

Как Рунет троллит Роскомнадзор. Хроника необъявленной войны

Больше двух недель в Рунете идут боевые действия: недовольные политикой в отношении интернета россияне троллят Роскомнадзор. «Активисты» добавляют к сайтам из списка запрещенных IP-адреса «добропорядочных» порталов, а часть операторов связи блокирует их. Запретить менять IP Роскомнадзор не может, потому что это невозможно. Наказать провайдеров регулятор тоже не может, потому что они действуют по его же инструкциям. Пока Роскомнадзор ищет выход, страдают люди и компании. С чего конфликт начался и как развивался — в хронике SmartBabr.

Июль 2012 года. Принят закон о блокировках

В июле 2012 года Госдума приняла 139-ФЗ — о «черном списке» сайтов. Закон обязывает операторов связи ограничивать доступ к ресурсам из реестра запрещенных. Ограничивать по доменному имени и по IP-адресу.

Против закона во время его рассмотрения высказывались все — от Яндекса до Совета по правам человека. Больше всего говорили о цензуре в интернете, но были и другие замечания.

«Множество веб-сайтов и сервисов могут размещаться **на одном IP-адресе**, это значит, что при ограничении доступа к отдельно взятому материалу, могут быть закрыты и другие, не нарушающие законодательство ресурсы», — предупреждали в Google.

Первый такой случай произошёл сразу после принятия закона. В конце июля 2012 года заблокировали сайт экстремистов, а вместе с ним и сайт «Доброй машины правды» Навального. Позже эту дыру в законе кое-как залатали, научившись блокировать поддомены. Но другие дыры остались, и до поры до времени не давали о себе знать.

Февраль 2016 года. Дмитрий Медведев заходит на сайт заблокированного торрент-трекера RuTracker

Закону о блокировке сайтов уже четыре года. Казалось бы, все механизмы отлажены, дыры залатаны. В правительстве используют блокировку не только для защиты детей от вредной для них информации и борьбы с экстремизмом, но и для других целей. «Пожизненное» ограничение доступа теперь грозит и «пиратским» ресурсам — сайтам, на которых незаконно распространяется авторский контент. Под блокировку попал популярный в России RuTracker. Права издателей книг Донцовой защищены, все хорошо. Но тут происходит нечто нетривиальное.

На заседании правительственного совета по кино премьер-министр России Дмитрий Медведев решил зайти на RuTracker, и — смог. Несмотря на «вечную» блокировку сайта в России.

«Ну и как же ваш Роскомнадзор это блокирует?» — спросил Медведев у присутствовавшего на совещании министра связи Николая Никифорова.

Стало ясно, что у Роскомнадзора нет рабочего инструмента для мониторинга блокировок. В России четыре тысячи операторов связи и проверить, кто из них заблокировал сайт из списка запрещённых, а кто нет — не самая простая задача. После инцидента с Медведевым поиск её решений ускорился.

Ноябрь 2016 года. Операторам раздали «Ревизорро»

Уже к весне 2016 года была готова программа «Агент-Ревизор». Чуть позже сделали пробную «коробочку» для операторов. В октябре 2016 года появилась законченная версия устройства, которую раздали провайдерам. В ноябре вступили в силу поправки в КоАП: теперь за блокировку сайтов операторов должны заплатить штраф в 50-100 тысяч рублей.

Первые несколько месяцев показали: блокировать только по доменному имени или только по IP недостаточно. Сайт может сменить доменное имя, но сохранить IP-адрес. Или наоборот, может сменить IP-адрес или добавить еще один, но сохранить доменное имя. Если заблокировать что-то одно, блокировка будет неполной и для части аудитории при определенных условиях сайт может быть доступен.

«Агент-Ревизор» это увидит обязательно увидит. Потому что «Агент-Ревизор» проверяет не только доступность всех IP-адресов и доменных имен из единого реестра, но и всех IP-адресов, связанных с доменным именем сайта. Эта процедура называется **DNS-резолвинг**.

