meduza

РАЗБОР

# **Какие VPN самые надежные? Как понять, что сервис сотрудничает со спецслужбами? Могут ли Россию вообще отключить от нормального интернета?** Эксперты отвечают на вопросы читателей «Медузы» о VPN

06:00, 29 июля 2022 · Источник: Meduza

Ссылка на материал

Это PDF-версия материала, опубликованного на «Медузе». Вы можете отправить этот файл в любом мессенджере или по электронной почте вашим близким в России, особенно тем, кто не умеет обходить блокировки. Вы можете также распечатать этот текст и показать его тем, кто не пользуется интернетом.

«Медуза» признана «нежелательной» организацией на территории РФ, поэтому, пожалуйста, будьте осторожны и делитесь нашими материалами только с теми, кому доверяете.

Подробнее о «нежелательном» статусе.

Самый удобный способ читать «Медузу» без VPN — это скачать наше приложение. Оно работает в России, несмотря на блокировку, и это абсолютно безопасно. Версия для iOS и для Android. Приложение на Android также можно скачать по прямой ссылке. Устанавливайте приложение не только себе, но и близким!

Более 800 читателей «Медузы» откликнулись на призыв задать любые вопросы о технологии VPN. Мы отобрали те из них, что касаются блокировки VPN-сервисов в России, и задали их профессионалам. На вопросы[1] отвечали **Вадим Мисбах-Соловьев**, технический специалист «Роскомсвободы» и криптоэнтузиаст, **Станислав Шакиров**, основатель Privacy Accelerator, а также **ValdikSS**, основатель проектов для обхода блокировок GoodbyeDPI и «АнтиЗапрет».

---

## Сначала кратчайшая инструкция по тому, как решать проблемы с VPN

1. Если VPN перестал работать, попробуйте поиграть с настройками: переключить протокол[2] или включить режим обфускации.[3]
2. Все еще не работает? Обратитесь в службу поддержки своего сервиса VPN.
3. Подождите несколько дней: возможно, перебои пропадут благодаря усилиям вашего сервиса.
4. Если ничего не помогло, попробуйте поискать другой VPN.

5. Не забудьте поставить Tor, Psiphon и Lantern — программы, специально созданные для обхода блокировок.

ВОТ ЕЩЕ ДВА ТЕКСТА, КОТОРЫЕ МОГУТ ВАМ ПРИГОДИТЬСЯ

**Мой VPN перестал работать. Что делать? Как искать работающий?** Максимально короткая инструкция «Медузы»

**«Медуза» заблокирована в России. Мы были к этому готовы — и продолжаем работать** Отправьте этот материал тем, у кого нет доступа к нашему изданию (пояснения внутри)

Они же в гугл-доке (про то, как читать заблокированные ресурсы, и про то, что делать, если VPN не работает).

ЧАСТЬ 1

# Как устроены блокировки и как понять, что ваш VPN заблокирован

## Насколько технически сложно заблокировать VPN? Мне казалось,

## это решается только файерволом[4], как в Китае

**Коротко.** Возможно — обычно достаточно заблокировать IP-адреса сервиса.

**ValdikSS.** Конкретный VPN-сервис заблокировать просто: достаточно заблокировать IP-адреса серверов этого сервиса, чтобы клиент не мог к ним подключиться. Если сервис не имеет широкого пула IP-адресов, не меняет (не ротирует) серверы для затруднения их выявления и блокировки, а также не применяет различные ухищрения против цензуры, то блокировка по IP — вполне надежная мера, которая значительно или полностью заблокирует возможность подключения к сервису.

Блокировки по IP-адресам реализуются на провайдерских сетевых маршрутизаторах[5], для этого не требуется какого-либо дополнительного оборудования, вроде файрволов[6] или систем Deep Packet Inspection[7].

**Вадим Мисбах-Соловьев.** С точки зрения оборудования если трафик можно как-то определить, то его можно и заблокировать. В случае VPN-сервисов достаточно даже понимания, что адрес сервера,

на который уходит ваш трафик, принадлежит компании, на сайте которой написано «предоставляем услуги доступа к нашему VPN». Достаточно просто предоставить ТСПУ[8] список адресов, чтобы оборудование принимало решение о блокировке.

---

## Подробный ответ экспертов «Роскомсвободы» и Privacy Accelerator

Дело в том, что «файрвол», «браундмауэр», «фильтр трафика» и прочие подобные слова означают одно и то же: программное или аппаратно-программное решение, задача которого — диагностика проходящего трафика и принятие решений (на основе заданного списка правил) о пропуске этого трафика, его блокировке или иных действиях (включая добавление искусственных задержек или подмену ответа).

Так что можно сказать, что именно «файрволом» блокировки и осуществляются. Причем в два «слоя».

Во-первых, практически у каждого интернет-провайдера и так стоит подобное оборудование, которое он использует для своих целей (вроде приоритизации некоторых типов трафика, контроля пропускной способности абонента, учета его трафика или других целей). И первоначально функцию блокировки

возложили именно на провайдеров. И осуществляют они ее именно на своем оборудовании.

Чтобы понять, как это работает, немного отступим от темы VPN-сервисов и рассмотрим блокировки как таковые (то есть включая блокировки HTTP-сайтов).

Раз в определенный промежуток времени провайдеры скачивают список заблокированных ресурсов (IP, домены, HTTP URL) и блокируют теми средствами, которыми умеют. Именно поэтому некоторые блокируют по IP, полностью лишая доступа к удаленному серверу, а некоторые, имея более дорогое оборудование с функциональностью DPI[9], блокируют конкретные страницы в незашифрованном HTTP-трафике[10] и даже подменяют его.

Чтобы обезопасить пользователей и защититься от манипуляций трафиком, сайты переходят на использование шифрованной версии HTTP, которая называется HTTPS (S = Secure). В случае ее использования максимум, что умеет оборудование для блокировок, — узнать домен сайта, который вы запрашиваете с сервера. Но и эту проблему постепенно решают, и однажды в браузерах будут приняты обновления (этот вопрос политический — многие государства против этого), которые закроют лазейку.

Приблизительно так же оборудование может блокировать трафик VPN-сервисов и даже мессенджеров.

---

Вторым «слоем» блокировок является пресловутая система ТСПУ (оборудование, которое навязали для установки всем провайдерам).

Несмотря на название (технические средства противодействия угрозам), используется это оборудование не для противодействия угрозам, а для блокировки.

Причем если блокировки «первого слоя» происходят на базе относительно публичного реестра, а также на оборудовании провайдеров, которое не всегда достаточно мощно для полноценного анализа *всего* проходящего через него трафика, то в случае со «вторым слоем» дела обстоят иначе. Во-первых, ТСПУ — это комплекс из кучи довольно мощного оборудования (что дает очень широкие возможности на поле блокировки трафика), а во-вторых (и это самое главное), это оборудование — «черный ящик» даже для самих провайдеров. То есть непонятное неподконтрольное устройство, которое само что-то делает, и максимум, что

ты можешь видеть, — что в него поступает и что из него выходит. Повлиять на него нет возможности.

Это приводит к тому, что блокировки на ТСПУ мы можем «чувствовать» на себе, а Роскомнадзор при этом может с «покер-фейсом» заявлять, что никаких блокировок не осуществляется: «Вот, смотрите в реестр, видите, там их нет, так что вы тут фейк-ньюс распространяете». По факту же трафик до заблокированных (в обход реестра) ресурсов подменяется или «срезается» на ТСПУ.

