

[КАК СТАТЬ АВТОРОМ](#)[Тестировщики, вам сюда](#)[Обучение — новый тренд ИБ](#)

Deleted-user

17 янв 2023 в 00:17

# Интернет-цензура и обход блокировок: не время расслабляться



10 мин



155K

Информационная безопасность\*, Сетевые технологии\*, Исследования и прогнозы в IT\*

[Аналитика](#)

Статья опубликована под лицензией [Creative Commons BY-NC-SA](#).

*Disclaimer: практически всё, описанное в статье, не является чем-то принципиально новым или инновационным - оно давно известно и придумано, используется в разных странах мира, реализовано в коде и описано в научных и технических публикациях, поэтому никакого ящика Пандоры я не открываю.*

Нередко на Хабре в темах, посвященных блокировкам ресурсов, встречаются забавные заявления вида "Я настроил TLS-VPN, теперь будут смотреть что хочу и цензоры мой VPN не заблокируют", "Я использую SSH-туннель, значит все ок, не забанят же они весь SSH целиком", и подобное. Что ж, давайте проанализируем опыт других стран и подумаем, как же оно может быть на самом деле.

## 0

Итак, допустим мы купили у какого-то сервиса, или, как подкованные пользователи, установили в личном облаке/VPS и настроили VPN-сервер для себя. Допустим, это популярные WireGuard или OpenVPN. Знаете что? WireGuard - это такой прекрасный протокол, который всеми своими пакетами просто кричит "Смотрите все, смотрите, я - VPN". И это, в принципе, не удивительно, потому что авторы на сайте проекта прямым текстом пишут, что обфускация не входила и не будет входить в их цели и планы.

Соответственно, на оборудовании DPI (оно же ТСПУ) при небольшом желании протокол WireGuard выявляется и блокируется на раз-два. IPSec/L2TP - аналогично. С OpenVPN то же самое - это, наверное, вообще самый первый протокол, который китайцы научились выявлять и банить на своем "великом китайском фаерволе" (GFW). We are fucked.



+319



793



518

Окей, допустим мы сделали выводы, и вместо совсем уж палевных протоколов решили использовать TLS-VPN, такие как SSTP, AnyConnect/OpenConnect или SoftEther - трафик в них ходит внутри TLS, начальная установка соединения производится по HTTP - что должно быть совсем никак неотличимо от обычного подключения к любому обычному сайту. Ну, как сказать...

В случае с **MS SSTP** цензоры, желая выяснить, а чем же вы таким занимаетесь, просто сделают запрос на ваш сервер с URL `/sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/` с HTTP-методом `SSTP_DUPLEX_POST`, как это описано в стандарте протокола, и сервер радостно подтвердит в ответ, что он - да, действительно MS SSTP VPN.

**SoftetherVPN** в ответ на GET-запрос с путем `/vpnsvc/connect.cgi`, типом `application/octet-stream` и пэйлоадом `'VPNCONNECT'` выдаст в ответ 200 код и предсказуемый бинарный блоб с рассказом о том, кто он такой.

**AnyConnect/OpenConnect** при обращении по `/` или по `/auth` ответят очень характерной XML'кой. И от всего этого вы не избавитесь никак - это определено в протоколах, и именно через эту логику работают VPN-клиенты. We are fucked.

## 2

Ясно, мы будем умнее, и поскольку у нас все-таки TLS, давайте поставим перед VPN-сервером reverse-прокси (например, haproxy) и будем разруливать всё по SNI (server name identification): подключения с определенным доменом в запросе будем отправлять на VPN-сервер, а все остальные - на безобидный сайт с котиками. Можно даже попробовать спрятаться за какой-нибудь CDN - не забанят же они весь CDN, правда, и наш трафик из общего трафика ко всей CDN выцепить не смогут, да?

