Советы по Цифровой Безопасности для России и Беларуси

ОБНОВЛЕНО: 1 МАР 2022

accessnow

Для чего это руководство

Цифровые угрозы правам человека в России и Беларуси быстро нарастают, поскольку тысячи россиян и белорусов выходят на улицы в знак протеста против своих правительств. Это краткое руководство предназначено для предоставления практических планов действий по цифровой безопасности. Цель состоит в том, чтобы помочь активистам и правозащитникам защитить себя и продолжить свою работу, а также создать устойчивость к кибербезопасности среди гражданского населения. По мере того, как конфликт продолжает развиваться, также изменяются и цифровые угрозы, с которыми вы можете столкнуться, и **Служба Поддержки по Цифровой Безопасности** Access Now всегда готова помочь вам.

Цифровая подготовка - часть 1: защитите свои учетные записи

1. Не делитесь ни с кем своими паролями.
2. Всегда обновляйте свои приложения, системы и программное обеспечение. Совет: включите автоматические обновления.
3. Активируйте **двухфакторную аутентификацию (2FA)** чтобы защитить свои учетные записи.
4. Узнайте, как восстановить скомпрометированные или взломанные учетные записи:
   - **Google**
   - **Twitter**
   - **Instagram**
   - **Facebook** (**Сообщить о взломанных и фейк аккаунтах**)
   - **Apple**
5. Проверьте настройки безопасности вашей учетной записи:
   - **Google**
   - **Tiktok**
   - **Instagram**
   - **Facebook** (теперь вы можете **заблокировать** свой профиль в один щелчок в России)
   - **Twitter**
   - **Apple**

Узнайте больше: **https://digitalfirstaid.org/ru/topics/account-access-issues/**

accessnow

Цифровая подготовка - часть 2: защитите свои данные

1. Сократите объем данных, которые вы сохраняете на своих устройствах, насколько это возможно, особенно информацию о контактах. Имейте в виду, что брать с собой телефон на акцию рискованно, если его конфискуют.
2. Очистите свое присутствие в интернете, прежде чем идти на акцию. Это может помешать троллям доксировать вас.
3. Если вы берете с собой телефон, обязательно сначала сделайте зашифрованную резервную копию.
4. Отключите службы определения местоположения на вашем телефоне.
   a. iOS: Настройки → Конфиденциальность → Службы Геолокации → выключите или настройте его для каждого приложения, если вам нужно использовать «Найти мой iPhone, чтобы удаленно найти или отформатировать свой телефон.
   b. Android: Настройки → Геолокация → выключите (может отличаться в зависимости от модели).
5. Чтобы удалить историю местоположений с карты Google, пройдите **сюда** и **сюда**.

Узнайте больше: **https://securityinabox.org/ru/guide/physical/**

accessnow

Цифровая подготовка — часть 3: обезопасьте свое общение

1. Установите и начните использовать средства **сквозного шифрования (E2E)** для обмена сообщениями со контактами. **Signal** и **Wire** позволяют общаться в чате с шифрованием E2E по умолчанию. **Telegram** позволяет использовать шифрование E2E в чатах один на один в режиме **Секретного Чата.** Включите исчезающие сообщения.
2. Установите протокол связи с надежным человеком, который не пойдет с вами, или с юридической горячей линией, например с помощью секретного кода. Будьте готовы отправить его в срочных обстоятельствах. У устройств Samsung есть **режим SOS**, который позволяет это сделать.
3. Избегайте подключения к общедоступным сетям Wi-Fi (например, в близлежащих отелях или кафе), особенно к тем, которые не защищены надежным паролем. Если вы не пользуетесь мобильным доступом в интернет, включите режим полета. Ваш телефон наиболее безопасен, когда он выключен.
4. Отключите разблокировку телефона по лицу/отпечатку пальца. Вместо этого используйте длинный пароль.

Узнайте больше: **https://securityinabox.org/ru/guide/secure-communication/**

accessnow

В случае отключения интернета или цензуры - часть 1

Возможности подключения и интернет-трафик могут различаться в зависимости от интернет-провайдера (ISP). Для обеспечения связи **приобретите SIM-карты нескольких операторов**, таких как МТС, Билайн, Теле2 и Мегафон в России и A1, МТС и life:) в Беларуси, на случай, если карта одного оператора не работает.