На ТСПУ, не попадая в публичный реестр, блокируются не только VPN-сервисы. Так же происходило, например, с Google Docs, Play Market и YouTube. По сообщениям пользователей «Роскомсвободы», они до сих пор иногда сталкиваются с тем, что сервер YouTube, отвечающий за аватарки пользователей и каналов, а также рекламу, блокируется на ТСПУ, хотя Роскомнадзор уверял в обратном.

---

## Как провайдер видит использование VPN? И видит ли вообще? Может ли он определять использование VPN по тому, какие данные пересылаются?

**Коротко.** Иногда провайдер явно видит, что его клиент использует VPN. Но данные, которые просматривает пользователь, провайдеру недоступны.

**Вадим Мисбах-Соловьев.** Все зависит от технологии VPN.

Некоторые протоколы притворяются HTTPS-трафиком либо используют специальные дополнительные программы-обфускаторы, которые маскируют их трафик под HTTPS. Соответственно, DPI-оборудование (и более простое фильтрационное оборудование) это видит так, будто вы обмениваетесь кучей информации с каким-то сайтом.

Но теоретическая возможность отличить такой трафик от использования настоящего сайта есть. Просто требует ощутимо больше усилий для анализа, поэтому никто этим не занимается.

Те технологии VPN, которые не притворяются HTTPS (или не используют его непосредственно), для оборудования выглядят просто как зашифрованный трафик между вами и удаленным сервером (который все еще можно проверить на принадлежность к компании, предоставляющей услуги доступа к VPN). Либо, если технология не использует шифрование, трафик будет полностью открыт для фильтрационного оборудования,

и оно сможет анализировать его содержимое так же, как если бы трафик проходил через него напрямую, без VPN.

**ValdikSS.** Кратко: не все протоколы скрывают факт использования VPN, но шифрованное содержимое недоступно провайдерам. А значит, блокировать сайты и сервисы, открываемые через VPN, у провайдеров возможности нет.

---

## Подробный ответ ValdikSS

Существует, условно, три типа протоколов туннелирования трафика: стандартные, распространенные и специализированные под блокировки.

Стандартные протоколы, такие как IPsec, PPTP и L2TP, разработаны прежде всего для использования в корпоративной среде: они применяются повсеместно и поддерживаются всем промышленным оборудованием. Их используют для объединения офисов в единую сеть, удаленного подключения сотрудников и подобных задач. Эти протоколы провайдеру видны как на ладони: они полностью документированы в виде стандарта, работают по фиксированным портам, имеют четкую структуру пакетов и не скрывают информацию о VPN-подключении — провайдер может легко

обнаружить факт подключения без дополнительного оборудования и увидеть некоторую служебную информацию, например, о типе аутентификации.

Что не видно провайдеру, так это содержание передаваемых данных внутри туннеля — оно шифровано (но не в протоколе L2TP — для защиты его используют совместно с IPsec).

Заблокировать эти протоколы легко, для этого не требуется дополнительного оборудования — достаточно заблокировать порты, используемые протоколами.

К «распространенным» можно отнести широко используемые, но не задокументированные в виде стандарта протоколы OpenVPN, WireGuard, Cisco AnyConnect, Juniper SSL VPN и тому подобные.

Для их блокировки потребуется больше усилий и более дорогое оборудование, но это вполне посильная задача — они не спроектированы для защиты от фильтрации и имеют характерные признаки, выделяющие их среди остального трафика. Даже специализированные опции в OpenVPN, затрудняющие анализ, скрывают только часть информации, но не формат и характерную последовательность отправки пакетов при подключении.

Заблокировать эти протоколы возможно оборудованием DPI — оно определит характерные признаки VPN и завершит (либо замедлит, либо заставит зависнуть — зависит от настроек) соединение. Это однозначно возможно реализовать оборудованием ТСПУ в России.

Третий вид — протоколы, спроектированные под обход блокировок, такие как Shadowsocks, V2Ray vmess, Trojan, Cloak и другие (все это — прокси, но в контексте обхода блокировок разница между прокси и VPN не столь важна).

Эти протоколы созданы для максимального усложнения их автоматизированного обнаружения. Сами протоколы не имеют значимых характерных признаков, по которым их можно обнаружить, но бывают ошибки и огрехи в конкретных программах, которые с большой долей достоверности позволяют определить наличие туннеля, — подобные ошибки выявляются и закрываются разработчиками.

Также бывают характерные особенности языков программирования и их библиотек, а не самих протоколов — так, V2Ray, написанный на языке Go, заблокирован по характерным признакам TLS (протокола для защищенной передачи данных в интернете) у одного из провайдеров Туркменистана, и эта блокировка затрагивает все программы на этом языке программирования. Выход есть: существуют

библиотеки, имитирующие набор сетевых протоколов Chrome и Firefox, — блокировка их характерных признаков приведет к неработоспособности браузеров.

В части случаев провайдер может определить тип передаваемого трафика статистическими методами, не зная его содержимого: если ваш мобильный телефон продолжительно и равномерно передает и принимает пакеты небольшого размера с низкой скоростью, с большой долей вероятности это говорит о совершении звонка через мессенджер. Кроме того, Shadowsocks, например, не скрывает протокол трафика — TCP передается через TCP, UDP — через UDP, — что добавляет точности статистическим методам.

Блокировку характерных признаков отдельных программ и библиотек мы уже видели в России на примере альтернативного ютьюб-клиента NewPipe — попытки открыть www.youtube.com в этой программе блокировались на оборудовании ТСПУ, при этом сайт без проблем открывался через браузер.

---

## Как понять, что мой VPN действительно заблокирован? Вдруг это просто технические проблемы VPN-сервиса?

**Коротко.** Это не так просто понять самому, поэтому проще обратиться в службу поддержки вашего VPN-сервиса.

**ValdikSS.** Это бывает нетривиальной задачей даже для специалистов, и вот почему: серверы VPN-сервисов блокируют на оборудовании ТСПУ[11], не добавляя их в единый реестр запрещенных сайтов — официальный сайт Роскомнадзора не покажет вам факт блокировки, даже если вы знаете IP-адрес VPN-сервера или технический домен сервиса.

Например, приложение заблокированного ProtonVPN обращается к https://api.protonvpn.ch для скачивания информации о серверах. В реестре этот адрес не числится, но и не открывается на провайдерах с системой ТСПУ.

Вариантов два: либо для проверки воспользоваться VPN с сервером в России, на котором отсутствуют блокировки сайтов, либо попробовать использовать альтернативы VPN — автономные способы обхода, такие как GoodbyeDPI, zapret и DPI Tunnel. Эти программы изменяют трафик и добавляют поддельные пакеты, чтобы обдурить систему DPI без использования туннелей[12].

**Станислав Шакиров.** Простому пользователю это понять невозможно. Любая диагностика без специализированных инструментов, которыми пользуются системные администраторы, может носить только вероятностный характер.

Даже проверка такими инструментами, в силу особенностей работы ТСПУ, не может дать точного ответа, что имеет место именно блокировка конкретного сервиса, а не проблемы у провайдера, которые он не признает, или «ковровая бомбардировка» другого ресурса, под которую случайно попал нужный вам.

Самый действенный вариант:

1. Проверить работу сервиса из нескольких стран. Для этого могут подойти или арендованные виртуальные серверы (более точный ответ — но способ требует трат и знаний в IT), или сервисы проверки доступности (менее точный ответ, но способ бесплатный и относительно простой).
2. Написать письмо в службу поддержки самого сервиса и спросить, не наблюдается ли у них проблем (и попробовать попросить помощи).

## Если конкретный VPN оказался заблокирован, имеет ли смысл ждать

## обхода его блокировки со стороны разработчиков?

**Коротко.** Иногда ждать бессмысленно. Лучше всего спросить в службе поддержки VPN-сервиса, планируют ли они обходить блокировку.