Правда, есть одно "но". В нынешних версиях TLS поле SNI не шифруется, соответственно цензоры легко его подсмострят и сделают запрос именно с тем именем домена, что надо. На расширение Encrypted Client Hello (ECH), ранее известное как eSNI, можно не рассчитывать: во-первых, оно находится еще в состоянии Draft и неизвестно когда будет принято и повсеместно использоваться, а во-вторых, цензоры могут взять и просто-напросто заблокировать все соединения TLSv1.3 с ECH, как это сделали в Китае. Проблемы индейцев шерифа не волнуют. We are fucked.

## 3

Шутки в стороны, мы настроены решительно. Например, мы пропатчили OpenConnect-сервер, чтобы он принимал подключения только со специальным словом в URL'е (благо, AnyConnect/OpenConnect-клиенты такое позволяют), а всем остальным отдавал

правдоподобную заглушку. Или настроили обязательную аутентификацию по клиентским сертификатам.

Или же мы подключаем тяжелую артиллерию от товарищей-китайцев, которые на обходе блокировок собаку съели. Shadowsocks (Outline) отпадает, ибо его версии до 2022 года уязвимы к replay-атакам и даже active probing'y, но вот V2Ray/XRay с плагином VMess и VLess поверх Websockets или gRPC, либо Trojan-GFW - это то что надо. Они работают поверх TLS, могут делить один и тот же порт с HTTPS-вебсервером, и не зная заветной секретной строчки, которую подслушать снаружи не получится, выявить наличие туннеля и подключиться к нему, казалось бы нельзя, значит все хорошо?

Давайте подумаем. Каждый TLS-клиент при подключении передает серверу определенный набор параметров: поддерживаемые версии TLS, поддерживаемые наборы шифров, поддерживаемые расширения, эллиптические кривые и их форматы. У каждой библиотеки этот набор свой, и его варианты можно анализировать. Это называется [ClientHello fingerprinting](#). Отпечаток (fingerprint) библиотеки OpenSSL отличается от отпечатка библиотеки GnuTLS. Отпечаток TLS-библиотеки языка Go отличается от fingerprint'a браузера Firefox.

И когда с вашего адреса будут зафиксированы частые и долгие подключения к некому сайту клиентом с библиотекой GnuTLS (которая не используется ни в одном популярном браузере, но используется в VPN-клиенте OpenConnect), или с мобильного телефона через мобильного оператора подключается какой-то клиент на Go (на котором написан V2Ray), we are fucked. Такое детектирование, например, производится в Китае и в Туркменистане.

## 4

Ладно. Допустим, мы пересобрали наш V2Ray-клиент не со стандартной TLS-либой, а с uTLS, которая может маскироваться под популярные браузеры. Или вообще взяли исходники самого популярного браузера, выдрали оттуда весь код сетевого стека и написали свой прокси-клиент на его базе, чтобы быть совсем уже неотличимыми от обычного браузерного TLS. Или решили пойти в сторону маскировки под другие протоколы типа SSH, или взяли OpenVPN с XOR-патчем. Или какой-нибудь KCP/Hysteria с маскировкой под DTLS.

Короче говоря, допустим у нас что-то более редкое и незаметное. Казалось бы, все хорошо? Ну как сказать. Помните "пакет Яровой"? Тот самый, который требует, чтобы интернет-сервисы сохраняли все метаданные сессий, а интернет-провайдеры так вообще записывали дампы трафика своих абонентов? Многие, еще тогда смеялись - мол, ну тупые, что им дадут гигабайты зашифрованных данных, которые они все равно не расшифруют? А вот что.

Пользуетесь вы, допустим, своим туннельчиком, смотрите всякие там запрещенные сайты. А потом - клик! - и случайно заходите через свой туннель на какой-нибудь отечественный сайт или сервис, замеченный в сотрудничестве с государством - условные там VK/Mail.ru/Яндекс или еще что-нибудь. Или на каком-нибудь безобидном сайте попадаетесь виджет, баннер или счетчик от них же. Или кто-нибудь в комментарии вбросит ссылку на какой-нибудь сайт-honeypot, косящий под новостной ресурс, и вы на нее нажмете.