Если «Агент-Ревизор» находит три незакрытых оператором сайта, оператор получает штраф. Для крупной компании 50-100 тысяч рублей не проблема, а для небольшой два три таких штрафа — катастрофа. К тому же крупные операторы используют технологию глубокого анализа трафика, и проколов у них почти нет. А для мелких DPI — дорогое удовольствие. Поэтому небольшие операторы тоже начали проводить DNS-резолвинг и блокировать все найденные IP-адреса. И вот тут началось самое интересное.

Декабрь 2016 года. Звучат призывы троллить Роскомнадзор

Под новый год на «Хабрахабре» вышла [статья](#) «Как не распространять запрещенный контент, но всё равно ощутить на себе действие 139-ФЗ». В статье системный администратор хостинг-провайдера рассказал, как сайты на его хостинге попали под блокировку у клиентов некоторых операторов. Просто потому, что кто-то внёс IP-адрес хостинга в DNS заблокированного сайта.

Собственное расследование сисадмина показало, что всё дело в оборудовании для блокировок, которое производит DNS-резолвинг. И те операторы, кто такое оборудование использует, блокируют все сайты из выгрузки DNS.

«Большие провайдеры используют технологию блокировки DPI, которая позволяет избежать случайных жертв, — зато именно по IP-адресам блокируют сайты небольшие провайдеры. Короче говоря, оказывается, в России можно запросто заблокировать все что угодно — причём вовсе не по инициативе чиновников».

Хабрахабр

В обсуждении к статье разгорелась дискуссия, где стали звучать [призывы](#) устроить троллинг Роскомнадзора:

«Делаем сайт с явными нарушениями, ждём попадания в список, после чего вносим адреса топ-100 популярных у простого населения ресурсов в свои А-записи (DNS. — ред.). Есть подозрение, что такую самодеятельность (разрешение имен) через некоторое время провайдеры выключат. Правда, это нервов попортит простому народу, но...».

Из комментариев на «Хабрахабре»

Неизвестный комментатор как в воду глядел.

15 мая 2017 года. Кто-то ставит в DNS заблокированного сайта адрес сервера «Агента-Ревизорро»

Владелец домена pcsmedia.ru из реестра запрещенных сайтов прописал в DNS IP ресурсов РКН, к которым обращается система «Ревизор для передачи данных о фактической блокировке. Так он фактически

заблокировал доступ устройств «Агент-Ревизор» к Роскомнадзору. О происшествии стало известно из сообщения в Telegram-канале [IT уголовные дела СОПМ россиюшка](#). Авторы канала привели письмо операторам, в котором Роскомнадзор просит не резолвить сайт [portal.rfc-revizor.ru](#) и добавить его в белый список.

«Агент АС Ревизор не выходит на связь с сервером, так же не доступен веб-портал

Просим довести до сведения ваших сетевых администраторов.

В связи, с тем, что ресурс [ncsmmedia.ru](#) (запись реестра ЕАИС 217213) стал резолвится с адресами ревизора (и не только) агенты АС Ревизор не могут соединиться с сервером.

Прошу добавить адреса центра управления АС Ревизор в белый список:

213.59.243.131-135 ([no1.rfc-revizor.ru](#), [no2.rfc-revizor.ru](#) и т.д.), 46.61.230.185 ([portal.rfc-revizor.ru](#))».

[IT уголовные дела СОПМ россиюшка](#)

От оружия цензора пострадал сам цензор. Проблему быстро решили, но уязвимость в системе никуда не делась.

2 июня 2017 года. Под угрозой — «ВКонтакте» и Яндекс

Этот день можно считать началом активных боевых действий.

Хозяин одного из заблокированных доменов настроил CNAME (алиас) на [vk.com](#), и «ВКонтакте» стал частично недоступен у провайдеров.

В ответ на это Роскомнадзор снова разослал провайдерам письма с распоряжением не блокировать отдельные IP-адреса. Как выяснилось, это были IP «ВКонтакте» и Яндекса. Очевидно, ресурсы поисковика тоже пытались заблокировать.

3 июня 2017 года. В сети появляется сайт для троллинга

Активисты делают [сайт](#), чтобы троллинг Роскомнадзора стал доступен всем. Теперь кто угодно через этот сайт может ввести любой IP-адрес и он попадёт в DNS запись запрещенного ресурса.