**ValdikSS.** Все зависит от технической компетенции и желания сервиса предоставлять доступ в конкретном регионе. Роскомнадзор не особенно тщательно блокирует серверы и не спешит актуализировать информацию. Так, простая программа для перебора IP-адресов узлов в поисках рабочего позволяет подключиться к сети Tor в течение 30 секунд в 100% случаев: блокируются 60–70% промежуточных узлов, но остальные 30–40% остаются доступными; похожая ситуация с ProtonVPN — администрация изменила IP-адреса части серверов, и они снова доступны, пусть и не по всем протоколам.

**Вадим Мисбах-Соловьев.** Однозначного ответа нет. Некоторые сервисы заинтересованы в попытках обхода блокировок. Некоторые нет. Например, если для них затраты на обход блокировок превышают доход от сервиса.

Лучшим способом опять же будет спросить в службе техподдержки, планируют ли они что-то предпринимать

в связи с блокировкой или им это неинтересно.

## Почему в мобильных сетях VPN блокируется гораздо чаще и эффективнее, чем при проводном подключении?

**Коротко.** Потому что пока не у всех проводных операторов стоит специальное оборудование для блокировки. Мобильные сети таким оборудованием охвачены полностью.

**ValdikSS.** Потому что во всех мобильных сетях установлены системы ТСПУ[13], а у мелких проводных провайдеров они присутствуют не везде. К 2023 году ситуация может измениться — закон предписывает установку ТСПУ у всех провайдеров с 1 января.

**Вадим Мисбах-Соловьев.** Потому что у всех мобильных операторов трафик ходит через ТСПУ. И у них и без этого стоит очень много DPI-оборудования, одна из функций которого — блокировка.

А у проводных операторов (которых пока еще истребили не всех) бывают разные наборы оборудования, настроенные по-разному, да и сами они могут

использовать разных магистральных провайдеров с разными условиями.

И если у вас интернет не от условных «Дом.ру» или «Ростелекома» (а также не от «проводных» подразделений мобильных операторов) и никто из них до сих пор не купил вашего провайдера, то есть шанс, что у него не установлено ТСПУ, а реестровые блокировки он выполняет каким-нибудь кустарным способом.

## Какого типа DPI-оборудование установлено у крупных провайдеров и операторов «большой тройки»?

**Коротко.** Собственное оборудование для блокировки трафика и оборудование Роскомнадзора. Второе блокирует домены и серверы даже вне единого реестра запрещенных ресурсов.

**ValdikSS.** Типичная конфигурация крупного провайдера России по состоянию на лето 2022-го следующая: система ТСПУ[14] Роскомнадзора плюс DPI[15], который использовался до внедрения ТСПУ. Используются две (иногда и более) системы одновременно.

ТСПУ задумывался в качестве гибкой системы с разнообразными функциями, но пока используется

исключительно для блокировок.

Стандартное оборудование DPI блокирует только ресурсы из единого реестра запрещенных ресурсов, а ТСПУ — и из реестра, и дополнительные домены/протоколы/сервисы вне реестра. В отличие от стандартного DPI, который настраивается и управляется провайдером, ТСПУ управляется исключительно Роскомнадзором, у провайдера нет доступа к настройкам.

**Станислав Шакиров.** Известно, что в качестве ТСПУ у операторов стоит EcoDPI от компании RDP. Эта система — активный DPI, то есть может блокировать или подменять трафик.

## А если перекроют VPN, то граждане РФ за рубежом не смогут подключиться с его помощью к российским сервисам?

**Коротко.** Смогут, если нужные сайты не блокируют зарубежный трафик или у VPN есть российские серверы.

**Вадим Мисбах-Соловьев.** Прямой связи между этими событиями нет. Все зависит от конкретных VPN-сервисов и того, как у них построены сети.

Для того чтобы через VPN-сервис можно было зайти на российские сайты, должно выполняться какое-то из этих условий:

- у сервиса разные серверы для подключения к сети и для выхода из нее в интернет, при этом адрес сервера для выхода не заблокирован на целевом сайте (в том числе по географическому признаку);
- у сервиса сложная система маршрутизации трафика в зависимости от назначения и есть серверы выхода, расположенные в России, а трафик до российских сайтов выходит через них (или есть возможность это настроить).

**ValdikSS.** С VPN борются только в контексте обхода блокировок, сами туннели не запрещены в России. Например, Kaspersky VPN Secure Connection сотрудничает с Роскомнадзором и не позволяет заходить на заблокированные в РФ сайты.

Кроме того, ТСПУ различает направление подключения (из РФ или в РФ), так что технически даже при автоматических блокировках возможна настройка оборудования на подключение внутрь России.

ЧАСТЬ 2

# Сотрудничество с властями, силовики

## Можно ли узнать, почему вновь заработал заблокированный VPN: согласился сотрудничать с властями или научился обходить блокировки?

**Коротко.** Нет, но у администрации VPN-сервиса можно спросить об этом напрямую.

**Вадим Мисбах-Соловьев.** Наверняка — нельзя. Даже в случае некой договоренности стороны могут не признаться в этом. Проверить их довольно проблематично в принципе и совсем уж невозможно для обычного пользователя.

Можно напрямую спросить об этом в службе поддержки VPN-сервиса и, опираясь на ответ, сформировать свое мнение на основе опыта и интуиции.

**ValdikSS.** Самый простой вариант — задать вопрос администрации сервиса. Подавляющее их большинство охотно идут на контакт и рассказывают о проделанной

работе как публично в блогах, так и клиентам по запросу, ведь практически все они предоставляют сервис обхода цензуры и региональных блокировок, а не только VPN как таковой.

## Какова вероятность, что хотя бы за одним крупным VPN-сервисом стоят люди в погонах?

**Коротко.** Это сложно оценить.

**Вадим Мисбах-Соловьев.** Учитывая историю компаний [Евгения и Натальи] Касперских и их сотрудничества с обладателями погон, а также истории с Tor[16], такая вероятность существует, но оценить ее нет никаких возможностей.

Что касается крупных VPN-сервисов, нужно смотреть, кто основатели и в каких странах зарегистрирован сервис. Также стоит почитать отзывы на Reddit. Обычно за крупными иностранными сервисами не стоят российские «ребята в погонах».

ЧАСТЬ 3

# Корпоративные VPN, прокси, Lantern

## Что будет с VPN, которые компании используют не для обхода блокировок, а для связывания офисов в единую сеть?

**Коротко**. Скорее всего, они будут работать.

**ValdikSS.** Мой прогноз следующий: трафик внутри страны (Россия — Россия) будет фильтроваться минимально или не будет вообще, а стандартные протоколы VPN за рубеж не будут блокироваться, по крайней мере в автоматическом режиме.

**Вадим Мисбах-Соловьев.** Однозначно ответить нельзя, все зависит от того, какие именно технологии используются.

У одних сервисов вероятность пострадать (в качестве «побочного урона» от борьбы с сервисами, предоставляющими доступ к своим VPN для обхода блокировок) довольно мала. Например, шанс, что пострадают сети на базе Cisco AnyConnect, достаточно низок.

У других, например на базе WireGuard или OpenVPN, шанс выше. Но все равно есть варианты «подстелить солому» и уменьшить вероятность блокировки конкретной сети. Тут уже дело за администратором, который ее обслуживает.

Также гипотетически возможно введение «белых списков» [17]корпоративных VPN — по примеру того, как это работает в Китае.

## Правда ли, что власти не блокируют VPN по-настоящему из-за того, что многие бизнесы используют эти протоколы для корпоративной связи?

