

На следующих слайдах вы найдете подробную информацию о бесплатных VPN сервисах и браузере Tor, включая официальные источники для их скачивания

Узнайте больше о них!→

#KeepItOn 

БЕСПЛАТНЫЕ И ПРОСТЫЕ В ИСПОЛЬЗОВАНИИ VPN

ОБНОВЛЕНО: ФЕВ
2022



Свяжитесь с Службой
Цифровой
Поддержки Access
Now для получения
бесплатных кодов и
инструкции по
установке.

MULLVAD

Быстрый и простой в использовании VPN, помогающий скрыться от хакеров и слежки

ДОСТУПЕН НА



→ Android 8.0 and up
→ iOS 12.0 and up



→ Windows 7 and up
→ macOS 10.14 and up
→ Linux (Ubuntu 18.04+,
Debian 10+, Fedora 33+)

**ЗАГРУЗИТЬ И
ИСПОЛЬЗОВАТЬ**

<https://mullvad.net/en/download/>

Также доступен в виде
расширения для браузера
FIREFOX



Бесплатные 500MB
/
месяц в России.
Для некоторых
пользователей
может быть
заблокирован.

TUNNELBEAR

VPN который позволяет приватный браузеринг без регистрации

ДОСТУПЕН НА



→ Android 5.0 and up
→ iOS 12 and up



→ Windows 7 and up
→ MacOS 10.10 & up

**ЗАГРУЗИТЬ И
ИСПОЛЬЗОВАТЬ**

<https://www.tunnelbear.com/download-devices>

Также доступен в виде
расширения для браузеров
CHROME | FIREFOX | OPERA



Свяжитесь с Службой
Цифровой
Поддержки Access
Now для получения
бесплатных кодов и
инструкции по
установке.

AIRVPN

VPN основанный на базе OpenVPN системы

ДОСТУПЕН НА



→ Android
→ iOS



→ Windows 7 and up
→ macOS 10.15 and up
→ Linux (Ubuntu, Debian)
→ Chrome OS

**ЗАГРУЗИТЬ И
ИСПОЛЬЗОВАТЬ**

<https://airvpn.org/download/>

#KeepItOn

<https://www.accessnow.org/keepiton/>

БЕСПЛАТНЫЕ И ПРОСТЫЕ В ИСПОЛЬЗОВАНИИ VPN И ИНСТРУМЕНТ БРАУЗИНГА

ОБНОВЛЕНО: ФЕВ
2022



БЕСПЛАТНО

PSIPHON

Обязательный инструмент
для обхода цензуры

ДОСТУПЕН НА



→ Android 4.0 and up
→ iOS 10.2 and up



→ Windows
(XP/Vista/7/8/10)
→ macOS 11.0 and up
(with M1 chip)

**ЗАГРУЗИТЬ И
ИСПОЛЬЗОВАТЬ**

<https://psiphon.ca/download.html>



БЕСПЛАТНО

LANTERN

Быстрый, надежный и
безопасный
доступ в открытый интернет

ДОСТУПЕН НА



→ Android 4.4 and up
→ iOS 12.1 and up



→ Windows (XP/SP/3)
→ macOS 11.0 and up
(with M1 chip)
→ Linux Ubuntu

**ЗАГРУЗИТЬ И
ИСПОЛЬЗОВАТЬ**

<https://getlantern.org/>



БЕСПЛАТНО
(Есть
ограничения)

PROTONVPN

Высокоскоростной VPN,
который защищает вашу
приватность

ДОСТУПЕН НА



→ Android 5.0 and up
→ iOS 11.0 and up



→ Windows
→ OSX
→ Linux

**ЗАГРУЗИТЬ И
ИСПОЛЬЗОВАТЬ**

<https://protonvpn.com/download>



БЕСПЛАТНО

TOR BROWSER

Защитите себя от слежки и
цензуры

ДОСТУПЕН НА



→ Android



→ Windows
→ MacOS
→ Linux

**ЗАГРУЗИТЬ И
ИСПОЛЬЗОВАТЬ**

<https://www.torproject.org/download/>

Также доступен в виде
расширений для браузеров
CHROME | FIREFOX | OPERA

#KeepItOn

<https://www.accessnow.org/keepiton/>

Тестирование происходящих отключений интернета.

