Текст · 13 сентября 2021, 10:00
Давид Френкель, Александр Бородихин,

«Интернет в России будет все хуже, хуже и хуже». Чем война Роскомнадзора с VPN грозит россиянам

VPN — *Virtual Private Network* или «виртуальная частная сеть» — общее название технологий, с помощью которых компьютеры можно объединить через интернет в «частную» сеть, как будто они соединены напрямую, даже если они находятся далеко друг от друга. В такую сеть можно объединить любые устройства или даже целые локальные сети — например, так можно создать единое пространство для офисов или филиалов одной компании. Само *VPN*-соединение шифруется, поэтому стороннему наблюдателю — например, провайдеру — виден только зашифрованный трафик. Благодаря этому *VPN* стали использовать для обхода блокировок: если установить прямое соединение с точкой выхода в интернет, находящейся в другой стране, провайдер не будет знать, на какие сайты заходит пользователь, а следовательно, не сможет заблокировать доступ.

DPI — *Deep Packet Inspection* или «глубокое исследование пакетов» — поскольку информация передается по интернету в виде коротких блоков данных, называемых пакетами, существуют методы анализа их содержимого, даже если оно надежным образом зашифровано. Прочитать содержимое пакетов наблюдатель не может, но может понять, к примеру, с каким сайтом контактирует пользователь и

по какому протоколу обмена данными. Часто *DPI* называют и само устройство, установленное у интернет-провайдера, которое изучает трафик пользователей, чтобы распределять нагрузку в сети или блокировать запрещенную информацию.

ТСПУ — «Технические средства противодействия угрозам» — устройства, которые Роскомнадзор устанавливает у интернет-провайдеров в рамках закона о «суверенном интернете», чтобы иметь возможность контролировать трафик пользователей: изучать с помощью *DPI,* замедлять и даже полностью блокировать.

DNS — *Domain Name System* или «система доменных имен» — своеобразная телефонная книга интернета, соединяющая «адреса» сайтов и серверов в числовых значениях с привычными пользователям веб-адресами. Обычно запрос с адресом к конкретному сайту уходит в незашифрованном виде, и провайдер легко может узнать, какой ресурс посещает пользователь — так осуществляются блокировки сайтов по *DNS.* Современные технологии *DNS* через *HTTPS (DoH)* и *DNS* через *TLS (DoT)* пытаются затруднить такое подглядывание, шифруя сами *DNS*-запросы; осенью прошлого года министерство связи представило законопроект, в котором предложило наказывать за использование таких технологий.

Владислав Здольников — *IT*-специалист, в прошлом работавший над проектами Алексея Навального, создатель сервиса Red Shield VPN,

основатель проекта GlobalCheck по мониторингу блокировок.

Михаил Климарев — автор телеграм-канала «За Телеком», директор «Общества защиты интернета».

Филипп Кулин — интернет-эксперт, автор телеграм-канала «Эшер II».

Станислав Селезнев — адвокат, правовой аналитик проекта «Сетевые свободы».

Что происходит? Учения? Подготовка к масштабной блокировке VPN?

Здольников. Роскомнадзор, который последние два года активно занимался установкой государственного *DPI,* тестирует ТСПУ — инструмент для политической цензуры. Первыми заблокированными на ТСПУ, который, по заявлениям чиновников, был призван «повысить стабильность рунета», были ресурсы ФБК[1], блог Навального, а затем сайт «Умного голосования» и приложение.

Последнюю неделю РКН на какое-то время блокировал инструменты, которые использует или может использовать приложение «Навальный» для обхода блокировок — *DoH* и *DHT*[2]. Они смотрят, что будет: какие ресурсы и сервисы пострадают, какое возмущение это вызовет у «мирных» пользователей этих технологий. От блокировки *DoH*-сервисов *Google* и *Cloudflare* пострадали обычные пользователи, которые шифруют свои *DNS*-запросы, а от блокировки *DHT* — торренты, различные блокчейны и стриминговые сервисы, вроде *Twitch.* С помощью тестовых ударов РКН пытается

прогнозировать ущерб от полноценной блокировки этих инструментов 15 сентября, когда будут опубликованы рекомендации по голосованию, или во время выборов.

