Текст · 8 августа 2023, 15:55
Давид Френкель, Дмитрий Швец,

Новая атака на VPN может стать успешной. Обходить блокировки будет все сложнее, считают эксперты

Российские власти последние несколько лет наращивают степень контроля над интернетом. Роскомнадзор особенно старается контролировать *VPN*. Власти пытались заставить сервисы соблюдать законы о блокировках, отказавшихся также блокировали, а прошлой весной Роскомнадзор начал бороться уже не с отдельными сервисами, а запрещать сразу целые протоколы для использования *VPN*. Это продлилось недолго, но теперь, похоже, цензоры вернулись к этой практике в еще большем масштабе.

В понедельник, 7 августа, пользователи *VPN*-сервисов из России заметили проблемы с подключением к серверам. Одним из первых на это обратил внимание *IT*-специалист Филипп Кулин, он написал об этом у себя в телеграм-канале — и сотни пользователей поделились[1] своими наблюдениями.

Картина складывалась противоречивая: у абонентов одного оператора мог работать *VPN*, а мог — нет, в одном регионе у части пользователей были трудности с подключением, а другие не испытывали технических проблем. Корреспондент «Медиазоны» провел в твиттере небольшой опрос с таким же результатом.

В тот же день вечером создатель сервиса обхода блокировок *AntiZapret* под псевдонимом *ValdikSS* опубликовал пост, в котором он рассказал, что провел испытание разных типов подключения и их блокировки. Он пришел к выводу, что блокируются преимущественно подключения из России к серверам за границей у абонентов мобильных операторов и что эти блокировки заметно отличаются от того, что было раньше.

На этот раз под удар попали не популярные коммерческие сервисы, доступные всем желающим, а частные серверы, которые пользователи самостоятельно настраивали у зарубежных провайдеров. Поменялся и характер блокировки: как считает *ValdikSS*, теперь Роскомнадзор с помощью *DPI* и ТСПУ оценивал тип трафика и сразу же его блокировал, если определял как подключение через *VPN*. Блокировались популярные протоколы *WireGuard*, *L2TP* и *OpenVPN*.

Как считает технический директор «Роскомсвободы» и основатель *Privacy Accelerator* Станислав Шакиров, это были «блокировки не втупую». По его мнению, цензоры пытаются сделать так, чтобы блокировка *VPN* затронула только частных лиц, но не повлияла на работу корпоративных клиентов.

С ним согласен создатель *RedShield VPN* Владислав Здольников: по его мнению, власти раньше не блокировали *VPN*-протоколы, потому что «договаривались с крупным бизнесом об исключении адресов, чтобы не обрушить им служебные туннели». Еще в 2021 году было известно, что Центробанк рассылал в банки письма с просьбой назвать

VPN-сервисы, которыми те пользуются, чтобы не навредить кредитным организациям.

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.

Эксперты ищут способы обхода новых блокировок

На техническом форуме *ntc.party* уже приводятся методы обмана технологии *DPI*, к которой прибег Роскомнадзор. В частности, комментаторы советуют направлять безобидные запросы, чтобы система блокировки помечала соединение как разрешенное, а затем уже подключаться через *VPN*, правда, этот

способ требует серьезных навыков и не подходит обычным пользователям.

Авторы канала *VPN Generator* анонсировали решение, «ради остановки которого нужно будет вообще обрубать весь интернет». Они также описали проявившиеся побочные последствия новых блокировок: «У многих легло видеонаблюдение (воруй-убивай, гуси — бегити!), обычные бизнесы не могут достучаться до своих серверов и разрушена связность между филиалами».

Шакиров из «Роскомсвободы» советует простым пользователям устанавливать несколько программ для *VPN*, например *Psiphon*, *Lantern*, *Amnezia* и *Tor-*: «Пока что-то одно всегда работало, что бы ни происходило».

«Если вдруг ничего не работает, надо подождать несколько дней, потому что какое-то время необходимо разработчикам всех этих систем, чтобы обновить свой софт, — объясняет он. — Во-первых, нужно время для того, чтобы его написать. Потом какое-то время релиз апрувится в *Apple Store* и *Google Play*».

Также специалисты обращают внимание на протоколы *Shadowsocks* и *XTLS*: они позволяют устанавливать *VPN*-соединение, которое сложно обнаружить методами Роскомнадзора.

Они появились в Китае для преодоления «Великого китайского фаервола», а теперь широко используются и в России. Например, основанный на *Shadowsocks* проект *Outline* лежит в основе *VPN*-сервиса

петербургского издания «Бумага». Правда, как считают в «Роскомсвободе», именно эти протоколы могут стать следующей целью властей.

Что будет дальше

«Массово задавить так, чтобы подключения не работали у большинства людей, уже сделали — фильтры написаны и работают. Надежность обходных методов невелика и затратна по времени — у меня ушло три полных дня, чтобы соорудить модификацию протокола *OpenVPN* с обходом блокировки на стороне сервера, которая бы работала на всех провайдерах под блокировкой (фильтры чуть разнятся от провайдера к провайдеру), — объясняет *ValdikSS*, создатель сервиса обхода блокировок *AntiZapret*. — Перспективы для пользователей — использование не коммерческих протоколов *VPN*-, а специальных средств обхода блокировок — *Shadowsocks*, *VMESS*, *Trojan* со товарищи. Они поддерживаются в меньшем количестве устройств (едва ли присутствуют в какой-либо официальной прошивке роутеров), зато разрабатываются с учетом цензуры и активно дорабатываются».

Шакиров из «Роскомсвободы» убежден, что в конечном итоге в России будет введена «китайская модель» интернета, то есть почти автономное существование, когда мировые сервисы вроде ютуба или фейсбука заблокированы и заменены отечественными аналогами. Впрочем, он полагает, что способы обходить блокировки все равно останутся, но с каждым разом нужно будет прибегать ко все более сложным манипуляциям.

С ним согласен Владислав Здольников. «С усложнением доступа количество людей, которые будут получать альтернативную информацию, неизбежно снизится», — считает он.

По мнению Филиппа Кулина, такой качественный переход в блокировках может простимулировать *IT*-компании к борьбе с цензурой: «Так скажем, война РКН с *VPN* до позавчера была "странной войной". Так, толкали друг друга в грудь. А вот теперь — война».

В этом его тоже поддерживает Здольников. «Сейчас в российском *IT*-сообществе происходит тяжелый процесс смирения, который можно наблюдать в профильных чатах, — констатирует специалист. — Несколько лет никто не хотел верить, что власти дойдут до этого, и почти никто не хотел изучать новые для себя инструменты, но теперь осознание необходимости приходит».

Он думает, что протоколы *OpenVPN* и *Wireguard* будут заблокированы, а значит, почти все сервисы, которые оставались незамеченными Роскомнадзором, теперь будут недоступны для пользователей из России. Он добавляет, что в *RedShield VPN* давно начали работать над способами замаскировать *VPN* под какой-нибудь другой вид трафика: с точки зрения анализа данных Роскомнадзором это выглядит, как будто пользователь открывает обычный разрешенный сайт.

Редактор: Дмитрий Трещанин

Обновлено в 19:03. Добавлен комментарий *ValdikSS*.

1. Сейчас комментарии к публикации скрыты.