Когда вы теряете интернет-соединение или не можете получить доступ к определенным веб-сайтам, сервисам или приложениям, крайне сложно определить, какие технические причины стоят за этими перебоями. Однако благодаря всемирному сообществу интернет-измерений у вас есть инструменты и данные для изучения технических деталей.

Вы можете измерить свое интернет-соединение, используя приложение [OONI Probe](#), которое позволяет вам производить тесты и собирать доказательства различных форм сбоев в работе сети.

Давайте взглянем на приложение OONI Probe, к примеру→

ТЕСТИРУЙ СВОЕ ИНТЕРНЕТ-СОЕДИНЕНИЕ С OONI

ОБНОВЛЕНО: ФЕВ 2022



OONI

Инструмент для проверки блокировки веб-сайтов, приложений социальных медиа и VPN сервисов

O O N I P R O B E ДОСТУПЕН НА



Android
& iOS

<https://ooni.org/install/mobile>



Windows,
macOS,
Linux

<https://ooni.org/install/desktop>



ПРИМЕЧАНИЯ

1. Для проведения тестов OONI Probe необходимо отключить VPN.
2. Проведение тестов может быть рискованным. Любой, кто отслеживает вашу активность в Интернете (например, интернет-провайдер, правительство, ваш работодатель), может увидеть, что вы используете OONI Probe и тот перечень веб-сайтов, которые вы пытались посетить.
3. Тесты используют мегабайты данных.



МЫ РЕКОМЕНДУЕМ

1. Узнайте больше о **возможных рисках** перед установкой OONI Probe.
2. Закройте все свои браузеры, другие приложения и отключите VPN сервисы перед проведением тестов.
3. Избегайте использования домашнего или рабочего Wi-Fi. Помните об использовании мегабайтов данных, особенно когда вы расходуете мобильный трафик.

Открой ссылку ниже в приложении, чтобы проверить блокировку социальных сетей

<https://accessnow.org/ooni-test-social>

Больше информации, включая описание возможных рисков, ищи на

<https://ooni.org/>

Узнайте больше о различных типах сбоев в работе сети и возможных способах их устранения.

Вы можете избежать определенных типов сбоев в сети с помощью готовых инструментов, таких как браузер Tor, виртуальные частные сети (VPN) и прокси, использующие шифрование. Следующая таблица поможет вам понять, с каким типом отключения вы можете столкнуться и какие методы помогут вам оставаться на связи.

Давайте взглянем подробнее →

Признаки	Возможный тип сбоя в работе сети	Возможные способы смягчения последствий
<p>Все веб-сайты сразу становятся недоступными. Нет подключения к интернету.</p>	<p>Полное отключение: отключение, вызванное критическими манипуляциями с инфраструктурой, такими как отключение электросети, вышек сотовой связи или прекращение услуг широкополосного интернета</p>	<p>Если возможно, приобретите SIM карту соседних стран с услугами роуминга. Зарубежная телекоммуникационная инфраструктура продолжит работать и, скорее всего, будет доступна и вам. Чтобы связаться с людьми поблизости, вы можете установить приложения для создания ячеистой Mesh-сети для шифрованной передачи данных такие как Briar (только для Android) и Bridgefy, или инструменты как goTenna.</p>
<p>Веб-сайты и приложения становятся медлительными и неудобными в использовании. Загрузки и / или скачивания занимают</p>	<p>Изменение пропускной способности Сети (дросселирование): намеренное снижение скорости интернета, что затрудняет или делает невозможным загрузку или скачивание информации пользователями</p>	<p>Есть несколько способов осуществить дросселирование сети, и смягчить последствия некоторых из них крайне затруднительно. Для начала вы можете попробовать использовать VPN, чтобы оценить, удастся ли обойти ограничения пропускной способности сети.</p>