И вот тут произойдет самое интересное. Что внутри TLS, что внутри SSH, что внутри OpenVPN+хор, данные передаются в зашифрованном виде, и их не расшифровать. Но вот "внешняя форма" (размеры пакетов и тайминги между ними) у зашифрованных данных точно такая же, как и у нешифрованных. Цензоры видят, что от абонента к какому-то неизвестному серверу и обратно ходит трафик, а поток со стороны какого-нибудь подконтрольного сервиса видит, что с того же IP-адреса, что у "неизвестного сервера", туда прилетают какие-то запросы и улетают ответы, и - вот интересно - размеры пакетов и временные моменты практически полностью совпадают. Что весьма характерно говорит о том, что *у нас тут прокси, возможно VPN, Андрюха, по коням!*

И да, если вы поступите мудрее и у вашего сервера будет два IP-адреса, один на вход, а другой на выход, то сопоставить ваш "вход" и "выход" по адресам не получится, но по "форме" переданных данных, хоть и ощутимо сложнее, но при желании по прежнему можно. We are fucked again.

## 5

Не так уж плохо дело. Мы настроили для своего туннеля rule-based access. А именно, будем ходить по нему только туда, куда надо, и тогда, когда надо - а во всех остальных случаях пусть пакетики бегают сразу по обычному интернет-подключению. Правда, добавлять каждый раз новый ресурс в список - тот еще геморрой, особенно когда вы держите прокси/VPN не только для себя, но и, например, для далеко живущих немолодых родителей, которые, например, хотят читать всяких там иноагентов - но это, на самом деле, мелочи, мы справимся.

Допустим, мы по-прежнему используем SSH-туннель. Правда, проработает он, скорее всего, недолго. Почему? Потому что дело во всех тех же паттернах трафика. И нет, записывать и мучительно сравнивать ничего никуда уже не надо. Паттерны трафика у ssh-as-console, ssh-as-ftp и ssh-as-proxy очень разные и элементарно выявляются довольно просто должным образом натренированной нейросетью. Поэтому китайцы и иранцы уже давно всё подобное "неправильное" использование SSH выявляют и режут скорость подключения до черепашьей, что в терминале работать вы еще сможете, а вот серфить - практически нет.

Ну или, допустим, вы все-таки используете `whatever-over-TLS`-туннель с учетом всего приведенного в этой статье. Но проблема в том, что все сказанное в предыдущем абзаце, применимо и к нему - а именно, `TLS-inside-TLS` выявляется сторонним наблюдателем с помощью эвристик и машинного обучения, которое еще можно дополнительно натренировать на наиболее популярных сайтах. `We are still fucked`.

## 6

Ладно. Мы добавили в наш тайный туннель `random padding` - "дописывание" в конец пакета какого-нибудь мусора случайно длины, чтобы сбить с толку наблюдателей. Или специально бьем пакеты на маленькие кусочки (и получаем проблемы с MTU, ой, придется потом старательно пересобирать). Или, наоборот, когда у нас внутри туннеля устанавливается `TLS`-соединение с каким-нибудь сервером, мы начинаем слать эти пакеты `as-is` без дополнительного слоя шифрования, таким образом выглядя со стороны на сто процентов как обычный `TLS` без двойного дна (правда, придется еще потратить несколько итераций на доведение протокола до ума и затыкание очень тонких и очень неочевидных уязвимостей реализации). Кажется бы, `happy end, we are not fucked anymore?`

А тут начинается все самое интересное. А именно, рано или поздно в вопросах выявления туннелей и блокировок, особенно с развитием технологий их обхода (в конце концов, мы ещё не затронули стеганографию и много других интересных вещей), начинает расти то, что называется `collateral damage` - ущерб, возникший случайно в ходе атаки намеренной цели. Например, как говорят *инсайдеры* и подтверждают сводки с полей, то самое упомянутое выше выявление `tls-inside-tls` даже с *random padding*'ом китайцы научились выявлять примерно с точностью 40%. Понятно дело, что при такой точности возможны также ложные срабатывания, но когда проблемы индейцев волновали шерифа?

