# Введение

Существует довольно распространенное заблуждение того, что вы не сможете помешать правительству вашей страны шпионить за вами. Это не так. Не позволяйте страху перед репрессиями со стороны правительства помешать вам высказывать свое мнение. Набор инструментов Ritser Privacy Toolkit разработан, чтобы помочь вам быть в курсе всех событий, оставаясь при этом в безопасности.

# Как работает интернет

Все компьютеры в Интернете имеют IP-адрес, который они используют для связи друг с другом. Веб-сайты также имеют IP-адреса, но для облегчения просмотра в Интернете у них также есть доменные имена (например, www.facebook.com и www.google.com), которые связаны с их IP-адресами. Когда ваш компьютер хочет перейти на www.google.com для выполнения поиска, он получает связанный с этим именем IP-адрес и подключается к соответствующему компьютеру для получения информации, в данном случае результатов поиска Google.

Ваш провайдер интернет-услуг – это та компания, которая подключает ваш компьютер к Интернету. Вероятно, у вас есть модем, подключенный к сети провайдера с помощью телефона, телевидения или оптоволоконного кабеля. А поскольку ваш Интернет проходит через инфраструктуру провайдера, то они могут видеть все данные, которые вы передаете, и на какие IP-адреса отправляете информацию.

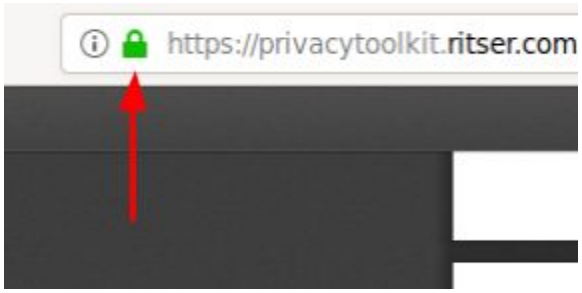

Но это не означает, что они будут знать, какие веб-страницы вы посещаете. Если вы зашифруете свои данные с помощью HTTPS, то они не увидят, что происходит, включая URL (www.google.com/search?q=news). Они будут знать только IP-адрес, к которому вы подключаетесь, время, когда вы подключаетесь, и размер зашифрованных данных, которые вы отправляете.

# Что правительство сможет отследить

Давайте рассмотрим, что может отслеживать правительство или интернет-провайдер. Предполагая, что вы используете HTTPS, ваше правительство может отслеживать, какие веб-сайты вы используете и когда. Это означает, что они смогут узнать, что вы получили доступ к IP-адресу www.facebook.com в 19:38, но они не узнают, какие страницы или профили вы открывали. Они будут знать только, что вы посетили www.facebook.com.

Если вы не используете HTTPS, ваше правительство сможет отслеживать также и то, что вы отправляете на сайт. Сюда входят пароли и URL-адреса.

Но как узнать, что вы используете HTTPS? Обычно ваш браузер отображает символ блокировки, как показано ниже, когда вы используете HTTPS.




HTTPS работает путем шифрования данных между вашим браузером и веб-сайтом. Это означает, что он использует математические алгоритмы, чтобы гарантировать то, что эти данные не читаются во время передачи. Современные алгоритмы шифрования считаются безопасными, поскольку даже самые могущественные спецслужбы не в состоянии их взломать.

Незашифрованные соединения (HTTP без S) выглядят так:

**Из:** 70.210.154.182

**На:** 103.190.246.203 (baidu.com)

**Время:** 4:42 утра 2020-09-02

**Данные (70 байт):**

Посещенная веб-страница: baidu.com/account

Имя пользователя: alex2

пароль: password

Зашифрованные соединения (HTTPS) выглядят так:

**Из:** 70.210.154.182

**На:** 103.190.246.203 (baidu.com)

**Время:** 4:42 утра 2020-09-02

**Данные (68 байт):**

o866)F(Yu~1]TEjP47h6(vIEs!dq_'|/Sl^ZMbFriN_"LejUyUYZ%d?sRx;F##Coq9M&

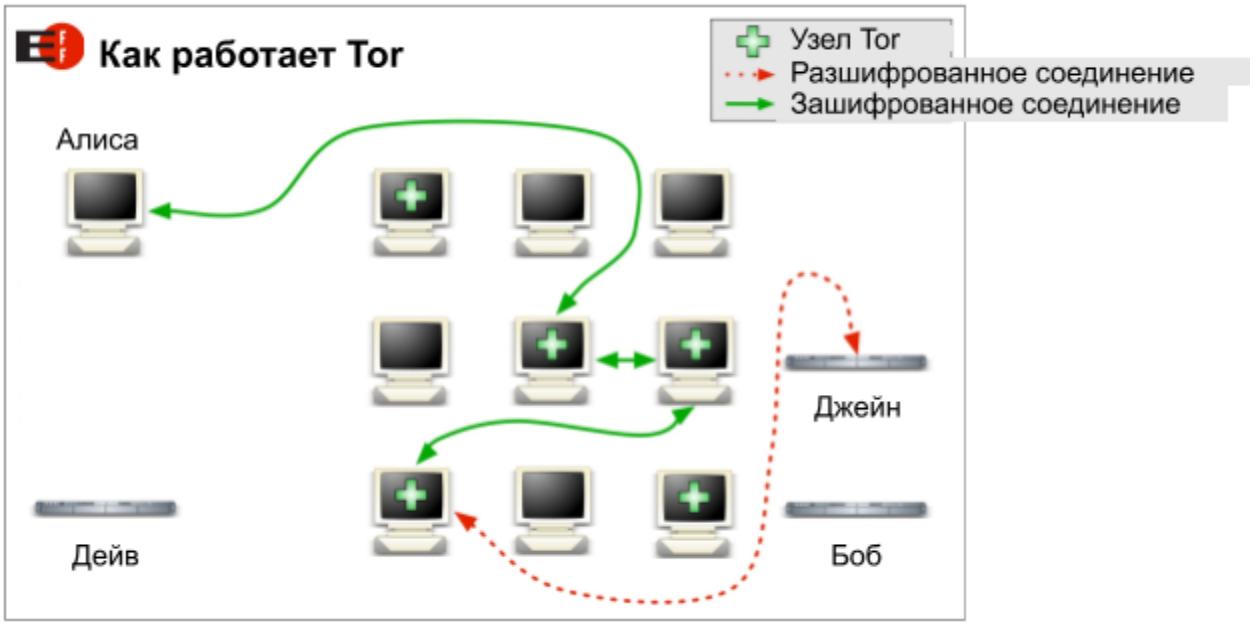
# Какие данные правительство может отслеживать с помощью владельцев сайтов

Однако HTTPS не **мешает** веб-сайту передавать ваши данные в полицию. Каждый веб-сайт, к которому вы обращаетесь в Интернете, может видеть ваш IP-адрес. Если веб-сайт решает предоставить правительству IP-адрес вашей учетной записи, они могут использовать его**, чтобы вычислить ваш реальный адрес.** Важно убедиться, что власти не могут найти IP-адреса ваших учетных записей в Интернете.

На крупных веб-сайтах, таких как Facebook, Reddit и Google, есть процедуры для обработки правительственных запросов на получение пользовательских данных. Этот процесс обычно в некоторой степени прозрачен и справедлив, поскольку они обычно игнорируют законы авторитарных правительств. Например, в период с 2014 по 2018 год Google обработал 3 запроса на данные египетских пользователей и все их отклонил.

## Скрытие вашей личности от веб-сайтов

Однако отдавать свою безопасность в руки многонациональных коммерческих корпораций – не лучший вариант. Если вы живете в стране, где ваша безопасность находится под угрозой в случае раскрытия вашей личности, рекомендуется использовать браузер Tor (входит в этот набор инструментов). Tor скрывает ваш IP-адрес, отправляя интернет-трафик через другие компьютеры. И получается, что сам сайт, к которому вы обращаетесь, сможет видеть лишь IP адрес последнего компьютера вместо вашего. Ваше правительство будет знать, что вы используете Tor, но они не будут знать, что вы отправляете через него и с кем общаетесь.




Еще одно преимущество использования Tor заключается в том, что, поскольку интернет-провайдер не знает, к каким веб-сайтам вы обращаетесь, он не сможет их заблокировать.

Однако Tor не безупречен. Если правительству известно ваше примерное местоположение, а владелец веб-сайта сообщает им, что вы используете Tor, то они могут проверить, кто использовал сервера Tor в этом месте в то время, когда вы просматривали веб-сайт, чтобы определить вашу настоящую личность. ФБР делало это раньше, но это редко вызывало проблемы. Если для вас это особо важно, вы можете использовать общедоступный Wi-Fi.

**Примечание:** VPN сети не так эффективны, как Tor, если речь идет о сохранении вашей анонимности в сети.

## Очевидное

Обычно людей ловят не из-за того, что правительство получает их IP-адреса. А из-за того, что они отправляют в Интернет то, что может раскрыть их личность или же они излишне откровенничают со своими друзьями. Людей ловят на глупых ошибках. Вот несколько правил, которые вы всегда должны соблюдать:

1. Делясь своей историей, будьте расплывчаты и попытайтесь просто перекрутить детали. Самая незначительная информация, такая как количество ваших братьев и сестер, может быть использована для раскрытия вашей личности.
2. Будьте **очень** осторожны при отправке фотографий в Интернет. Очистите данные EXIF со всех загружаемых снимков и убедитесь, что нет никаких сведений, которые могут быть использованы для вашей идентификации.
3. Если ваш компьютер используют другие люди, убедитесь, что ваша история просмотров не сохраняется. Не сохраняйте на свой компьютер ничего, что может выдать вашу личность.
4. Не используйте свое настоящее имя для регистрации учетных записей, анонимной идентификации.
5. Не раскрывайте свой псевдоним людям, которых вы знаете в реальной жизни.
6. Не раскрывайте свою настоящую личность людям, которых вы знаете, через свой псевдоним.

## Вывод

Если вы создаете анонимные учетные записи Reddit или Facebook, на какое-то время вы сможете оставаться в безопасности. Но вы можете не доверять полностью этим компаниям, если от этого зависит ваша жизнь. Если вы хотите быть уверены, что остаетесь анонимным, то используйте Tor. PrivacyTools – это хороший ресурс для любого программного обеспечения, ориентированного на конфиденциальность.

И помните: только вы несете ответственность за свою безопасность!