Селезнев. Об учениях вести речь нельзя, поскольку план учений должен быть утвержден на год вперед, а этого не сделано (тут Фил Кулин хорошо разбирает вопрос). Таким образом, это не учения, а полноформатный выход России за пределы «сетевого нейтралитета», обоснованный исключительно волей Роскомнадзора. О какой-либо легитимной процедуре речь вести не получается. Фактически, нынешняя атака на свободу рунета началась с замедления твиттера в марте и продолжается уже полгода.

Кулин. Я реально верю и в «мы тестируем готовность к массовому суверенному Рунету» и в «мы зачем-то бегаем за УмГ». В первом случае я считаю, что они еще не готовы к отдаче. А во втором я не понимаю смысла. Они пиарят УмГ больше, чем от него вообще толку.

Климарев. Мы говорили два года назад, когда там начали принимать суверенный рунет — когда только-только начали принимать его, были дебаты в Госдуме, и мы говорили о том, что самая главная его проблема будет в том, что блокировки станут непрозрачными.

Роскомнадзор сможет делать что угодно. Никто не знает, что там происходит, никто не знает и что там блокируют, как там блокируют. Это черный ящик. Черный ящик стоит на пути всего интернет-трафика и пропускает через себя все пакетики, и он эти

пакетики может в теории анализировать. Это все управляется из Центра управления и мониторинга сетями связи, короче, это РКН всем управляет.

Логотип NordVPN. Фото: Omar Marques / SOPA Images / Sipa USA / East News

VPN заблокируют в России целиком?

Кулин. В перспективе — да. Причем не только сервисы [, а технологию как таковую].

Климарев. Оказалось, что могут. Ну, то есть вот мы думали, что нет, а оказалось, что могут. В теории в интернете ничего заблокировать по определению нельзя, потому что это полносвязный граф, и если на пути этого графа стоят какие-то преграды, ты всегда сможешь найти обходные пути. Тем более при современном развитии криптографии. Разумеется, мы придумаем что-нибудь, что потом будет массово использоваться. Но на текущий момент получается, что Роскомнадзор может блокировать, в том числе и протоколы.

Здольников. Роскомнадзор понимает, что на точечную блокировку тысяч *VPN*-сервисов у них просто не хватит ресурсов, поэтому они решили ударить по самым популярным, заблокировав самый современный протокол *WireGuard.* Его по умолчанию использует и бесплатный *Cloudflare WARP,* и многие платные, вроде *NordVPN.* Скорее всего еще несколько популярных *VPN*-сервисов, которые используют другие протоколы, будут блокировать точечно перед выборами или во время них.

Селезнев. Могу лишь сказать так: Роскомнадзор атакует своими ТСПУ пока крупные сервисы. Если говорить о законодательстве в этой сфере, то практически вся нормативная база, которая последние пару лет принимается в этой сфере, прямо противоречит международным стандартам. Так, ООН считает анонимность и шифрование в интернете базовым правом человека — смотреть утвержденный в 2015 году доклад Дэвида Кая.

Утром 13 сентября в канале «За Телеком» появился скан приказа по «Ростелекому», в котором начальство требует от сотрудников «в целях организации устойчивого доступа абонентов в сеть "Интернет"» прекратить выдачу абонентам DNS-адресов через сервисы *Google* (8.8.8.8, 8.8.8.4), *Cloudflare* (1.1.1.1, 1.0.0.1) и *Cisco* (*OpenDNS* по технологии *DoH*). Вместо этого предлагается использовать DNS-сервера самого «Ростелекома» или «Национальной системы доменных имен».