Для части аудитории Рунета ресурсы на этом IP-адресе окажутся недоступны. Напомним, страдают только те люди, чьи операторы при блокировке используют DNS-резолвинг.

4-7 июня 2017 года. Блокируют «Википедию», «Медузу», [ivi.ru](#)

Для части пользователей стал недоступен Telegram. Оказалось, что владелец заблокированного домена [dymoff.space](#) добавил в DNS IP-адреса многих ресурсов. Кроме Telegram, в DNS домена нашли IP сайтов «Первого канала», «Одноклассников», «ВКонтакте», НТВ, сайта [Booking.com](#), Facebook, РЖД, [Mail.Ru](#) и ряда других.

В течение следующих дней с проблемами столкнулись Instagram, «Википедия», «Медуза», [ivi.ru](#) и десятки других сайтов. От троллинга Роскомнадзора стали страдать люди. Владельцы заблокированных ресурсов стали рассылать своим пользователям рекомендации по обходу блокировок. Суть их сводилась к следующему: сообщайте о проблемах своему провайдеру, используйте VPN и анонимайзеры.

Вместо того, чтобы отправить всем провайдерам рекомендации с описанием верного механизма блокировок, Роскомнадзор продолжает вручную рассылать IP-адреса, запрещенные для блокировки. При этом формулировки «запрет блокировок» нет даже в законе.

В Telegram-каналах прямо [указывают Роскомнадзору на некомпетентность](#).

7 июня 2017 года. Роскомнадзор публикует «белый список»

Роскомнадзор [составил](#) «белый список» из более чем 2000 интернет-ресурсов, которые нельзя блокировать.

Роскомсвобода [опубликовала](#) этот список полностью.

Ожидается, в нем оказались адреса сайтов правительственных учреждений, но не только. Роскомнадзор запретил блокировать также Яндекс, Facebook, Vk.com, Google, Twitter, YouTube, Instagram, Github и еще много других сервисов.

Принцип, по которому отбирали сайты в белый список, не понятен ником. Но всё ничего, если бы не одна деталь. На неё Роскомнадзору снова указали в Telegram:

Как вам, такая доменная маска в этом списке, по которой нельзя ничего блочить: «*.google.*»? Роскомнадзор как бы намекает: делай на своём сайте домен третьего уровня с наименованием "google" и тебе ничего не будет - ты защищён от блокировок именем государства!

Закрывая одну брешь, Роскомнадзор создал другую.

9 июня 2017 года. В России не работают банкоматы. Сбой связывают с троллингом

Дыру в системе блокировок использовали против платёжных серверов российских банков.

Во второй половине дня 9 июня в России произошел сбой платёжных терминалов. Как сообщали разные издания ([1](#), [2](#)) платежи не проходили через терминалы Сбербанка и «ВТБ 24».

Сбой подтвердил Сбербанк. Оказалось, что IP-адреса серверов авторизации интернет-платежей крупнейших российских банков оказались заблокированы. На устранение проблемы потребовался примерно час.

Активисты находят в DNS-записях сайтов из реестра запрещенных ресурсов IP-адреса серверов авторизации.

9 июня 2017 года. МВД грозит проверить ложную инфу о сбоях в банках

Роскомнадзор считает все заявления о сбоях выдумкой и обращается в МВД. Ведомство [сообщает](#) о начале проверки.

По обращению в Министерство внутренних дел Российской Федерации Роскомнадзора в связи с распространённой в сети Интернет ложной информации о якобы сбоях в работе платёжных систем ряда крупных российских банках в результате DNS-атаки начата проверка.

МВД России совместно с Роскомнадзором установили лиц, причастных к распространению заведомо ложной информации.

По результатам проверки будет принято процессуальное решение в соответствии с действующим законодательством.

Пресс-служба МВД

9 июня 2017 года. Роскомнадзор рассылает операторам письмо с требованием не делать DNS-резолвинг

Роскомнадзор призвал провайдеров блокировать сайты только по указанным в черном списке IP-адресам. В письме регулятора призвал провайдеров до 16 июня 2017 года отказаться от так называемой «эффективной блокировки» интернет-ресурсов – DNS-резолвинга.