**Коротко.** Да, корпоративные клиенты действительно, возможно, спасают Россию от массовой блокировки VPN.

**ValdikSS.** Полагаю, что это основной фактор.

**Станислав Шакиров.** Да, риски для корпоративных клиентов — одна из причин, почему уже сейчас не началась массовая блокировка VPN. Но с этим работают, это решается «белыми списками», и это дело

времени. Полагаться на то, что именно из-за возможной поломки корпоративных каналов не заблокируют все остальное, точно не стоит. Когда будет на то политическая воля, не будут особо церемониться ни с кем. Все это уже обкатано в Китае.

Другой вопрос, что полностью заблокировать все VPN нельзя, всегда будут протоколы, которые работают.

## Такие провайдеры, как Psiphon или Lantern, обещают, что их трафик неблокируем. Почему остальные не идут тем же путем?

**Коротко.** Это действительно надежные сервисы с широким набором функций для обхода блокировок, но все же заявления о «неблокируемости» — преувеличение.

**ValdikSS.** Я не встречал таких заявлений от авторов этих программ, но они действительно созданы с расчетом на работу в условиях блокировки. Частичную блокировку Psiphon мы видели в России в декабре 2021 года, Lantern — в мае — июне, причем попытка блокировки Lantern привела к недоступности многих адресов крупной хостинг-площадки DigitalOcean.

Могу сказать про Psiphon: программа имеет встроенные методы обфускации, использует технологию domain fronting[18], мимикрирования под другие протоколы, получения списка серверов через дополнительные каналы и умные методы поиска рабочего способа подключения.

Из интересных особенностей Psiphon можно отметить поддержку Refraction Networking — особого протокола туннелирования, сервер для которого устанавливается у зарубежного провайдера прямо на транзитных каналах связи. Такой метод позволяет превратить любой чужой сайт в прокси[19], если данные каким-либо образом проходят через провайдеров с установленной технологией, что еще сильнее усложняет жизнь цензорам.

**Вадим Мисбах-Соловьев.** В определенном смысле это маркетинговый трюк, основанный на недосказанных допущениях. Суть в том, что они используют элементы так называемой технологии mesh[20]. Суть этой технологии — в том, что, условно, все участники общаются со всеми. И даже если большинство путей между ними заблокировано, но есть хоть один незаблокированный, трафик найдет его и пойдет по нему. Конкретно у этих сервисов все немного сложнее, но основа идеи такая.

Однако все зависит от того, насколько сильно тем, кто блокирует, хочется заблокировать конкретный сервис. А также от того, насколько сервис готов к активному противодействию. Теоретическая возможность заблокировать что угодно существует всегда. Вопрос — в компетенции и затраченных ресурсах.

## Есть успешный опыт борьбы против цензуры с помощью mesh-сетей?

**Коротко**. Вроде бы нет. Для массового пользователя это сложная технология.

**ValdikSS.** Мне о таком неизвестно. На Кубе используются mesh-сети, но для обмена файлами и онлайн-игр.

**Вадим Мисбах-Соловьев.** Примеры борьбы с блокировками mesh-сетей единичные и остаются на уровне энтузиастов. Большинство обычных пользователей не осилит настоящие mesh-сети. К тому же чем больше людей будут про них знать, тем быстрее узнают и те, кто блокирует, — и начнут блокировать узлы mesh-сетей, усложняя подключение новых пользователей.

## Почему все еще работают расширения для браузеров, которые перенаправляют запросы для заблокированных сайтов на прокси-серверы[21]? Насколько они безопасны?

**Коротко.** Роскомнадзор просто еще не взялся за них — технические возможности блокировки у властей есть. С безопасностью могут быть проблемы.

**ValdikSS.** Заблокировать прокси-серверы не составит Роскомнадзору никакого труда: браузерные расширения сильно ограничены в возможностях и не могут использовать методы обфускации или нестандартные протоколы. Тем не менее в случае блокировки авторы расширений могут сменить IP-адреса или домены серверов в автоматическом режиме, без необходимости обновления расширения.

С безопасностью этих расширений бывает по-разному: какие-то достаточно примитивны и только меняют настройки сервера, другие ранее вмешивались в содержимое страниц и «отбирали» кешбэк в интернет-магазинах. Политика относительно прокси-расширений

в каталогах Chrome и Firefox не позволит встроить совсем уж вредоносный код, но бывают нюансы.

**Вадим Мисбах-Соловьев.** Работают они в большей степени потому, что:

- за прокси-серверами идет не такая сильная охота, как за VPN-сервисами;
- при определенной настройке отличить (на блокирующем оборудовании) зашифрованный прокси-трафик от HTTPS очень сложно; скорее, даже невозможно;
- ну и «жонглировать» ими в выдаче клиентам, то есть менять один на другой в случае блокировки, все же легче, чем в случае VPN-сервисов.

А вот с безопасностью «в среднем по больнице» все плохо. Очень много таких расширений гоняют незашифрованный прокси-трафик, и блокирующее оборудование в подобных случаях может его анализировать, вмешиваться в него и подменять (осуществляя блокировки).

В случаях, когда такие расширения используют только зашифрованное соединение с прокси-сервером (как, например, Censor Tracker от «Роскомсвободы»), для оборудования это выглядит практически как HTTPS-трафик. Соответственно, нет возможности понять, что это прокси, и заблокировать. Тут возможны только

целевые атаки со стороны блокировщиков на конкретные сервисы (и попытка «душить» их серверы).

---

### Вадим Мисбах-Соловьев. Важное соображение про безопасность

Даже если с прокси-сервером или с сервером VPN-сервиса идет зашифрованный обмен трафиком, нужно помнить, что владельцы этих серверов могут анализировать ваш трафик. И точно так же имеют теоретическую возможность модификации незашифрованного трафика, идущего внутри зашифрованного туннеля (защищенного от вторжения со стороны провайдера и блокирующего оборудования).

А значит, подобно тому, как это делает «Ростелеком» и вроде бы все или как минимум большинство мобильных операторов, владелец сервера может подменять и даже вставлять свою рекламу в HTTP-трафик[22] (если вы заходите на сайт, у которого нет HTTPS). А еще у него есть теоретическая возможность красть пароли. В случае некоторых VPN такая возможность может быть не только у владельцев, но и у других пользователей, которые подключены к тому же серверу.

Так что, если вам важна безопасность и приватность, нужно следить за наличием шифрования на каждом этапе:

- между вами и сервером, через который подключаетесь к VPN;
- между вами и целевым сервером, к которому подключаетесь, пропуская трафик через VPN;
- в случае если сеть (VPN) построена так, что «входной» и «выходной» узлы разные — чтобы обмен трафиком между ними тоже шел по зашифрованному каналу. Вы не можете это контролировать напрямую или влиять на это, но это тоже важно, если вы криптопараноик.

---

ЧАСТЬ 4

# Какие протоколы VPN эффективнее

## Может ли РКН блокировать такие протоколы, как WireGuard, OpenWeb, Stealth VPN, SoftEther, VLess и Xray?

## A Stunnel + OpenVPN или Shadowsocks + OpenVPN?

**Коротко.** Может, но точно не все.

**ValdikSS**. WireGuard — однозначно да, с остальными сложнее.

Система ТСПУ[23] обладает гибким движком блокировок с динамическими правилами, которые позволяют постоянно или временно блокировать доступ к определенным адресам или портам после срабатывания определенного события. Это может быть использовано для определения OpenVPN внутри другого туннеля, например Stunnel, с довольно высокой степенью достоверности.

