировки сервиса на кабельном интернете.

Респонденты поделились, что найти альтернативную площадку для видео пока не представляется возможным: в российских видеохостингах (VK, Rutube) присутствует повсеместная цензура, Discord блокируется в России с октября 2024, Twitch и Vimeo остаются доступными, но недостаточно популярными у целевой аудитории. Для небольших СМИ, использующих YouTube, негативные последствия блокировки и замедления видеохостинга пока не были ощутимы.

Блокировка CDN и хостинг-провайдеров

В ходе наших интервью с независимыми российскими новостными СМИ респонденты сообщили, что блокировка Content Delivery Networks (CDN) и хостинг-провайдеров в России также повлияла на их работу. В частности, они рассказали, что эти блокировки снижают скорость загрузки контента, увеличивая расходы на инфраструктуру и делая инфраструктуру медиа более уязвимой для кибер-атак, что особенно важно для независимых изданий, работающих под политическим давлением.

2 марта 2020 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. Спустя два года, в мае 2022 года, пользователи в России сообщили о проблемах при попытке

получить доступ к сетям Cloudflare и DigitalOcean через отдельные порты. Пользователи сообщали, что им не удается установить TCP-соединение через порт 443, и все пакеты сбрасываются. Однако через другие порты (не 443), у пользователей получалось успешно установить соединение. Такое поведение наблюдалось во многих кабельных и мобильных сетях, включая принадлежащие «Билайну», «Ростелекому», «Дом.Ru» и другим. TCP-порт 443 используется протоколом HTTPS, наиболее распространенным способом безопасного доступа к веб-сайтам. Поскольку большинство сайтов осуществляют перенаправление с HTTP (порт 80) на HTTPS (порт 443), чтобы перевести соединение пользователя в зашифрованный и безопасный режим, подобная блокировка делает недоступными все сайты, размещенные на DigitalOcean, даже те, которые не попали в правительственные блок-листы.

Данные OONI показывают, что такая схема блокировки длилась с 19 мая 2022 года по 7 июня 2022 года, как показано ниже.

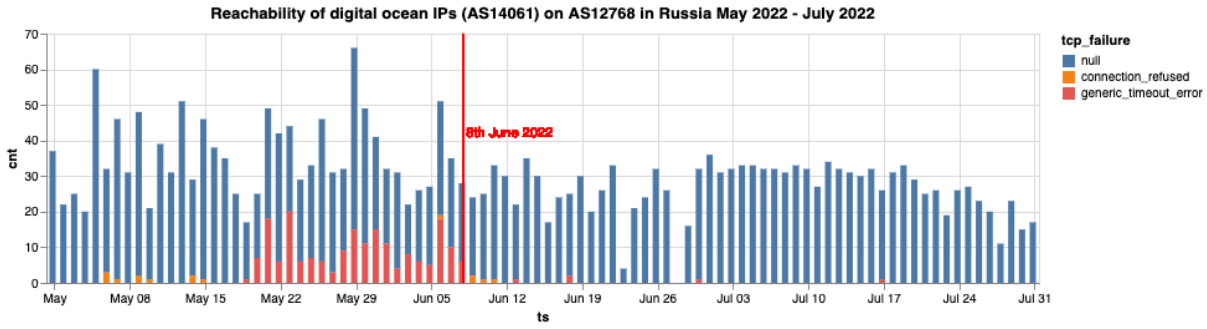

График: Доступность IP-адресов DigitalOcean IPs (AS14061) на сети AS12768 в России с мая по июль 2022 (источник: данные OONI).

В сентябре 2023 года Cloudflare подключил протокол Encrypted Client Hello (ECH) для всех сайтов, использующих их сервера. 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 реализацию цензуры с помощью технологии DPI, которая позволяет просматривать и фильтровать определенные поля в сообщении TLS-рукопожатия ClientHello. В результате этого сайты, размещенные на Cloudflare, которые ранее были недоступны из-за государственной цензуры, оказались доступны внутри страны без использования каких-либо специальных технологий обхода цензуры.

Однако 5 ноября 2024 года пользователи в России сообщили, что Роскомнадзор начал блокировать доступ к ECH на Cloudflare. Использование ECH компанией Cloudflare было названо «нарушением российского законодательства», и цензоры

рекомендовали владельцам российских сайтов отказаться от использования ECH и использовать отечественные CDN-сервисы. Это решение Службы национальной безопасности России, как сообщается, привело к потере доступа из России к сотням тысяч сайтов, в том числе к сайтам, не имеющим отношения к политике: от форумов поклонников аниме до Якутской государственной сельскохозяйственной академии.