Протоколы, которые снаружи не похожи ни на что (например, `shadowsocks obfs4`, и т.д.) тоже при большом желании можно выявить по... статистике нулей и единичек в байтах, потому что у зашифрованного трафика это соотношение очень близко к 1:1 - хотя, понятное дело, при этом могут пострадать невиновные. Можно банить адреса, когда висят слишком много или слишком долго подключения к не-являющимся-очень-популярными-сайтам. Подобных вариантов довольно много, и если вы думаете, что цензоров остановят ложноположительные срабатывания и ущерб от блокировок добропорядочных сайтов - то вы заблуждаетесь.

Когда Роскомнадзор пытался заблокировать Telegram, они вносили в бан-лист целые подсети и хостинги, таким образом побанив кучу ни в чем невиновных сайтов и сервисов - и им за это ничего не было. В Иране, в связи с популярностью упомянутого выше похожего-на-браузер-прокси-клиента, цензоры вообще тупо запретили подключения с Chrome TLS fingerprint к популярным облачным сервисам. В Китае массово попадают под раздачу CDN, услугами которых пользуются безобидные и невиновные сайты и сервисы. В

Туркменистане так вообще заблокирована почти треть (!) всех существующих в мире IP-адресов и подсетей, потому что стоит цензорам только выявить хотя бы один VPN или прокси, как в бан отправляется целый диапазон адресов около него или даже вся AS.

Вы, наверное, можете спросить, а что же делать юрлицам, которые тоже пользуются VPN для работы, или чьи сервисы могут случайно попасть под раздачу? Этот вопрос легко решается белыми списками: если юрлицу нужен VPN-сервер, или нужно обезопасить от случайной блокировки какие-либо свои сервисы, то стоит обязать их заранее сообщать о нужных адресах и протоколах в соответствующие ведомства, чтобы те добавили их в какой-либо список - именно такие запросы Роскомнадзор через ЦБ рассылал в банки, задумывая что-то нехорошее, и механизм таких списков уже существует.

Ну и, естественно, вполне вытекающим продолжением из этого будет "все что не разрешено - то запрещено". Закон о запрете VPN и анонимайзеров в целях обхода блокировок в РФ уже есть. Запрет использования несертифицированных средств шифрования - тоже. Подкрутить и расширить их зоны применения и многократно ужесточить наказания за такие "нарушения" - дело несложное. В Китае вежливые ребята пришли в гости к разработчикам небезизвестных ShadowSocks и GoAgent и сделали им предложения, от которых те никак не смогли отказаться. В Иране есть случаи возбуждения дел в связи с использованием VPN для доступа к запрещенным сайтам. Механизм стукачества в органы на неблагонадежных соседей был отлично отработан еще в прошлом веке в СССР. У государств есть монополия на насилие, не забывайте. We are fucked again?

## 4294967295

К чему это всё?

Как я уже сказал, большая часть того, что описано в статье, не является выдумками или голый теорией - оно давно известно, используется в некоторых странах мира, реализовано в коде и даже описано в научных публикациях.

Обход блокировок - это постоянная борьба щита и меча, и одновременно игра в кошки-мышки: ~~иногда ты ешь медведя, иногда медведь ест тебя~~ иногда ты догоняющий, иногда догоняемый.

Если у вас сейчас есть прокси или VPN, и он работает - не расслабляйтесь: вы всего-лишь на полшага впереди недоброжелателей. Можно, конечно, спокойно сидеть и думать "Да они там все дураки и криворукие обезьяны и ниасилият ничего сложного и реально работающего", но, как говорится, надейся на лучшее, а готовься к худшему. Всегда есть смысл изучить опыт тех же китайских коллег и присмотреться к более сложновывяляемым и более цензуроустойчивым разработкам. На чем больше шагов вы будете впереди цензоров, тем больше времени у вас будет в запасе чтобы адаптироваться к

изменившейся ситуации. Если вы разработчик и разбираетесь в сетевых протоколах и технологиях - можно присоединиться к одному из существующих проектов, помочь с разработкой и подумать над новыми идеями. Люди всего мира скажут вам спасибо.