Относительно Shadowsocks, Vless и Xray — скорее нет, чем да. Эти протоколы не позволяют идентифицировать туннель, заблокировать их можно только ценой блокировки всех шифрованных неидентифицируемых протоколов.

---

### Существует ли технология VPN over HTTPS «из коробки» — без дополнительных настроек? Насколько сложно блокировать такой трафик, замаскированный под HTTPS или TLS?

**Коротко.** Придется настраивать.

**ValdikSS.** Промышленные решения не маскируются под HTTPS, потому что это негативно влияет на скорость, особенно для VPN, где весь трафик туннелируется через одно TCP-соединение. Поэтому для VPN чаще всего используются протоколы поверх UDP. Протокол HTTP/3, недавно стандартизированный, использует протокол QUIC, работающий поверх UDP, — возможно, через несколько лет мы увидим внедрение VPN over QUIC. Однако в России он частично блокируется.

Протоколов прокси over HTTPS в достатке: NaïveProxy, Cloak, Trojan, v2fly vless. Их можно использовать и для туннелирования VPN, как минимум OpenVPN TCP.

## Протоколы Iodine (технология VPN over ICMP[24]) работают даже в Китае. Какие VPN-сервисы используют этот протокол и другие аналогичные варианты (например, DNS[25])?

**Коротко.** VPN-сервисы, использующие такие протоколы, встречаются редко, они сложны в настройке и работают

медленно.

**ValdikSS.** Коммерческих решений подобного рода мало, потому что VPN over ICMP непрактичен в настройке и не работает через прокси-серверы, а VPN over DNS обычно работает медленно (есть только одна быстрая реализация, которая появилась в апреле 2020-го, — dnstt, но ее скорость на порядок ниже классических туннелей).

Преимущество DNS-туннеля заключается в возможности переиспользования публичной инфраструктуры DNS как промежуточного узла — резолверы[26] предоставляет Google, «Яндекс», Cloudflare и множество других IT-компаний, интернет-провайдеров и сетевых энтузиастов. Если заблокировали один, можно попробовать использовать другой.

Этим же преимуществом обладает так называемое проксирование через CDN[27], которое позволяет «привязать» множество IP-адресов и доменов к одному VPN-серверу: это и дешево (домены стоят 1–3 доллара в год), и эффективно маскирует трафик, и затрудняет работу цензора.

## Подробный обзор VPN-протоколов по критериям устойчивости к блокировкам РКН от экспертов

## «Роскомсвободы» и Privacy Accelerator

Протокол **L2TP** — один из самых старых VPN-протоколов, но на этом его преимущества заканчиваются. Его очень просто обнаружить и заблокировать.

**IKEv2** — это протокол, разработанный Microsoft и Cisco и стандартизированный в RFC[28]. Использует те же порты, что и L2TP, и так же легко блокируется.

Протокол **OpenVPN** имеет два режима работы: по TCP и по UDP. Чаще всего используется режим работы по UDP, так как он имеет более высокую скорость и лучше работает на мобильных устройствах. OpenVPN в режиме UDP достаточно просто определяется и блокируется средствами DPI. OpenVPN в режиме TCP использует для соединения технологию TLS, также пригодную для передачи web-трафика, что затрудняет его блокировку средствами DPI, но тем не менее он тоже может быть заблокирован.

Нужно добавить, что существуют модификации OpenVPN (например, xor patch), которые затрудняют его обнаружение. Эти технологии начали разрабатываться в Китае еще на заре становления файрвола, поэтому OpenVPN с патчами неплохо обходит блокировки DPI.

Такие реализации можно найти во многих коммерческих VPN, по большей части ориентированных на Китай и другие страны Азии.

Протокол **WireGuard** заблокировать тоже очень просто — это стандартизированный протокол с выраженными сигнатурами (отличительные признаки, достаточные для идентификации, — аналог почерка или отпечатков пальцев). WireGuard изначально был спроектирован на максимальную скорость работы и минимальное потребление ресурсов (при достаточном уровне шифрования), без учета вопросов гибкости и устойчивости к блокировкам.

Протокол **Shadowsocks** — это «почти» VPN-протокол, технически это протокол Socks Proxy. Он достаточно сложен для блокировки по DPI ввиду того, что разработчики добавили поддержку Pluggable Transport — подключаемых и взаимозаменяемых программ, обеспечивающих транспортировку, шифрование и обфускацию (маскировку) трафика.

**SoftEther** — это проект с открытым исходным кодом, программное обеспечение для создания self-hosted VPN-решения (то есть для самостоятельной установки VPN на своем сервере), которое можно настроить на работу по многим популярным протоколам (L2TP/IPsec, OpenVPN, SSTP), а также по собственному VPN-протоколу SSL-VPN, который, по заявлениям авторов,

неотличим от обычного HTTPS-трафика. Утверждается, что SoftEther достаточно устойчив к блокировкам VPN по DPI. Проект имеет хорошую репутацию, но сложный интерфейс и рассчитан на профессионалов.

---

Также существует множество проприетарных VPN-протоколов с закрытыми или частично открытыми исходными кодами. Разработчики чаще всего основывают эти протоколы на OpenVPN путем его модификации, но существуют и VPN-протоколы, созданные с нуля. Вот некоторые из них.

**Stealth VPN** — закрытый VPN-протокол от компании Astrill. Вероятно, является доработкой OpenVPN, которая снижает его видимость для средств DPI.

**OpenWeb** — еще один закрытый VPN-протокол, который используется OpenWeb VPN от Astrill. На сайте OpenWeb указано, что этот протокол маскирует VPN как трафик HTTP и HTTPS и его трудно заблокировать с помощью автоматических систем брандмауэров и DPI. Так как протокол закрытый, отсутствует возможность использовать его для сторонних или собственных VPN-решений. Отсутствует и какая-либо публичная информация о пройденных Astrill аудитах безопасности, в том числе безопасности самого протокола.

**Lightway** — это VPN-протокол, разработанный компанией ExpressVPN. Lightway разработан полностью с нуля и оптимизирован для работы на мобильных устройствах, имеет режимы работы по UDP и TCP и, по утверждению авторов, спроектирован так, чтобы к нему было легко подключать плагины для защиты от DPI. К сожалению, в публичный доступ выложена только часть lightway-core (часть протокола, обеспечивающая основной функционал без «излишеств» в виде маскировки трафика), а детали реализации плагина, отвечающего за маскировку VPN от DPI, не опубликованы и являются коммерческой тайной. Сам протокол lightway-core успешно прошел аудит безопасности.

**NordLynx** — это VPN-протокол, разработанный компанией NordVPN на базе протокола WireGuard. Судя по информации на сайте NordVPN, доработки направлены на повышение приватности VPN-сессий, таким образом NordLynx не имеет повышенной устойчивости к DPI по сравнению с WireGuard.

Нужно подчеркнуть, что речь идет об устойчивости VPN-протоколов к DPI. Но, как показывает практика, в частности ситуация по коммерческим VPN-сервисам, устойчивости VPN-протокола к DPI чаще всего недостаточно для избежания блокировки надзорными органами. Могут быть применены самые простые блокировки VPN-серверов по их адресам или сложные

блокировки управляющих серверов — тут уже не имеет значения, какой протокол использован.

---

Помимо VPN-протоколов, существуют еще различные плагины и утилиты, которые позволяют обфусцировать трафик самих протоколов.

В таком случае для DPI не важно, какой используется внутренний протокол — например, связки протоколов OpenVPN over Stunnel и WireGuard over Stunnel определяются одинаково.