> В начале сентября в канале «Эшер II» публиковалась выдержка из другого документа, авторство которого не упоминалось. В нем говорилось, что Роскомнадзор планирует «осуществление комплекса мер по ограничению доступа к ряду иностранных DNS-сервисов». В этом письме также упоминались сервисы *Google*, *Cloudflare* и *Cisco*.

Те сервисы, которые РКН называл, теперь не работают в России?

Селезнев. У меня есть подписка на один из заблокированных сервисов, и он действительно не работает сейчас.

Кулин. Некоторые сервисы работают. Некоторые стали сервисами Шредингера: то работают, то нет. Очень секторально.

Здольников. Почти все сервисы из «расстрельных списков» работают в России, но если выбрать другой протокол в настройках приложения.

Wireguard — протокол, который проще заблокировать, чем другие?

> WireGuard — современный открытый протокол для организации VPN-сетей, который используется большинством популярных коммерческих VPN--сервисов. Предположительно, именно этот протокол стал основной целью Роскомнадзора в борьбе с сервисами Nord VPN и Express VPN. «Блокируют целиком протокол WireGuard», — написал 8 сентября автор канала «За Телеком» Михаил Климарев.

С началом блокировок VPN-сервисов в России пользователи онлайн-игры World of Warships начали испытывать сложности с доступом — трафик геймеров системы DPI, по всей видимости, принимали за VPN.

Здольников: Да, но не по техническим причинам, а по политическим: он новый, и, несмотря на популярность в *VPN*-сервисах, его почти не используют компании для служебных нужд. Именно поэтому Роскомнадзор опасается блокировать *OpenVPN* или *IKEv2* — от этого пострадает много фирм, включая банки. С технической точки зрения, почти все *VPN*-протоколы заблокировать просто, причем без последствий для других протоколов или ресурсов.

Кулин. Нет. Протокол как протокол. Он просто довольно современный, популярный, и есть в ядре *Linux.* Но он неплохо опознается, потому что не был предназначен для скрытности. Но, кстати, опознается он при этом с заметным числом ложного опознания.

Климарев. Он не проще, но он же рассчитан был, что не будет такой шняги, и он работал максимально оптимальным способом. Сейчас эти протоколы пересматриваются, и он будет, видимо, обфусцирован-[3], будет немножечко работать по-другому. На стандартных портах и на стандартных настройках им удается блокировать. Если перевести клиенты и сервера *WireGuard* в какие-то неочевидные порты, например, 80-й порт — это порт *HTTP,* то он не блокируется, нормально работает. Они его пока не могут, видимо, отличить. Пока, подчеркну.

Помимо платных и бесплатных VPN-сервисов есть частные VPN, которые люди сами поднимают за границей. Может ли ТСПУ блокировать такие VPN — или это слишком трудозатратно?

Здольников. Блокировки по протоколам, которые сейчас применяет Роскомнадзор для борьбы с *VPN*, затрагивают любые подключения. Не важно, к большому сервису или к собственному серверу.

Селезнев. Даже при перекрытии всех коммерческих *VPN*-серверов очень сложно перекрыть все индивидуальные *VPN*, которые энтузиасты разворачивают для личного/семейного/корпоративного использования. Просто по причине их скрытности и огромного количества. Таким образом, будет идти речь о техническом противостоянии между ТСПУ, оборудованием, которое при помощи *DPI* пытается выявить трафик *VPN* и средствами маскировки этого трафика. Такие технологии вовсю обкатываются, достаточно почитать форумы *IT*-энтузиастов.

Кулин. Я думаю, это сейчас и тестируют, именно этот вопрос. Одна из основных проблем блокировки частных *VPN* в том, что на этих же технологиях построены *VPN* компаний. Так можно сделать, только если ты опричник и метешь метлой мразь всякую, недостойных граждан и фирмы, которые не опричь. Но да, мы уже видим победившую опричнину. «Системообразующие компании не пострадали» А.Жаров. «Мы разослали по ведомствам» , и так далее.