Сообщается, что подсети многих хостинг-провайдеров также стали недоступны в России в ноябре 2024 года. Впервые о проблеме стало известно в апреле 2024 года (когда Роскомнадзор заблокировал сайты хостинг-провайдеров, не выполнивших требования закона о приземлении) и в июле 2024 года, когда 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, стали временно недоступны. С ноября 2024 года пользователи стали сообщать о проблемах с сайтами, размещенными на хостингах Greenhost, Cloudflare, Hetzner, OVH, Aeza и других. Скорее всего, это результат блокировки VPN, так как многие VPN имеют подсети IP-адресов у этих хостинг-провайдеров.

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, как показано ниже.

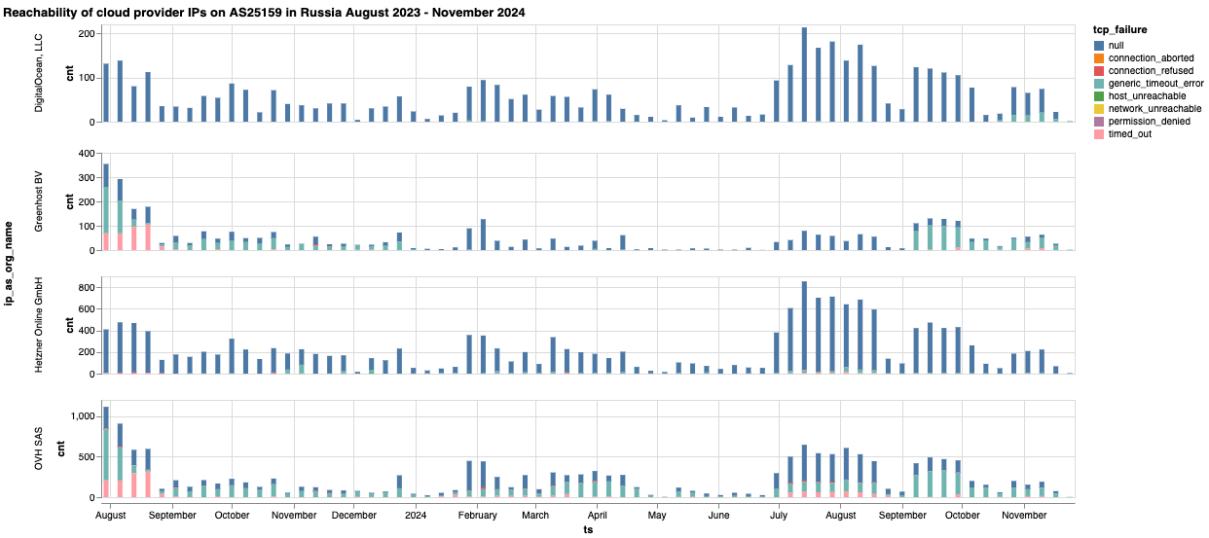

График: Доступность IP-адресов облачных провайдеров на сети AS12768 в России с августа 2023 по ноябрь 2024 (источник: данные OONI).

В частности, на приведенном выше графике показан всплеск таймаут-ошибок при попытках подключения к IP-адресам Greenhost в начале сентября 2024 года, а также всплеск таймаут-ошибок при попытках подключения к IP-адресам

DigitalOcean с начала октября 2024 года. С другой стороны, OVH, похоже, испытывает проблемы с доступностью на этой конкретной сети как минимум с августа 2023 года.

Блокировка VPN-сервисов

Борьба с VPN, анонимайзерами и другими сервисами по обходу блокировок началась еще с 2016 года. В 2020 году РКН обязал интернет-операторов устанавливать ТСПУ в рамках закона о «суверенном интернете». Комплекс устройств позволяет ведомству определять трафик VPN с помощью DPI. Российские ТСПУ позволяют определять разные виды трафика, включая фильтрацию отдельных SNI-полей и трафика QUIC. В 2022 году российские пользователи из разных регионов начали сообщать о блокировке трафика отдельных VPN-протоколов.

В 2023 и 2024 годах ТСПУ продолжили применять для блокировки отдельных VPN-протоколов. Эти блокировки происходили скоординированно в одно и то же время у разных провайдерах в разных регионах, однако все блокировки оставались временными, чтобы избежать урона сторонним сервисам (часть протоколов, используемых VPN-сервисами, задействована в работе, например, банкоматов).