Самые распространенные плагины и утилиты последних поколений — **Stunnel**, **V2Ray**, **Cloak**. Также существует множество устаревших и менее популярных плагинов. Такие плагины разрабатываются специально для маскировки от блокировок VPN по DPI, поэтому показывают высокую эффективность по маскировке. Большинство разрабатывается китайскими энтузиастами, поэтому можно утверждать, что если их не могут заблокировать в Китае, то в России и подавно не смогут.

---

Стоит отдельно упомянуть и VPN-протоколы, маскирующиеся не под web-трафик, а под такие протоколы, как ICMP и DNS (например, **Iodine**). Такие протоколы успешно обходят DPI, но только по той причине, что имеют крайне низкое распространение. Как утверждают специалисты, при желании их легко заблокировать по критерию аномально большого количества трафика, идущего по ICMP или DNS.

---

Альтернативой коммерческим VPN являются так называемые self-hosted VPN-решения. Self-hosted VPN — это VPN-сервис, который пользователь устанавливает на собственном виртуальном сервере, следовательно, этот сервер нужно сначала приобрести. Традиционно эта сфера считалась прерогативой IT-специалистов, так как требовала определенного уровня знаний, чтобы установить на сервер все необходимое и настроить его. Но с течением времени ситуация менялась, появлялось все больше средств автоматизации этого процесса. Можно выделить два поколения таких утилит автоматизации.

Первое поколение — это такие утилиты, как **StreisandEffect**, **AlgoVPN**. Это консольные утилиты, которые упрощают установку сервера до уровня введения в консоль одной команды. Такой подход имеет

существенный недостаток, так как требует от пользователей минимальных навыков работы с консолью.

Утилиты второго поколения — Outline и Amnezia VPN. Это полноценные *out of the box* VPN-клиенты («из коробки» — то есть не требующие длительной настройки и особых навыков для работы), которые имеют функцию автоматизированной установки всего нужного на сервер и не требуют от пользователей вбивать команды в консоль.

Проект **Outline** начал разрабатываться еще в 2017 году в лаборатории Jigsaw при содействии Google, поэтому имеет характерные для продукта Google черты, такие как трекинг использования приложения и интеграция с поставщиками виртуальных серверов — Google Cloud, Amazon AWS, DigitalOcean. Еще одним недостатком является то, что Outline — ShadowSocks (и при этом не поддерживает плагины маскировки) и технически может быть достаточно легко заблокирован DPI.

Проект **Amnezia VPN** на несколько лет младше, он был основан в 2020 году и учел недостатки Outline. Amnezia VPN имеет поддержку множества разных VPN-протоколов, в том числе и связки OpenVPN over Cloak, которая маскирует VPN-соединение под настоящий web-трафик и устойчива к блокировкам по DPI.

Что касается VPN over HTTPS out of the box (решение для маскировки трафика VPN под HTTPS, работающее прямо «из коробки»): к таким относится, например, Cisco AnyConnect. А вообще, большинство таких продуктов — корпоративные VPN.

ЧАСТЬ 5

# Какие ограничения еще возможны в России, китайский опыт и суверенный Рунет

## Заставят ли интернет-пользователей в России расшифровывать свой трафик для властей — устанавливать сертификаты для MitM[29]?

**Коротко.** Вряд ли — технически это не так просто. Но технология может быть внедрена в браузерах и других программах, подконтрольных госорганам.

**ValdikSS.** Сомнительно: как минимум в современных версиях Android (начиная с седьмой) установка сторонних сертификатов затруднена, программы должны отдельно разрешить их использование. Основной набор приложений откажется работать, даже если сертификат будет импортирован в хранилище. Кроме того, мощности, требуемые для перешифровки данных, на порядки выше мощностей, необходимых для анализа в стиле систем DPI[30].

**Станислав Шакиров.** Можно рассмотреть угрозу внедрения корневых сертификатов государственных регуляторов в хранилище сертификатов конечных пользователей для осуществления mitm-атаки на пользовательский веб-трафик. Это может быть реализовано путем популяризации браузеров, подконтрольных государственным органам, или приложений и утилит, которые сами устанавливают корневые сертификаты.

В любом случае можно предположить, что такой процесс не может быть осуществлен в одночасье. Более того, конъюнктура Рунета препятствует таким действиям — введение обязательного использования государственных корневых сертификатов при посещении сайтов будет равносильна полному отключению страны от внешней части интернета.

## Смогут ли в России блокировать P2P-мессенджеры?[31]

**Коротко.** Только если власти этого сильно захотят.

**Вадим Мисбах-Соловьев.** Если вкратце, то это вопрос затраченных сил и компетенций. На данный момент власти не прикладывают достаточное количество сил (или им не хватает компетенций), чтобы заблокировать P2P-мессенджеры. Но если очень захотят — смогут сделать и это.

В этом плане федеративные мессенджер-сети (Jabber, Matrix, с натяжкой Fediverse[32]) будут понадежнее. Всю сеть не заблокируешь, не вводя «белые списки» сервисов.

## Чем отличаются блокировки в России и Китае? Сколько нужно России времени, чтобы создать аналог китайского файрвола[33]?

## Есть ли у России технологии и оборудование для его создания собственными силами?

**Коротко.** В Китае используются более продвинутые технологии блокировки, но со временем в России тоже могут на них перейти.

**Станислав Шакиров.** До сих пор в России блокируют только по IP-адресам и по доменам. В Китае искусственный интеллект обучен находить протоколы внутри трафика. Сколько потребуется времени, чтобы в России появился аналог китайского файрвола, неизвестно. С технологической точки зрения все нужное оборудование и софт у нас уже есть. Но есть трудности.

Компетентные органы пока не очень хорошо могут определять, что нужно блокировать. Роскомнадзор на отдельных ТСПУ тестирует различные более интеллектуальные способы блокировок, чем просто по IP и домену: иногда — успешно, иногда — внезапно ложится смежная инфраструктура, например «Сбер.Онлайн» или вроде того. Пока не получается блокировать VPN без сопутствующих потерь. И вопрос в том, как скоро государство заставит важные «государствообразующие» сервисы использовать те протоколы, подсети и IP-адреса, которые разрешены («белый список») и не будут блокироваться. После этого блокировки по протоколам или, как еще это называют, по сигнатурам (то, что умеет DPI) станут массовым явлением.

Поэтому с точки зрения «железа» китайский файрвол есть у нас уже сейчас, а с точки зрения алгоритмов — нужно дорабатывать. Для этого уже не нужны «западные спецы», опыта китайских специалистов и сервисов достаточно, чтобы сделать, «как у них», выстроить цензуру по китайскому сценарию. С другой стороны, она тоже не является совершенной и безупречно эффективной: миллионы китайцев ежедневно пользуются VPN, и все у них хорошо.

**ValdikSS.** В Китае применяются более точные методы обнаружения туннелей. Российские системы не столь продвинуты, но, судя по темпам развития и ТСПУ[34], и коммерческих систем, это вопрос времени.

Софт для DPI[35] делается в России, железо все достаточно стандартное и доступное. Из сравнительно немассовых вещей, которые сложно достать на рынке, разве что оптические байпассеры[36] Silicom (модель IS401U-48 как минимум).

## Возможно ли полное отключение России по собственной инициативе от всемирной сети и создание «суверенного интернета», из которого невозможно будет выйти

## даже при помощи VPN? В корпоративной сети крупной компании я такое видел

**Коротко.** Могут попробовать, но лазейки наверняка останутся.

**ValdikSS.** Моя оценка такова: если доступ вовне когда-то отключат, то только на обычном интернете для частных лиц, с сохранением связи внутри страны. На серверах в дата-центрах останется обычный доступ в интернет — VPN-подключение к серверу внутри страны обеспечит доступ в мировую сеть. Такой сценарий уже был в Иране.