Смысл в том, что сервисы имеют понятные эндпойнты[4]. А связь между филиалами «Рогов и Копыт» можно идентифицировать десятилетиями. А

главное, что они ничем не отличаются от Росатома, Ростеха, Роскосмоса и так далее, где свой бардак.

Климарев. Ребята, которые умеют что-то делать, они все эти вещи тоже обойдут. Они решат эти проблемы: есть возможность сделать обфускацию трафика, сделать нестандартные порты, какие-то вещи поднастроить, это индивидуально делается. Не думаю, что кто-то будет бегать [за рядовыми пользователями] ради таких вещей, поэтому да, это возможно, но связь даже при такой архитектуре в любом случае будет хуже, чем без *[VPN]*. Приедете в любую страну со свободным интернетом, включите *VPN*, а потом выключите его — и почувствуете разницу.

ТСПУ — вообще само по себе продвинутое программное обеспечение?

Климарев. Оказалось продвинутое. Мы не знаем, что это такое, никто его не видел. Это все в условиях секретности ставится, для операторов это черный ящик. Просто вот коробка, которую поставили под страхом всяких писем, всяких соглашений о секретности, и не пускают никого.

Я даже фото от человека не могу получить, мне обещают фото прислать, как выглядят все эти штуки, но не могут, потому что там телефоны отбираются при заходе в зал, где стоит это оборудование. В закрытый шкаф [устанавливается], к нему подводится электричество, интернет — в смысле, оптика — и отвод тепла, и стойка закрыта на ключ, алюминиевые печати ставят.

Если такие работы [проводятся], находят окно [по времени], чтобы никому не мешало — или наоборот всех [сотрудников] разгоняют. Это планируется все, в виде письма какого-то, просим обеспечить доступ наших специалистов в особых условиях. Договариваются об особых условиях, в каждом же операторе связи до сих пор существуют всякие «секретчики». Служба мобилизации, поскольку это связь, военные, гражданская оборона, всякие МЧС и так далее. У крупных операторов есть целые отделы, которые занимаются взаимодействием с этими службами, вот через эти службы это проводится, и организуется так, чтобы в условиях секретности это все ставилось.

Здольников. Получив опыт блокировок, включая провал с *Telegram,* власти сделали очевидный вывод: не нужно пытаться делать технические решения самостоятельно. Тогда они стали присматривать компанию, которая качественно поможет решить технические задачи по цензуре в интернете.

Выбор пал на ООО «РДП.ру» — фактически бывший отдел подмосковного оператора «Экотелеком», который делал решения сначала для собственных нужд, а затем стал продавать их другим операторам в России и СНГ. В итоге его купил Ростелеком в качестве поставщика оборудования для ТСПУ.

Коробочки ЭкоDPI, которые ставят в качестве ТСПУ, много лет до этого покупали за свой счет — и покупают до сих пор — операторы, чтобы решать свои задачи: *BRAS*[5], *NAT*[6], ну и *DPI,* чтобы эффективно блокировать сайты, не получая штрафы от системы

«Ревизор». Это качественное железо и софт, которое, к сожалению, эффективно блокирует сайты и протоколы.