В январе 2023 года жители восточных регионов России (Алтайского края, а также Бийска, Новосибирска и Омска) на время потеряли возможность использовать протоколы OpenVPN и IKeV2, в то время как IP-адреса самих VPN-сервисов оставались доступными. В феврале 2023 блокировки продолжились в других регионах: Перми, Орске, Новочеркасске, Тольятти, Якутске, Казани, Елабуге, Уфе, Чебоксарах и Нижнем Новгороде. В мае 2023 наряду с OpenVPN, IKEv2 и IPvSec начал блокироваться протокол Wireguard, и география расширилась до Москвы и крупнейших интернет-провайдеров, таких как Билайн и МТС. Эта волна временных VPN-блокировок продолжалась до начала августа 2023, только чтобы завершиться и начаться снова в сентябре 2023.

В середине сентября 2023, масштаб VPN-блокировок продолжил увеличиваться, и уже к концу месяца Wireguard и OpenVPN перестали работать для многих пользователей, у большинства после пика блокировок работа протоколов не восстановилась в течение нескольких недель. Роскомсвобода опубликовала большой отчет о блокировке популярных VPN в России в 2023 году: VPN в России: от блокировки сервисов к блокировке протоколов.

В 2024 году блокировки VPN продолжились, но продолжали колебаться: разные сервисы оставались доступными в разных регионах России в разные даты. Пока

сложно оценить реальный масштаб блокировок VPN в России и проанализировать методы этих блокировок. Несколько сообществ, таких как DPI Detector и ntc.party, стараются отслеживать и документировать развитие цензуры средств по обходу блокировок в России, и мы призываем исследователей продолжить работу над изучением состояния цензуры VPN в России.

За последний год стратегия РКН в отношении блокировок протоколов VPN не изменилась, ведомство по-прежнему делает это через ТСПУ. Но существенно снизилось правовое поле критерий блокировок информации в интернете, фактически запрещая публикации о средствах обхода блокировок.

С 1 марта 2024 года вступил в силу запрет на публикации «информации о способах обхода установленных в России блокировок ресурсов», под который подпадают и VPN-сервисы, а также Tor, анонимайзеры и т.п. Блокировка подобной информации реализуется на основании разработанных критериев, VPN нельзя рекламировать в качестве инструмента обхода блокировок (запрета на рекламу VPN в иных качествах нет). Официальная позиция ведомства заключается в необходимости обеспечения цифрового суверенитета и защиты от неправомерного использования технологий.

В ходе ручного мониторинга реестра запрещенных сайтов Роскомсвободы с марта по август было зафиксировано более 500 сайтов и ссылок, заблокированных за распространение информации о средствах обхода блокировок. Как правило, под блокировку попадают ссылки с советами, какой VPN лучше выбрать, а также инструкции по установке таких инструментов. В этом чёрном списке оказались также сайты VPN-сервисов, прокси и плагинов (например, Amnezia VPN, VPNpay, PrivateInternetAccess, VPN Generator, ExpressVPN, Censor Tracker и др.), рейтинги VPN (например, VPNLove) и ресурсы, осуществляющие мониторинг доступности VPN (например, антицензурный форум NTC party, OONI Explorer, DPIdetector). В реестр не попадают страницы сайтов, которые были удалены или скрыты владельцами ресурсов по запросу сервисов, например, хабр ограничиваются геоблокировками, то есть, страница с запрещенной информацией остается на ресурсе, но не доступна пользователям из России. Известно применение геоблокировок и среди VPN-сервисов: Tailscale в октябре установил ее для пользователей из России. Теперь при попытке залогиниться появляется надпись «Сервис недоступен по юридическим причинам». Требования на удаление информации о VPN получал в том числе Youtube, который направил, например, Роскомсвободе запрос на удаление ролика о VPN.

В случае отказа удалять информацию о VPN у владельцев сайтов возникает риск блокировки или штрафа до 4 млн руб. Ограничения распространяются на любые веб-ресурсы: онлайн-платформы, медиа, агрегаторы, соцсети.

Изначально, подобный запрет не относился к научной, научно-технической и статистической информации о способах обхода блокировок. Но с 30 ноября 2024 года вступил в силу запрет и на нее, новые правила будут действовать до 1 сентября 2029 года, и они уже вызвали вопросы со стороны российского научного сообщества и правозащитников. Согласно свежему приказу Роскомнадзора, блокировке подлежит: «Научная, научно-техническая и статистическая информация о способах и методах обмена данными в сети Интернет с использованием защищенных каналов связи».