Также велика вероятность, что отключение будет не полным — останутся «дырки» в виде незаблокированных протоколов или определенных портов, которые можно будет использовать для создания туннеля. Такое было в Казахстане.

Надеюсь, такого никогда не случится.

**Станислав Шакиров.** Да, могут все закрыть наглухо. Но в масштабах страны должен отсутствовать риск, что «левые доступы» будут неправильно влиять на инфраструктуру.

Сейчас ведется работа по перенастройке систем, чтобы в ситуациях, когда отключаются какие-то VPN или протоколы на выход из страны, не пострадала важная для государства инфраструктура. Поэтому одна из масштабных целей регулирования — сделать так, чтобы и VPN не работал, и все остальное работало.

## Нигде ведь (кроме КНДР) не было такого, чтобы внешний интернет отключали полностью и перманентно? Могут ли издержки перманентной изоляции Рунета показаться властям приемлемыми по сравнению с сохранением доступности хотя быть отдельных VPN-сервисов?

**Коротко.** Сложно сказать наверняка, но полная изоляция — это точно чрезвычайная мера.

**ValdikSS.** Мне кажется, глобальная и постоянная блокировка «внешки» — крайне маловероятный сценарий. Могу представить применение замедления доступа к определенным ресурсам до такой скорости,

которая не позволит ими пользоваться. При блокировке велика вероятность, что пользователь будет пытаться ее обойти, а при замедлении, во-первых, не очевидно, чем вызвана проблема (может, что-то произошло у сервиса или провайдера?), а во-вторых, это психологически более раздражающая мера, которая может вынудить пользователя самостоятельно перейти на альтернативный сервис. Но опять же применение подобных мер — экстремальный сценарий, который, надеюсь, маловероятен. С другой стороны, стране мало что осталось терять.

Депутат [Госдумы Александр] Хинштейн говорил о замедлении YouTube в апреле, а 22–23 мая у клиентов провайдеров в ЛНР и ДНР замедлился YouTube до 128 кбит/с, что не позволяло смотреть видео без прерываний даже в качестве 144p. Инцидент остался обделен вниманием со стороны СМИ.

**Станислав Шакиров.** Все верно: полная изоляция российского сегмента интернета — это полный экономический коллапс страны. Тут вопрос политической воли, того, когда власти будут на это готовы. Хотелось бы, чтобы никогда. Но некоторые сценарии говорят, что полная изоляция на время не исключена. К тому же уже ведутся работы, чтобы минимизировать потери: например, в России сделан аналог SWIFT, к которому подключены банки стран ЕАЭС[37].

## Что делать, если введут «белые списки»[38]? Как подготовиться к сценарию тотального закрытия внешнего интернета?

**Коротко.** Заранее установите и настройте необходимые программы (например, Tor и Psiphon), в случае необходимости — арендуйте собственный сервер в России.

**ValdikSS.** Я бы порекомендовал арендовать серверы в России — магистральные каналы будут фильтровать в последнюю очередь. Не лишним будет настроить DNS-туннели за рубеж: всемирная связность DNS-инфраструктуры очень важна даже для сайтов в зоне .ru и .рф, поэтому ее будут поддерживать в рабочем состоянии с высокой вероятностью.

**Станислав Шакиров.** Обычно, если вводятся «белые списки», то обход блокировок производится через них, то есть трафик маркируется, как будто он идет на один из разрешенных сайтов из списка и по протоколам, по которым невозможно узнать, что там на самом деле происходит. Там используется даже не выход в mesh-сети, а протоколы типа Cloak.

Можно заранее установить программы для обхода блокировок, которые будут работать в случае полного локдауна: Tor, Lantern, Psiphon, Amnezia и некоторые другие.

## Насколько реален сценарий входа в интернет только по паспорту или токену с электронной цифровой подписью[39] в этом десятилетии?

**Коротко.** В России и так уже давно идентифицируют пользователей, но о дополнительном контроле речь пока не идет.

**ValdikSS**. Интернет, по сути, и сейчас работает по паспорту: проводные подключения и сим-карты оформляются на конкретного человека, публичный Wi-Fi требует идентификации по номеру телефона.

Если речь об идентификации личности конкретного пользователя на домашних подключениях, то об этом ничего не слышно.

**Станислав Шакиров.** Сложно сказать, будет ли это действительно осуществлено и в каком виде. Это вопрос политической воли.

Де-факто вход в интернет по документу, идентифицирующему личность, уже практикуется. Домашний интернет невозможно подключить без паспорта, пользователь заключает с провайдером именной договор аренды. В публичных местах невозможно подключиться к Wi-Fi без введения номера телефона, который привязан к вашему контракту с оператором связи.

Выход в интернет по токену ЭЦП — история маловероятная.

---

**Отдел «Разбор»**

### (1) Формулировки вопросов

В этом материале мы слегка изменили некоторые формулировки вопросов, но эксперты видели их в оригинале.

Вернуться к тексту

### (2) Протокол VPN

Он описывает последовательность действий, необходимых для установления защищенного соединения между клиентом и провайдером услуг. Все эти действия автоматически выполняются приложением. Протоколы отличаются друг от друга по разным параметрам, например по используемым криптографическим алгоритмам.

Вернуться к тексту

### (3) Обфускация

Маскировка трафика VPN.

Вернуться к тексту

### (4) Что такое файрвол?

«Файрвол», «браундмауэр», «фильтр трафика» и прочие подобные слова означают одно и то же: программное или аппаратно-программное решение, задача которого — диагностика проходящего трафика и принятие решений (на основе заданного списка правил) о пропуске этого трафика, его блокировке или иных действиях (включая добавление искусственных задержек или подмену ответа).

Вернуться к тексту

### (5) Сетевой маршрутизатор

Он же роутер. Устройство, которое пересылает пакеты с данными в компьютерных сетях.

Вернуться к тексту

### (6) Что такое файрвол?

«Файрвол», «браундмауэр», «фильтр трафика» и прочие подобные слова означают одно и то же: программное или аппаратно-программное решение, задача которого — диагностика проходящего трафика и принятие решений (на основе заданного списка правил) о пропуске этого трафика, его блокировке или иных действиях (включая добавление искусственных задержек или подмену ответа).

Вернуться к тексту

### (7) Deep Packet Inspection

«Глубокий анализ трафика». Это система для детального исследования сетевых пакетов, которая позволяет фильтровать («отбрасывать») сетевые пакеты по определенному признаку и в итоге блокировать доступ к определенным ресурсам либо замедлять к ним доступ.

Вернуться к тексту

### (8) ТСПУ

С ноября 2019 года, когда вступил в силу закон о суверенном Рунете, на сетях операторов связи начали установку специальных «технических средств противодействия угрозам» (ТСПУ). Позднее выяснилось, что под аббревиатурой ТСПУ скрывались системы Deep Packet Inspection (DPI). Управляет всеми установленными DPI специальное подразделение Роскомнадзора.

Вернуться к тексту

### (9) ТСПУ

С ноября 2019 года, когда вступил в силу закон о суверенном Рунете, на сетях операторов связи начали установку специальных «технических средств противодействия угрозам» (ТСПУ). Позднее выяснилось, что под аббревиатурой ТСПУ скрывались системы

Deep Packet Inspection (DPI). Управляет всеми установленными DPI специальное подразделение Роскомнадзора.

Вернуться к тексту

### (10) Туннель

Синоним VPN — зашифрованное подключение между компьютером или мобильным устройством пользователя и интернетом.