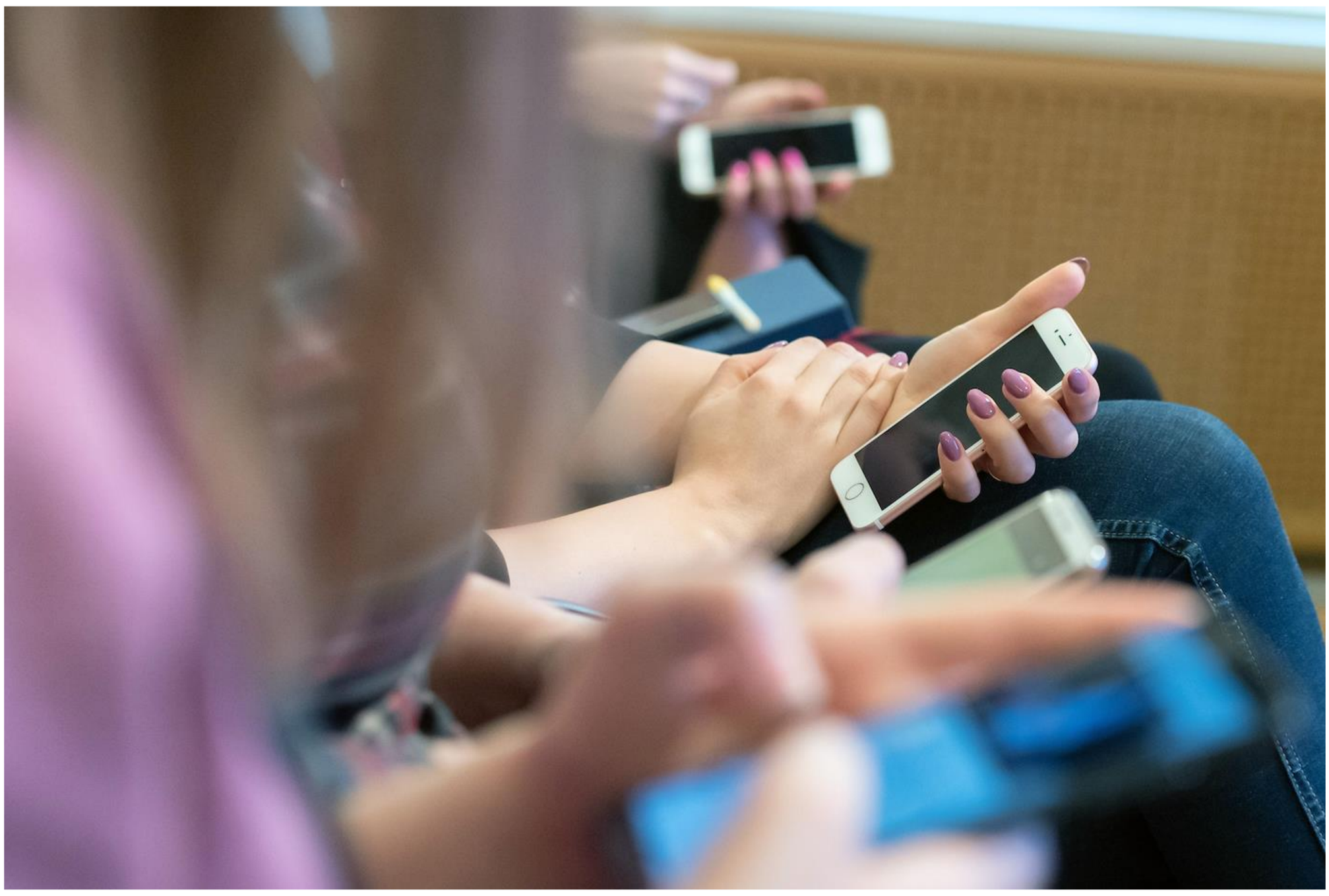

Фото: Олег Харсеев / Коммерсант

Почему при блокировках страдают другие сервисы? Могут ли они улучшить качество блокировок, чтобы не страдали другие сервисы?

Кулин. Во-первых, потому что им пофиг. Во-вторых, где-то могут [блокировать, чтобы не страдали другие сервисы], где-то нет. Обычно это взаимоисключающие вещи.

Теория блокировок многогранная. Я, например, согласен с мнением бывшего чиновника Минсвязи Вартана Хачатурова. Если уж хотелось что-то заблокировать, сделали бы блокировку на *DNS* и обязали бы провайдеров прямо всем только фильтрованный *DNS* выдавать. И волки были бы сыты, и овцы целы. А так бурный токсичный подогрев воздуха.

Здольников. Зависит от того, что именно они будут блокировать. Два года назад РКН не мог эффективно заблокировать сайт «Умного голосования», при этом не задев другие ресурсы на *Google,* а теперь у них есть такая возможность.