Возможные последствия для научного сообщества России:

1. Ограничение доступа к научным ресурсам. Запрет может негативно повлиять на научные и исследовательские публикации в области кибербезопасности, сетевых технологий и криптографии. Блокировки, осуществляемые Роскомнадзором, редко бывают избирательными. Как следствие, ресурсы, обсуждающие широкий спектр вопросов, включая методы защиты информации, могут попасть под санкции.

2. Цензура криптографических исследований. Статьи, посвящённые технологиям шифрования, могут оказаться под угрозой блокировки, даже если они не связаны напрямую с обходом ограничений. Это может замедлить развитие фундаментальных исследований в области информационной безопасности.

3. Риск самоцензуры. Учёные и инженеры могут начать избегать определённых тем исследований, чтобы не быть обвинёнными в нарушении законодательства. Это приведёт к снижению качества и объёма исследований в критически важных областях.

Правовое давление

Штрафы и административные взыскания

Штрафы создают значительную финансовую нагрузку для независимых российских СМИ, что мешает их работе и существованию. Основания для штрафов самые разные: от отсутствия на публикациях пометки «иностранный агент» до штрафов за публикации, «дискредитирующие» армию. Только в 2024 году российским СМИ пришлось заплатить не менее 1 265 000 рублей штрафов за свою журналистскую деятельность. А с начала 2024 года «иностранных агентов» оштрафовали на более чем 12 млн рублей за отсутствие маркировки материалов, общая же сумма таких штрафов достигла 1 млрд рублей.

Обыски

Преследование журналистов и редакций сопровождается систематическими обысками и изъятием техники, приводя к самоцензуре и угрозам личной безопасности журналистов. За последние годы многие журналисты в России были арестованы за свою работу. Наиболее известные инциденты:

- Вячеслав Ященко (Кавказский узел) — обыск по делу о фейках о российской армии, Волгоград.
- Дмитрий Фоминцев (Точка Ньюс) — обыск из-за материалов о митрополите Екатеринбургском Евгении Кульберге, Екатеринбург.
- Александр Скворцов (Ижевский вестник) — угрозы, спам-атаки, нападение; обыски у родственников сотрудников.
- Редакция Фонтанки — обыск по делу об уклонении от обязанностей «иноагента», Санкт-Петербург.
- Редакция Арктического обозревателя — изъятие техники по подозрению в сборе государственных тайн.
- Редакция газеты Новости Режа и главный редактор Ольга Романчева — обыски в рамках дела о клевете на прокурора.

Задержания и аресты

В 2024 году в России было арестовано и задержано множество журналистов, особенно тех, кто освещал акции протеста и мобилизационные мероприятия. Задержания лишают журналистов возможности освещать протестные темы,

заставляя их выбирать менее рискованные темы. Вот некоторые из известных случаев:

- 30 журналистов из различных СМИ — задержаны за освещение акции матерей и жен мобилизованных «Путь домой» в Москве.
- Ксения Старикова (RusNews) — задержана за съемки погрома мемориала Алексея Навального в Челябинске.
- Рустем Османов (Крымская солидарность) — отправлен в СИЗО по делу о террористической организации.
- Антонина Фаворская (SOTAvision)— дважды арестована: сначала на 10 суток за посещение могилы Навального, затем помещена в СИЗО по делу о сотрудничестве с экстремистской организацией.
- Сергей Мингазов (Forbes) — задержан по делу о фейках об армии.
- Дмитрий Богмут — арестован за репост репортажа Deutsche Welle.
- Надежда Кеворкова — арестована по обвинению в оправдании терроризма.

Уголовные обвинения

Журналистам и активистам грозят новые уголовные и административные обвинения за высказывания и публикации, среди них:

- Екатерина Фомина (экс-сотрудница «Важных историй») — уголовное дело за распространение фейков о российской армии.
- Мария Пономаренко — приговорена к 6 годам колонии за публикации о событиях в Украине.
- Михаил Зыгарь — заочно арестован и приговорён к 8,5 годам за посты о событиях в Буче.
- Эван Гершкович (корреспондент WSJ) — осуждён на 16 лет за шпионаж.
- Татьяна Лазарева — заочный арест за оправдание терроризма.
- Дмитрий Колезев — заочно арестован по делу о военных фейках.
- Светлана Прокопьева — объявлена в розыск после обвинений в дискредитации армии.
- Наталья Баранова – также объявлена в розыск по уголовному делу.