Надзорное ведомство подчеркивает, что штрафовать за такое действие провайдеров не будут.

В сети связали дату с «прямой линией» президента РФ Владимиром Путиным, которая была намечена на 15 июня. В Telegram-каналах традиционно язвительно отозвались на очередной ход регулятора:

В итоге мы заставили РКН вернуть «защищённость» механизма блокировки на прежний уровень, когда заблокированному ресурсу зачастую достаточно сменить IP, чтобы выйти из-под блокировки.

15 июня 2017 года. Роскомнадзор обвиняет во всём небольших операторов и сторонников Навального

Руководитель Роскомнадзора Александр Жаров заявляет: «Роскомнадзор прекрасно осознает не только как работает система блокировок, но и как ее нужно совершенствовать и развивать». По мнению чиновника, масштабы проблемы сильно преувеличены, угрозы устойчивости Рунета не возникало.

В проблеме с блокировками, по словам Александра Жарова, виноваты небольшие провайдеры. Они составляют 50-55% численности, не имеют систем анализа трафика и блокируют сайты с использованием «грубого» механизма — по IP-адресу. Решением проблемы, по мнению чиновника, может стать новый закон. Он должен дать органам власти право самостоятельно определять порядок блокировки.

Как выяснилось чуть позже, Роскомнадзор нашел еще виноватых.

Регулятор заподозрил сторонников Навального в организации ложных блокировок, сообщили «Ведомости». По мнению Роскомнадзора, ложные блокировки устроили активисты Фонда борьбы с коррупцией Александр Литреев, Владислав Здольников и Александр Брусенцов. Владислав Здольников и Александр Брусенцов уезжают из России. Александр Литреев продолжает освещать ситуацию.

21 июня. Сторонники Навального жалуются на Роскомнадзор в Следственный комитет

Сторонники Навального пожаловались в Следственный комитет на Роскомнадзор и Минкомсвязи, сообщили «Ведомости». Литреев, Здольников и Брусенцов считают, что чиновники намеренно скрывали информацию об уязвимости в своей системе блокировок.

Активисты расценили, что поведение чиновников можно квалифицировать как халатность. В Роскомнадзоре знали об уязвимости более двух месяцев, но не совершили необходимых действий. По словам авторов заявления, об этом свидетельствуют письма о совещаниях, которые проводились по теме в марте. В действиях чиновников можно усмотреть и признаки злоупотребления служебным положением: желая избежать ответственности за уязвимость, они не информировали о ней законопослушных владельцев сайтов.

Представители Минкомсвязи и Следственного комитета отказались от комментариев.

27 июня. Роскомнадзор запретил операторам без DPI проводить резолвинг

Роскомнадзор выпустил рекомендации для интернет-провайдеров, в которых запретил DNS-резолвинг операторам, не имеющим DPI. Теперь они должны фильтровать запросы к DNS-серверам.

Новые правила Роскомнадзора запрещают не имеющим DPI провайдерам самостоятельно вычислять IP-адреса. Они должны ограничивать доступ к доменному имени посредством фильтрации запросов ко всем DNS-серверам — чтобы компьютер пользователя «не узнал», по какому адресу находится запрещенный сайт, и не мог к нему подключиться.

Операторы также могут договариваться о совместной блокировке: когда один провайдер получает трафик у другого и тот уже заблокировал сайт, то дополнительно его фильтровать не нужно.

Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 7701 21.06.2017, 13:54

URL: <https://babr24.com/?IDE=272377> Bytes: 17209 / 10115 Версия для печати

 [Порекомендовать текст](#)

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)
- [ВКонтакте](#)

Связаться с редакцией Бабра:
newsbabr@gmail.com



Автор текста: **Полина Чехова**,
журналист.

На сайте опубликовано **494**
текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: [@babr24_link_bot](#)
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: [@bur24_link_bot](#)
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: [@irk24_link_bot](#)
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: [@kras24_link_bot](#)
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: [@nsk24_link_bot](#)
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: [@tomsk24_link_bot](#)
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: [@babrobot_bot](#)
эл.почта: equatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)