Вернуться к тексту

### (11) ТСПУ

С ноября 2019 года, когда вступил в силу закон о суверенном Рунете, на сетях операторов связи начали установку специальных «технических средств противодействия угрозам» (ТСПУ). Позднее выяснилось, что под аббревиатурой ТСПУ скрывались системы Deep Packet Inspection (DPI). Управляет всеми установленными DPI специальное подразделение Роскомнадзора.

Вернуться к тексту

### (12) ТСПУ

С ноября 2019 года, когда вступил в силу закон о суверенном Рунете, на сетях операторов связи начали установку специальных «технических средств противодействия угрозам» (ТСПУ). Позднее выяснилось, что под аббревиатурой ТСПУ скрывались системы Deep Packet Inspection (DPI). Управляет всеми установленными DPI специальное подразделение Роскомнадзора.

Вернуться к тексту

### (13) Deep Packet Inspection

«Глубокий анализ трафика». Это система для детального исследования сетевых пакетов, которая позволяет фильтровать («отбрасывать») сетевые пакеты по определенному признаку

и в итоге блокировать доступ к определенным ресурсам либо замедлять к ним доступ.

Вернуться к тексту

### (14) О чем идет речь?

Есть много свидетельств (например, вот и вот) разной степени достоверности о том, что спецслужбы разных стран вкладывают ресурсы в подключение своих серверов к Tor в качестве «серверов для выхода» (exit node — узлы, через которые запрос «выходит» из сети Tor в глобальный интернет; IP-адрес этого узла видит владелец сайта, который пользователь открывает в tor-браузере), чтобы на них перехватывать и анализировать трафик.

Вернуться к тексту

### (15) «Белые списки»

Список разрешенных для доступа сайтов, запрещающий все остальное автоматически. Альтернатива черному списку запрещенных сайтов, доступ к которым власти пытаются ограничить.

Вернуться к тексту

### (16) Domain fronting

Технология, позволяющая скрыть реальный адрес сайта, с которым устанавливается соединение.

Вернуться к тексту

### (17) Прокси-сервер

Это сервер-посредник. Через него идут запросы пользовательской программы и ответы сайта или сервиса.

Вернуться к тексту

### (18) Mesh-сети

Сеть, в которой узлы соединяются между собой по принципу «каждый с каждым», к примеру, по Wi-Fi. При этом все узлы в такой сети равны между собой, а пользователи сами выступают провайдерами друг для друга. Они могут быть замкнутыми, как локальные сети, или иметь выход в интернет через отдельные узлы.

Вернуться к тексту

### (19) Прокси-сервер

Это сервер-посредник. Через него идут запросы пользовательской программы и ответы сайта или сервиса.

Вернуться к тексту

### (20) HTTP-трафик

Сейчас его уже редко используют, так как отсутствие шифрования позволяет не просто узнавать, на какую страницу какого сайта вы заходите, но и понимать, что именно вы там читаете, что именно вы туда отправляете, и даже какие логин и пароль вы используете для входа.

Вернуться к тексту

### (21) ТСПУ

С ноября 2019 года, когда вступил в силу закон о суверенном Рунете, на сетях операторов связи начали установку специальных «технических средств противодействия угрозам» (ТСПУ). Позднее выяснилось, что под аббревиатурой ТСПУ скрывались системы Deep Packet Inspection (DPI). Управляет всеми установленными DPI специальное подразделение Роскомнадзора.

Вернуться к тексту

### (22) Internet Control Message Protocol

Это интернет-протокол, который в основном используется для передачи сообщений об ошибках.

Вернуться к тексту

### (23) Domain Name System

Система доменных имен выполняет функцию «переводчика». DNS-сервер переводит доменные имена в IP-адреса.

Вернуться к тексту

### (24) Что еще за резолверы?

DNS-серверы, занимающиеся переводом доменных имен в IP-адреса.

Вернуться к тексту

### (25) CDN

Content Delivery Network («сеть доставки контента») — оборудование, позволяющее пользователям быстрее загружать контент при условии, что сайт использует CDN-сервис.

Вернуться к тексту

### (26) Man-in-the-middle

Атака на криптографически защищенные соединения, при которой вместо прямой связи между браузером пользователя и конечным сайтом возникает связь через третью сторону — посредника. В результате зашифрованное соединение устанавливается не между пользователем и сайтом, а между пользователем и атакующим. Он, в свою очередь, ретранслирует перехваченный трафик к запрошенному пользователем сайту и может его расшифровывать.

Вернуться к тексту

### (27) Deep Packet Inspection

«Глубокий анализ трафика». Это система для детального исследования сетевых пакетов, которая позволяет фильтровать («отбрасывать») сетевые пакеты по определенному признаку и в итоге блокировать доступ к определенным ресурсам либо замедлять к ним доступ.

Вернуться к тексту

### (28) P2P-мессенджеры

Это децентрализованные мессенджеры, которые позволяют обмениваться сообщениями напрямую между устройствами пользователей. То есть сообщения не хранятся на серверах компании-посредника.

Вернуться к тексту

### (29) Почему с натяжкой?

Это, скорее, соцсети, а не мессенджеры, но грань между ними тонка.

Вернуться к тексту

### (30) Что такое файрвол?

«Файрвол», «браундмауэр», «фильтр трафика» и прочие подобные слова означают одно и то же: программное или аппаратно-программное решение, задача которого — диагностика проходящего трафика и принятие решений (на основе заданного списка правил) о пропуске этого трафика, его блокировке или иных действиях (включая добавление искусственных задержек или подмену ответа).

Вернуться к тексту

### (31) ТСПУ

С ноября 2019 года, когда вступил в силу закон о суверенном Рунете, на сетях операторов связи начали установку специальных «технических средств противодействия угрозам» (ТСПУ). Позднее выяснилось, что под аббревиатурой ТСПУ скрывались системы Deep Packet Inspection (DPI). Управляет всеми установленными DPI специальное подразделение Роскомнадзора.

Вернуться к тексту

### (32) Deep Packet Inspection

«Глубокий анализ трафика». Это система для детального исследования сетевых пакетов, которая позволяет фильтровать («отбрасывать») сетевые пакеты по определенному признаку и в итоге блокировать доступ к определенным ресурсам либо замедлять к ним доступ.

Вернуться к тексту

### (33) Что это такое?

Устройство в волоконно-оптической сети, которое помогает сохранить связь с сетью при потере питания отдельными узлами.

Вернуться к тексту

### (34) ЕАЭС

Евразийский экономический союз, куда входят Россия, Армения, Беларусь, Казахстан и Кыргызстан.

Вернуться к тексту

### (35) «Белые списки»

Список разрешенных для доступа сайтов, запрещающий все остальное автоматически. Альтернатива черному списку запрещенных сайтов, доступ к которым власти пытаются ограничить.

Вернуться к тексту

### [36] Токен с электронной цифровой подписью

Устройство с ключами для электронной цифровой подписи — обычно в виде USB-брелока или смарт-карты.

Вернуться к тексту

### [37] Deep Packet Inspection

«Глубокий анализ трафика». Это система для детального исследования сетевых пакетов, которая позволяет фильтровать («отбрасывать») сетевые пакеты по определенному признаку и в итоге блокировать доступ к определенным ресурсам либо замедлять к ним доступ.

Вернуться к тексту

### [38] HTTP-трафик

Сейчас его уже редко используют, так как отсутствие шифрования позволяет не просто узнавать, на какую страницу какого сайта вы заходите, но и понимать, что именно вы там читаете, что именно вы туда отправляете, и даже какие логин и пароль вы используете для входа.

Вернуться к тексту

### [39] Request for Comments

Документ с техническими спецификациями и интернет-стандартами.

Вернуться к тексту