- Ника Новак – приговорена к 4 годам колонии за сотрудничество с иностранной организацией

Другие события

- Ася Казанцева — научная журналистка уехала из России после того, как была отменена серия её лекций, а её домашний адрес был опубликован депутатом Госдумы.
- Мария Пономаренко — объявила голодовку в ШИЗО в знак протеста против условий содержания.
- Марина Юдкевич — умерла, её лечение задерживалось из-за обыска и изъятия документов.

Ограничения Big Tech и влияние санкций

В рамках интервью многие СМИ отметили, что крупные корпорации (Meta, Google, Telegram, Apple и др.) в лучшем случае занимают нейтральную позицию по отношению к цензуре: они не оказывают помощи независимым российским медиа, но и не инициируют блокировки или удаления контента без конкретного запроса от российских регуляторов. В то же время российские платформы (VK, Яндекс, Rutube) подвергаются самой радикальной цензуре — от удаления каналов и отдельных материалов медиа до подавления SEO независимых медийных сайтов и полного исключения таких сайтов из поисковой выдачи Яндекса.

Самыми «нейтральными» платформами, по мнению респондентов, оказались Meta и Telegram. Несмотря на то, что они не помогали независимым российским медиа продвигать их публикации, они, по крайней мере, не блокировали контент и/или каналы по запросам Роскомнадзора и других российских органов. Основные сложности, связанные с публикацией на этих платформах, касались непрозрачной системы модерации, теневые баны, бот-атак и проверки официальных аккаунтов медиа. Представители медиа, которым удалось восстановить аккаунты после взломов или вернуть публикации после бот-атак, отметили, что без личных связей внутри компаний это было бы невозможно.

Препятствия для сбора донатов и оплаты сервисов

Некоторые сервисы усложнили независимым российским медиа сбор средств, создавая дополнительные юридические и технические барьеры.

Например, в начале октября 2024 года крупнейший иностранный платежный сервис Stripe лишил издание «The Bell» возможности получать доход от платных подписок, так как посчитал его «краудфандинговой платформой». Платежи через этот сервис составляли 30% финансирования издания. После общественной кампании в поддержку «The Bell» удалось возобновить сбор пожертвований через Stripe.

В июле 2024 года Boosty заблокировал сбор пожертвований для издания «Дискурс» по запросу Роскомнадзора без объяснения причин. В августе 2024 года сервис CloudPayments (принадлежащий Тинькофф Банку) отключил возможность сбора пожертвований для издания «Такие дела», что поставило его на грань закрытия. Причины этого решения остались неизвестными. Ранее издание существовало благодаря пожертвованиям, собирая около 1,2 млн рублей (~12 000 долларов США) ежемесячно.

Уход других технологических компаний и отказ работать с российскими организациями, включая независимые медиа, вынудил многие редакции перестраивать свою работу и искать альтернативные инструменты. Иногда это приводило к потере доступа к архивам их предыдущих работ, облачным хранилищам и истории переписок.

Количество доступных рекламных источников дохода также сократилось. После блокировок, повлекших за собой снижение трафика на основных сайтах, а также присвоения статусов «иностранного агента» или «нежелательной организации», многие независимые российские медиа больше не могли продавать рекламу на своих ресурсах. Кроме того, Google отключил рекламу и все платные сервисы в России (например, рекламу на YouTube, AdSense, GSuite, платные приложения, дополнительное хранилище для почты и т. д.). Это привело к тому, что российские медиа с основной аудиторией в России, собирающие миллионы просмотров на YouTube, не могут монетизировать этот трафик и теряют до 60% потенциального дохода с платформы. Facebook и Instagram также отключили рекламные услуги в России, что, с одной стороны, усложнило распространение контента на платформах Meta, так как медиа не могут использовать платное продвижение для охвата российской аудитории, а с другой стороны, лишило независимые медиа еще одного источника дохода.

Big Tech помогает цензорам: удаление мобильных приложений и контента

Google и Apple неоднократно замечены в удалении контента по запросам российских государственных органов, а также в отказе поддерживать независимые российские проекты. Например, с 20 мая 2024 года YouTube начал блокировать

«оппозиционный» контент по запросам Российской Федерации, что вызвало кампании в поддержку пересмотра таких блокировок с точки зрения прав человека.