Интересными и полезными в этом плане будут [Net4People](#), [No Thought is a Crime](#), [дискуссии в проекте XTLS](#) (там большая часть на китайском, но автопереводчик на английский справляется неплохо), [GFW report](#). Если кто-то знает ещё хорошие ресурсы и сообщества по этой теме - напишите в комментарии

Ну и не стоит забывать, что рано или поздно, не имея возможности противостоять подобному свободолобию технически, государство может начать противостоять административно (та самая монополия на насилие), причем так, что с вашей стороны, в свою очередь, технически противостоять может уже не получиться. Но это уже совсем другая история, требующая отдельной статьи, и, скорее всего, на другом ресурсе.

Когда я писал эту публикацию, я хотел вставить в нее картинки из какого-нибудь мрачного киберпанк-фильма, где в результате развития технологий слежения и цензуры и невозможности противостоять этому, люди целиком и полностью стали подконтрольны государствам и потеряли все права на свободу мысли и приватность личной жизни. Но я надеюсь, до этого не дойдет. Все в наших руках.

Если вы хотите сказать спасибо автору — сделайте пожертвование в один из благотворительных фондов: "Подари жизнь", "Дом с маяком", "Антон тут рядом".

**Теги:** vpn, проху, блокировки сайтов, цензура интернета

**Хабы:** Информационная безопасность, Сетевые технологии, Исследования и прогнозы в IT

## Редакторский дайджест

Присылаем лучшие статьи раз в месяц

**11****0**

Карма Рейтинг

**Deleted user** @Deleted-user

Так вышло



 Комментарии 518

## Публикации

ЛУЧШИЕ ЗА СУТКИ

ПОХОЖИЕ

**UranusExplorer**

12 часов назад

### Надежный обход блокировок в 2024: протоколы, клиенты и настройка сервера от простого к сложному

**Простой**

36 мин



27K

Тutorial

**+198**

444



73

**Telnov\_WIKI**

19 часов назад

### Исследование деградации Li-ion аккумуляторов в результате “быстрой” зарядки

**Простой**

4 мин



19K

Аналитика

**+43**

48



39

**Lunathecat**

вчера в 12:00

### 115 лет прогресса: от механического осциллографа до самодельного цифрового

**Простой**

9 мин



6.7K

Ретроспектива

**+37**

42



13

**Exosphere**

вчера в 12:27

### Инженеры, мы в ваших руках

**Простой**

6 мин



4.4K



 +29 25 13**DAN\_SEA**

20 часов назад

## Ещё один шаг в сторону оптических наушников

**Средний**

10 мин



8K

[Обзор](#) +27 23 50**madyouth**

23 часа назад

## Как мы создаём редакторы документов. Ядро и его роль в кроссплатформенной разработке



10 мин



1.1K

 +27 19 1**iMonin**

19 часов назад

## Энергетика большой страны. Почему мы все не можем отапливаться электричеством?



28 мин



10K

 +25 36 67**sacredtree**

22 часа назад

## Почему рациональный выбор невозможен



8 мин



3.2K

 +18 38 7**it\_union**

3 часа назад

## Снижение зарплат в ИТ



2 мин




10K

+16

8

10

 **WizAlx**  
19 часов назад

### Интеграция нативных SDK во Flutter-приложение

9 мин

851

Тutorial

Перевод

+15

33

1

### А если всё рухнет при первой атаке? Почему нужно вкладываться в ИБ-обучение сотрудников

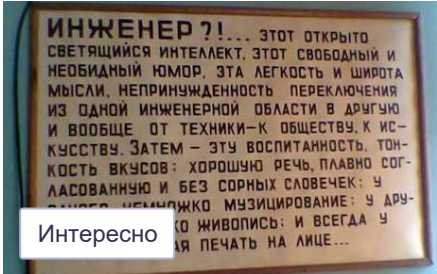
Турбо

Показать еще

#### МИНУТОЧКУ ВНИМАНИЯ



Выбирайте команду тестирования по вайбам



«Инженерный подход»: новая номинация в Технотексте



Топим снег скидками: промокодус в деле

#### ВАКАНСИИ

Специалист технической поддержки платформы  
до 100 000 Р · CRAFTED · Москва

Оператор 1-я, 2-я линия техподдержки(поддержка клиентов)  
от 30 000 Р · MYRTEX · Можно удаленно