Если, как в случае с *WireGuard,* протокол используется только сервисами для обхода блокировок, то от его блокировки ничего больше не пострадает. Если они будут блокировать протоколы, которые маскируются под «легитимный» трафик, или, например, под мусор, как это умеет *Telegram,* то это неизбежно повлечет за собой проблемы с доступностью других ресурсов.

Климарев. Чем дальше, тем будет хуже. Это все равно, что бомбить город. Это называется *collateral damage,* сопутствующие потери, сопутствующие жертвы. Похожие протоколы, где-то рядышком находились, случайные какие-то срабатывания. Именно так *[-DPI]* работает, по каким-то признакам определяют пакет, что он должен быть заблокирован. Выясняется, что блокируется не только [то, что планировалось заблокировать], но и вот эти сервисы.

Селезнев. ЕСПЧ летом 2020 года в решении по делу «Харитонов против России» указал четко и ясно, что подобные действия властей недопустимы и однозначно являются недопустимым вмешательством в свободу получения и распространения информации. Так что шансы на получение компенсаций у всех пострадавших сервисов и их клиентов весьма реальны.
Проект «Сетевые свободы», кстати, готов оказать

юридическую помощь. Но, судя по всему, и страдания пользователей, и потенциальный финансовый ущерб от выплат компенсаций власти оценивают как приемлемые для них неудобства ради достижения контроля над сетью.

Могут ли VPN-сервисы как-то сопротивляться блокировкам? Есть ли данные, что они сопротивляются?

Здольников. Некоторые платные сервисы, которые закладывают это в стоимость подписки, и у которых есть соответствующие механизмы, могут активно сопротивляться блокировкам: ротировать адреса *API* и самих *VPN*-серверов. Это делает *ExpressVPN* и отчасти *NordVPN* в Китае, это делают некоторые сервисы в ОАЭ, Индии и других регионах. Наш *Red Shield VPN* будет сопротивляться блокировкам точно так же, как и в предыдущие две попытки нас заблокировать (плюс последует еще одно дело в ЕСПЧ против российского государства). Возможно, таких сервисов будет еще 1-2.

Кулин. Да, конечно.

Климарев. С кем я общаюсь, по крайней мере, почти все в голос говорят, что будут [сопротивляться], и *Nord VPN,* и *Tunnel Bear* будет. У них бизнес-модель такая, они же деньги зарабатывают именно с того, что они обходят блокировки.

Telegram не удалось заблокировать, что с тех пор изменилось? РКН стал сильнее? ТСПУ массово установлены?

Климарев. Конечно, все учли. На этот раз все серьезно.

Здольников. Безусловно, ТСПУ — это, в первую очередь, результат работы над ошибками первой

войны с *Telegram.* ТСПУ дает возможность блокировать протоколы, в том числе пытаться блокировать те, что скрываются под мусор или под другие протоколы.

Вторую войну *Telegram* будет выиграть гораздо сложнее. Это во многом зависит и от увеличения ресурсов со стороны *Telegram.* Не получится стоять на месте в то время, как твой враг наращивает ресурсы. Нет никаких сомнений в том, что вторая война будет — российское государство умеет делать шаг назад, но только на время.

Кулин. Появились ничем, вообще ничем не ограниченные ТСПУ. Появилось понимание, что их можно и нужно ставить на транзит [трафика между границами стран], в этом есть смысл для них. Это сильно упрощает обхват. Думаю, они не установлены прямо массово и не охватывают большинство транзита, но охватывают уже заметную часть сетей. Я субъективно думаю, что меньше 50%, но больше 20%.

Это навсегда — или забудут про блокировки после выборов?

Здольников. Нынешнее обострение блокировок происходит в том числе из-за выборов: они хотят, чтобы «Умным голосованием» воспользовалось как можно меньше людей.

Но нужно помнить, что политическое пространство в России было практически полностью зачищено, и «докручивание» цензуры в интернете было неизбежно. Тренд на блокировки протоколов и технологий, которые могут использоваться

пользователями или блокируемыми сервисами для их обхода, безусловно, сохранится.