В сентябре 2024 года проект GreatFire опубликовал исследование, согласно которому Apple тайно удалила 98 VPN-приложений для российских пользователей (из которых только 25 были официально сообщены) по запросу Роскомнадзора. К ноябрю 2024 года этот список расширился до более чем 102 приложений, включая популярные и эффективные инструменты обхода блокировок, такие как Amnezia VPN, Red Shield VPN, ExpressVPN, Nord VPN, Proton VPN и другие.

В октябре и ноябре 2024 года из AppStore были удалены первые приложения медиа — «Свобода» с контентом Русской службы Радио Свобода и ее проектов Сибирь.Реалии и Север.Реалии, приложение Кыргызской службы Радио Свобода, приложение «Настоящее Время» — по запросу Роскомнадзора. Кроме того, Apple скрыла подкасты «The Insider» и «Эхо Москвы», а также новостное шоу BBC Russian Service «Что это было?» для российских пользователей. Компания также потребовала удаления независимого подкаста «Привет, ты иностранный агент» с платформы Apple Podcasts.

Браузер Opera удалил расширение Censor Tracker из своего онлайн-магазина по запросу Роскомнадзора. Ранее Censor Tracker и несколько других расширений для обхода цензуры пропали для российских пользователей из магазина браузера Firefox от Mozilla из-за региональных блокировок. После привлечения общественного внимания к проблеме Mozilla восстановила доступ к сервису. Однако 5 ноября 2024 года стало известно, что компания была оштрафована на 3,5 млн рублей (34 156 долларов США) за отказ удалить Censor Tracker и другие расширения.

На подобные процессы все еще можно повлиять с помощью международных институтов, правозащитных организаций и общественных кампаний. Например, 8 января 2024 года Европейская комиссия призвала Google и Meta содействовать продвижению независимых медиа в России и Беларуси, улучшив их поисковые алгоритмы, которые иногда исключают заблокированные сайты. Представители гражданского общества призвали YouTube и Google оценивать все запросы на блокировку в соответствии с международными стандартами прав человека.

Заключение

Во время военных конфликтов свобода прессы важна как никогда. Публикация своевременной и проверенной информации необходима для защиты гражданского населения и повышения международной осведомленности о реальной ситуации на территории конфликта. Однако на фоне продолжающейся войны в Украине цензура в российских СМИ остается широко распространенной.

Наш анализ данных OONI и интервью с 15 независимыми российскими СМИ свидетельствуют о том, что за последний год цензура в России усилилась. Это привело к увеличению финансовых сложностей и проблем с безопасностью, которые влияют на способность журналистов публиковать материалы для российской аудитории.

Проанализировав данные OONI, собранные в России с 1 сентября 2023 года по 1 сентября 2024 года, мы смогли автоматически подтвердить блокировку 279 доменов новостных СМИ по отпечаткам (это вдвое больше, чем в предыдущем исследовании, в 2023 году мы подтвердили блокировку лишь 139 доменов). Эти заблокированные домены включают как иностранные, так и независимые российские новостные сайты, причем большинство из них заблокированы более чем на 10 различных сетях в России. В таких случаях интернет-провайдеры, по-видимому, осуществляют блокировку на основе DNS децентрализованным способом (например, возвращая 188.186.146.208 как часть DNS-разрешения).

Большинство блокировок осуществляются с помощью TLS-вмешательства, это основная технология блокировок, наблюдаемая в данных OONI собранных из России. В некоторых случаях данные OONI показывают обрыв TLS-сессии, в других – вброс RST-пакета сразу после сообщения ClientHello во время TLS-рукопожатия. Для осуществления подобной выборочной фильтрации на уровне сети обычно требуется использование технологии Deep Packet Inspection (DPI). Поскольку мы наблюдаем одну и ту же картину TLS-вмешательства в подавляющем большинстве измерений, собранных из множества сетей за один и тот же период времени, данные OONI позволяют предположить, что эти блокировки новостных СМИ, скорее всего, централизованно управляются Роскомнадзором с помощью ТСПУ (системы DPI, которую в последние годы обязаны устанавливать интернет-провайдеры в России).