SEO-специалист в Digital-агентство  
от 80 000 Р · 2x2 Digital Agency · Можно удаленно

SEO-специалист

от 70 000 Р · ВЕКТРА · Можно удаленно

Тестировщик / QA engineer

до 130 000 Р · МИЦ «Известия» · Москва · Можно удаленно

Больше вакансий на Хабр Карьере

ЧИТАЮТ СЕЙЧАС

Надежный обход блокировок в 2024: протоколы, клиенты и настройка сервера от простого к сложному

 27K

 73

Снижение зарплат в ИТ

 10K

 10

Голодные игры начались. Развитие ИИ приведёт к естественному отбору населения

 43K

 196

Исследование деградации Li-ion аккумуляторов в результате “быстрой” зарядки

 19K

 39

Сколько мы заработали за год на 1 товаре из Китая. Продаем коврики для ноутбука на маркетплейсах

 39K

 65

А если всё рухнет при первой атаке? Почему нужно вкладываться в ИБ-обучение сотрудников

Турбо

ИСТОРИИ



**GitVerse: открой вселенную кода**



**Нейросети: интересное**



**Что умеет калькулятор зарплат в IT**



**Яндекс 360 призывает героев бэкэнда**



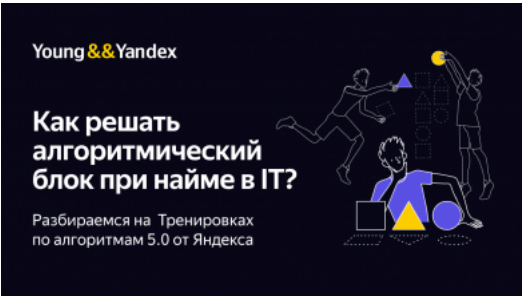
**Полезные книги для библиотеки айтишника**

РАБОТА

Специалист по информационной безопасности  
140 вакансий

Все вакансии

БЛИЖАЙШИЕ СОБЫТИЯ



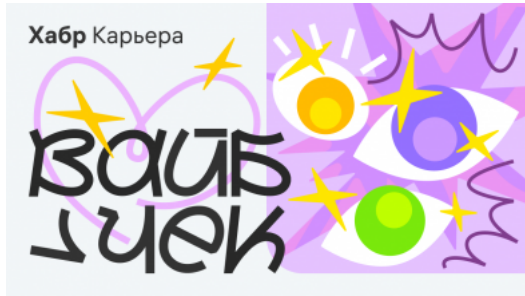
**Серия занятий «Тренировки по алгоритмам 5.0» от Яндекса**

1 марта – 19 апреля

19:00

Онлайн

Подробнее в календаре



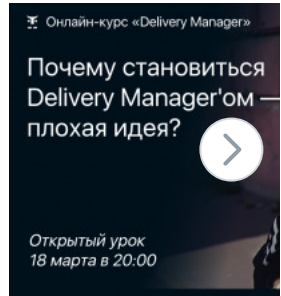
**Тестировщики, выбирайте себе команду по вайбам на Хабр Карьере**

18 – 24 марта

09:00 – 23:00

Онлайн

Подробнее в календаре



**Открытый урок становиться Delivery Manager'ом — плохая идея?**

18 марта

Онлайн

Подробнее в календаре

Ваш аккаунт	Разделы	Информация	Услуги
Войти	Статьи	Устройство сайта	Корпоративный блог
Регистрация	Новости	Для авторов	Медийная реклама
	Хабы	Для компаний	Нативные проекты
	Компании	Документы	Образовательные
	Авторы	Соглашение	программы
	Песочница	Конфиденциальность	Стартапам



Настройка языка

Техническая поддержка

© 2006–2024, Habr