В случае блокировки или цензуры онлайн-контента и коммуникаций могут помочь такие инструменты, как виртуальные частные сети (VPN). На следующих страницах вы найдете подробную информацию о некоторых бесплатных VPN и ёбраузере Tor, включая официальные каналы для их загрузки.

Узнайте побольше о них перейдя на следующую страницу →

accessnow

БЕСПЛАТНЫЕ И ПРОСТЫЕ В ИСПОЛЬЗОВАНИИ VPN

ОБНОВЛЕНО: 1 МАР 2022

MULLVAD

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

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

TUNNELBEAR

Свяжитесь с Службой Цифровой Поддержки Access Now. Заблокирован в RU, используйте режим GhostBear (не для iOS)

VPN который позволяет приватный браузинг 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

AIRVPN

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

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: 1 МАР 2022

PSIPHON

БЕСПЛАТНО

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

LANTERN

БЕСПЛАТНО

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/

PROTONVPN

ProtonVPN

БЕСПЛАТНО (Есть ограничения)

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

TOR BROWSER

БЕСПЛАТНО

Защитите себя от слежки и цензуры

ДОСТУПЕН НА

- → Android
- → Windows
- → MacOS
- → Linux

ЗАГРУЗИТЬ И ИСПОЛЬЗОВАТЬ

https://tor.eff.org/ru/download/

#KeepItOn

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

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 (английский | русский)** от EFF, 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.

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 OONI Probe app например →

accessnow

ТЕСТИРУЙ СВОЕ ИНТЕРНЕТ-СОЕДИНЕНИЕ С OONI

ОБНОВЛЕНО: ФЕВ 2022

OONI

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

OONI PROBE 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 использования мегабайтов данных, особенно когда вы расходуете мобильный трафик.**

Открой ссылку ниже в приложении, чтобы проверить блокировку социальный 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 →

accessnow

Признаки	Возможный тип сбоя в работе сети	Возможные способы смягчения последствий
Все веб-сайты сразу становятся недоступными. Нет подключения к интернету.	**Полное отключение:** отключение, вызванное критическими манипуляциями с инфраструктурой, такими как отключение электросети, вышек сотовой связи или прекращение услуг широкополосного интернета	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.
Веб-сайты и приложения становятся медлительными и неудобными в использовании. Загрузки и / или скачивания занимают намного больше времени, чем обычно.	**Изменение пропускной способности Сети (дросселирование):** намеренное снижение скорости интернета, что затрудняет или делает невозможным загрузку или скачивание информации пользователями	Есть несколько способов осуществить дросселирование сети, и смягчить последствия некоторых из них крайне затруднительно. Для начала вы можете попробовать использовать **VPN**, чтобы оценить, удается ли обойти ограничения пропускной способности сети.

Признаки	Возможный тип сбоя в работе сети	Возможные способы смягчения последствий
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.	**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	Попробуйте использовать **надежный VPN**. **Установите и протестируйте несколько** на случай, если один их 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.
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.	**Сетевая фильтрация:** использование «промежуточных ящиков» (мидлбоксов), установленных в сетевом трафике для нарушения протоколов связи, таких как защищенный протокол передачи гипертекста (HTTPS).	Надежный **VPN** должен сработать. Вы также можете попробовать переключиться на **другого провайдера интернет-услуг**, например, использовать широкополосный интернет вместо мобильного.

Признаки	Возможный тип сбоя в работе сети	Возможные способы смягчения последствий
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.	**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.	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.
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.	**Отказ обслуживания:** переполнение веб-сервера или связанной системы веб-сайта или приложения таким количеством запросов, что они зависают или дают сбой.	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.

Получите помощь и ресурсы

Служба Поддержки по Цифровой Безопасности Access Now предоставляет техническую поддержку 24/7 журналистам, гражданскому оществу, и правозащитникам на девяти языках, включая русский и английский.

Cyber Beaver предоставляет консультации по цифровой безопасности на белорусском, русском и английском.

Самозащита от Слежки (английский | русский) от EFF предоставляет целостный план защиты и меры для отдельных лиц по реализации плана.

Руководства WITNESS по документированию критических событий: **Документирование во время отключений Интернета (английский | русский) и Съемка протестов и злоупотреблений со стороны полиции.**

ОВД-Инфо и **Апология** в России и **Probono.by, Probono.help** (в отношении Украины), **Avocado.help** и **Legal Hub** в Беларуси (доступны через VPN) предоставляют бесплатные юридические справочники, горячие линии и защиту в суде.