Хотя установка ТСПУ децентрализована (каждый интернет-провайдер должен установить эти устройства в своей сети самостоятельно), блокировки, по-видимому, централизованно управляются Роскомнадзором. Данные OONI показывают, что одни и те же сайты новостных СМИ были заблокированы в одно и то же время в большинстве сетей. Блокировке подвергаются сайты крупнейших независимых российских СМИ (таких как meduza.io, doxa.team, zona.media и tvrain.tv), а также сайты небольших региональных независимых российских новостных изданий (таких как gubernia.media и ichkeria.info).

В ходе интервью с представителями 15 независимых российских медиа нам удалось получить общее представление о том, какое влияние эти блокировки оказали на свободу прессы в России. По словам наших собеседников, давление на независимые СМИ в России значительно усилилось в 2024 году, были введены новые законы о цензуре, заблокированы другие платформы, на которые медиаорганизации полагались для публикации своих материалов (например, YouTube). Методы цензуры становятся все более сложными, некоторые медиа отметили, что провайдеры научились реализовывать автоматическую блокировку зеркал и VPN-протоколов, стали больше использовать технологии Deep Packet Inspection (DPI), геоблокировки, ограничивать доступ к CDN и хостингам. Российские власти объявили, что планируют увеличить эффективность блокировки VPN до 96% к 2030 году.

Финансовые трудности, вызванные отсутствием рекламного дохода, усугубляются правовым давлением через статусы «иностранного агента», «нежелательной организации» или «экстремиста». Эти статусы не только ограничивают возможности для продвижения контента и сотрудничества с авторами и источниками, но и усиливают репрессии против журналистов, создавая атмосферу страха, которая приводит к закрытию редакций или эмиграции сотрудников. Дополнительно ситуацию осложняет готовность технологических компаний, таких как Google и Apple, выполнять требования Роскомнадзора, что ограничивает количество доступных для публикации площадок еще больше, и затрудняет доступ российских пользователей к независимому контенту.

Одним из положительных эффектов усиленной цензуры в России стало увеличение числа пользователей VPN-сервисов, что свидетельствует о стремлении граждан защитить свою конфиденциальность и обходить блокировки. Однако многие медиа отметили, что далеко не все россияне используют средства по обходу блокировок. Ключевой задачей также остаётся образовательная работа по грамотному использованию технологий обхода цензуры. Независимые СМИ и правозащитные организации продолжают призывать технологические компании к большей прозрачности и соблюдению прав человека.

Отвечая на задачи исследования, можно сделать следующие выводы:

1. **Цифровые стратегии независимых СМИ в условиях** повсеместной цензуры.

    - **Адаптация и гибкость.** Независимые медиа демонстрируют высокий уровень адаптации, используя зеркала, VPN и альтернативные платформы (например, Telegram) для обхода блокировок. Однако эффективное поддержание технических решений требует значительных ресурсов, что не всегда доступно для всех изданий.

    - **Диверсификация каналов.** Многие СМИ активно используют все возможные платформы (YouTube, Telegram), несмотря на их блокировку или замедление. Это помогает сохранять доступ к аудитории внутри России и за ее пределами.

    - **Солидаризация между разными медиа-проектами.** На протяжении последних трех лет, медиа проекты разного размера и формата стали больше сотрудничать друг с другом, делиться решениями и предупреждать о новых технологиях, применяемых цензором. Этот процесс очень позитивно сказывается на том, насколько эффективно медиа разного формата и масштаба научились обходить российскую цензуру.

2. **Влияние BigTech на доступ к независимой информации.**

    - **Нейтральная позиция платформ.** Крупные компании, такие как Meta и Google, занимают нейтральную позицию, не оказывая поддержки независимым СМИ, но и не блокируя контент по собственной инициативе. Однако они часто удаляют материалы или приложения по требованию российских властей, что ставит под угрозу доступ к информации.

    - **Проблемы с модерацией и безопасностью.** Непрозрачность модерации контента на платформах (особенно Telegram) вызывает беспокойство среди медиа. В связи с тем, что Telegram стал одной из основных платформ для публикации в России, многие проекты озвучили опасения относительно доступа российских властей к данным пользователей на этой платформе.

3. **Влияние санкций и блокировок.**

    - **Ограничение инструментов для сбора средств.** Усложнение работы с зарубежными платежными системами (например, блокировка Stripe) и удаление контента и приложений (например, VPN) препятствуют устойчивому функционированию медиа.

- **Обучаемость цензоров.** За последние три года российские провайдеры научились автоматизировать блокировки сайтов и зеркал, научились блокировать некоторые из VPN-протоколов. Большинство медиа рассматривают борьбу с цензурой как непрекращающуюся гонку, в которой на стороне цензора намного больше ресурсов.