Будет хуже, как мы все отлично понимаем.

Селезнев. Вряд ли власти допустят какой-то откат. Доктрина сетевой безопасности требует установить и сохранять полный контроль властей над рунетом. Наиболее удобный для этого способ — технически заблокировать все неподконтрольные сервисы международных *IT*-гигантов, а для избежания социальных взрывов приучить аудиторию рунета к пользованию *Russian-based* аналогами. Если они будут хотя бы на 1/10 часть функциональны, как заблокированные иностранные, то принцип движения человека по пути наименьшего сопротивления вполне может привести российских пользователей к «окукливанию» в рамках прозрачной для спецслужб инфраструктуры.

Климарев. Зубную пасту из тюбика уже выдавили, как ее назад теперь запихнуть. У них появилась возможность, они готовились целых два года, [глава Роскомнадзора Андрей] Липов пришел.

Я не утверждаю, что все пропало, надо [вещи] собирать, чемодан, вокзал, заграница. Я утверждаю только то, что действительно они могут сделать нашу жизнь хуже.

В любом случае, если у тебя пакетики бежали прямо, они бежали эффективно, *YouTube* работал, и он работал хорошо. С сентября 2021 года эта ситуация кардинально меняется, но на самом деле она поменялась с момента замедления *Twitter*. Любые

блокировки можно обойти, но нужно понимать, что качество связи при этом ухудшится. Либо у тебя пакетики прямо бежали, либо они у тебя побегут какими-то кривыми путями. Интернет в России будет хуже, все хуже и хуже.

Тут Христо Грозев тоже заявлял, что у него есть информация, что, в течение двух лет к тем сервисам по закону о приземлении [предъявят] невероятные какие-то требования, это тоже же звенья одной цепочки, типа желтую звезду на лоб клеить себе и писать, что я преступник. Понятно, что нормальный человек не будет этого делать. Никто не будет писать у себя на страницах, что «Я преступная организация».

И это будет *casus belli* для того, чтобы ограничивать доступ к этим ресурсам. Прежде всего *Facebook*, *Google* с *Youtube*, это точно. Их будут потихонечку, потихонечку, и не то чтобы прямо вот блокировать, а будут просто снижать качество связи с ними. Скорость будут прибирать, как с *Twitter*. Он как бы есть, он как бы работает, ничего как бы такого нет, но пользоваться им невозможно.

Редактор: Дмитрий Трещанин

---

1. Российские власти продолжают массово и бессистемно пополнять списки «иностранных агентов» — туда включают правозащитников, политиков, активистов, журналистов, некоммерческие организации и издания. Закон о СМИ обязывает нас указать, что Фонд борьбы с коррупцией внесен Минюстом в «реестр НКО, выполняющих функции иностранного агента». Кроме того, ФБК признан экстремистской организацией и запрещен.

2. DHT — distributed hash table или «распределенная хэш-таблица» — инфраструктура распределенных файловых систем, которую используют, в частности, торрент-трекеры.

3. Так называют намеренное «запутывание» кода разработчиком, чтобы работоспособность программы не менялась, а ее сторонний анализ был невозможен из-за лишней бессмысленной информации.

4. Конечный адрес или устройство в сети. В данном случае речь идет о публичных серверах VPN-сервисов, к которым подключаются пользователи, адреса которых известны — в отличие от непубличных серверов частных компаний, использующих VPN для своей внутренней работы, например, для связи нескольких офисов в единую внутреннюю сеть.

5. Маршрутизатор широкополосного удаленного доступа» — сервер, фактически являющийся входной точкой для клиентов интернет-провайдеров. Он может определять, по каким каналам в сетях провайдера в дальнейшем передается трафик каждого пользователя и распределять приоритет между разными запросами разных клиентов.

6. Собирательное название для ряда способов использования одного IP-адреса для нескольких клиентов.