Признаки	Возможный тип сбоя в работе сети	Возможные способы смягчения последствий
<p>Когда вы посещаете веб-сайт, вы получаете сообщение о том, что «соединение небезопасно» или «DNS-сервер не отвечает», или веб-страница выглядит непривычно, странно, или работает неправильно.</p>	<p>Блокировка DNS и отравление DNS кэша: нарушение работы поисковых запросов в системе доменных имен (DNS) таким образом, чтобы при вашей попытке посетить веб-сайт, вы направлялись на неправильный адрес</p>	<p>Попробуйте использовать надежный VPN. Установите и протестируйте несколько на случай, если один из них не будет работать. Вы также можете использовать проверенный DNS сервер с помощью служб поддержки гражданского общества. Вы также можете посетить IP-адрес веб-сайта.</p>
<p>Веб-сайт / приложение или его версия недоступны, или контент, который вы видите, отличается от того, что виден пользователям в других регионах. Например, вы можете посещать только HTTP-адрес веб-сайта, но не HTTPS-адрес.</p>	<p>Сетевая фильтрация: использование «промежуточных ящиков» (мидлбоксов), установленных в сетевом трафике для нарушения протоколов связи, таких как защищенный протокол передачи гипертекста (HTTPS).</p>	<p>Надежный VPN должен сработать. Вы также можете попробовать переключиться на другого провайдера интернет-услуг, например, использовать широкополосный интернет вместо мобильного.</p>

Признаки	Возможный тип сбоя в работе сети	Возможные способы смягчения последствий
<p>Отдельные функции/разделы определенных приложений, служб или веб-сайтов не работают или недоступны (например, вы можете создать новую учетную запись, но не можете войти в нее), в то время как все другие приложения или службы функционируют нормально.</p>	<p>Глубокая проверка пакетов (DPI): анализ данных интернет-трафика, проходящих через контрольную точку и использование полученной информации для принятия решения о блокировке прохождения определенных видов данных.</p>	<p>Если у вас есть представление о том, что именно является целью цензуры, вы можете восстановить соединение. Возможные способы смягчения последствий включают в себя использование надежного VPN, инструментов обхода цензуры, таких как Tor браузер, или переключение на другого провайдера интернет-услуг.</p>
<p>Веб-сайт или приложение, которое вы пытаетесь использовать, работает медленно или не отвечает. Иногда они начинают работать, но потом снова не отвечают, становясь все более медлительными.</p>	<p>Отказ обслуживания: переполнение веб-сервера или связанной системы веб-сайта или приложения таким количеством запросов, что они зависают или дают сбой.</p>	<p>Попробуйте получить доступ к сервису или веб-сайту из другой страны, используя VPN. Вы также можете попробовать посетить IP-адрес веб-сайта или сервиса вместо их доменных имен.</p>



Важные примечания

VPN может помочь вам обойти блокировку веб-сайтов или онлайн-платформ, включая такие сервисы как социальные сети и приложения для обмена мгновенными сообщениями. Загрузите несколько VPN заранее, если есть риск отключения интернета.

Не все VPN сервисы могут гарантировать вашу конфиденциальность и предложить определенный уровень защиты. Выбирая VPN-провайдера, предпочитайте инструменты с открытым исходным кодом и прозрачные относительно того, как они защищают ваши данные. Вы также должны убедиться, что VPN-провайдер публично отчитывается о процессах коллегиальной проверки своей безопасности и что их безопасность оценивается независимыми аудиторами. Прочтите [это руководство](#) от Electronic Frontier Foundation, чтобы определить, какие VPN подойдут вам лучше всего в конкретном случае.

Помните: ваш интернет-провайдер или другие люди в вашей сети могут сказать, используете ли вы VPN или Tor. В некоторых странах использование инструментов обхода цензуры и VPN является незаконным или ограничивается. Обязательно учитывайте любые юридические риски и риски для вашей личной безопасности, которые могут возникнуть в результате использования таких инструментов. **#KeepItOn**

Получите помощь

Служба Поддержки по Цифровой Безопасности Access Now

предоставляет техническую поддержку 24/7 журналистам, гражданскому обществу, и правозащитникам на девяти языках, включая русский и английский.