- **Проблемы с доступом и инфраструктурой**. Блокировки CDN и хостинг-провайдеров приводят к снижению доступности контента и росту затрат на инфраструктуру. Это особенно критично для СМИ, работающих в условиях политического давления.

- **Международная поддержка.** Международное давление на BigTech-компании и правозащитные инициативы остаются важными для защиты прав независимых медиа. Однако влияние этих усилий ограничено, и необходимость международной поддержки остается актуальной.

4. **Влияния статуса «иностранного агента» и «нежелательной организации».**

    - **Финансовые проблемы**. Ограничения на рекламу и платежи из-за статусов «иноагента» и «нежелательной организации» привели к поиску новых моделей финансирования (краудфандинг, международные гранты).

    - **Сложности с кадрами и безопасность сотрудников**. Наличие любого из статусов повышает риски безопасности для сотрудников, читателей и источников, что приводит к выгоранию, понижению эффективности редакций, ограниченному доступу к источникам и ограниченной виральности опубликованных материалов.

Тем временем цензурная борьба между Россией и ЕС, начавшаяся в начале 2022 года после полномасштабного вторжения на Украину, в последние месяцы усилилась. В ответ на решение Совета Европейского союза от 2022 года многие страны ЕС начали блокировать доступ к Sputnik и Russia Today (RT) – и эти блокировки продолжаются до сих пор. Это стало первым крупным случаем блокировки новостных СМИ в ЕС. 17 мая 2024 года Совет Европейского союза расширил ограничения, приняв решение о приостановке вещания еще 4 связанных с Россией СМИ: Голос Европы, РИА Новости, Известия и Российская газета. Как и в случае с приостановкой вещания RT и Sputnik, Совет Европы принял это решение для борьбы с российской пропагандой, которая, по его мнению, является частью более широкой стратегии по дестабилизации ЕС и увеличению поддержки войны России в Украине.

В ответ на решение Совета Европы, Министерство иностранных дел России 25 июня 2024 года (в день вступления в силу решения Совета Европы) объявило

об ограничении доступа к 81 СМИ стран-членов ЕС (включая несколько сайтов общеевропейских СМИ) на территории России. По данным OONI, доступ к сайтам этих новостных СМИ ЕС был заблокирован в России 2 августа 2024 года – и блокировка продолжается.

Сравнивая медиаблокировки в России и Европе, мы наблюдаем следующие различия:

- **Количество заблокированных сайтов медиапроектов**. Россия заблокировала гораздо больше СМИ в ЕС по сравнению с количеством российских медиа-сайтов, заблокированных в ЕС.
- **Эффективность блокировок**. Россия быстро и эффективно блокировала СМИ ЕС в многочисленных сетях (вероятно, с помощью ТСПУ), в то время как блокировка сайтов российских СМИ не осуществляется последовательно во всех странах-членах ЕС.
- **Легкость обхода**. Страны ЕС в основном осуществляли блокировку на уровне DNS, что легко обходится как пользователями Интернета в ЕС (путем смены DNS-резольвера), так и затронутыми российскими СМИ (например, Sputnik сменил домен). Тем временем Россия заблокировала доступ к новостным СМИ ЕС с помощью TLS-вмешательства, для обхода которого необходимо использовать Tor или VPN, рекламировать которые в России запрещено. Тем не менее, в последние годы в России наблюдается заметный рост использования VPN.

В то время как ЕС пытается ограничить российскую пропаганду, блокируя доступ к сайтам российских СМИ в Европе, эта цензура укрепляет нарратив российского правительства, чтобы оправдать блокирование международных СМИ в России (о чем свидетельствует решение Министерства иностранных дел России заблокировать 81 сайт европейских СМИ в ответ на блокировку большего количества российских СМИ в ЕС).

Блокировка сайтов российских СМИ в Европе – регионе, который стремится поддерживать демократические ценности и в котором нет повсеместной сетевой цензуры, – заставляет задуматься о том, не создает ли это прецедент для дальнейшей цензуры в ЕС и во всем мире, особенно в условиях глобального роста авторитаризма.

Благодарности

Мы благодарим пользователей OONI Probe в России за проведенные тесты и собранные измерения, использованные в этом отчете.

Мы также благодарим участников интервью, которые оказались готовы поделиться с нами своим опытом столкновения с российской цензурой.