

Написание статьи вызвана совершенным оборзением власти в целом и государственной думы в частности. По всей видимости, в нашей стране больше нечем заняться, видимо нет больше проблем, поэтому власти срочно озаботились введением цензуры и закрытием доступа к ресурсам в сети интернет: **http://ru.wikipedia.org/wiki/Википедия:Законопроект_№_89417-6**.



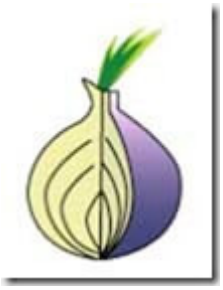
Те, кто скажут, что данное решение правильно и надо оградить детей от порнографии и т.д., смело могут идти на йух. Нужно смотреть за тем, что делают ваши дети и направлять их на путь истинный, а не всякой хренью заниматься.

Каждый должен выбирать сам то, что ему нужно. Никакое засратое правительство не имеет на это совершенно никакого права. Заебали переделывать под себя законы.

Доступ к ресурсам интернета, вообще, и Википедии (ru.wikipedia.org), в частности, должен быть свободным.

Альтернативных вариантов для свободного доступа к информации я знаю пока два. Это система **“Tor”** и проект **“I2P”**.

“Tor”



Использование **Tor** защищает вас от частой формы наблюдения в Internet, известной как "анализ потока данных". Анализ потока данных позволяет узнать кто с кем общается по публичным сетям. Знание источника и приёмника вашего Интернет-трафика позволяет третьим сторонам отслеживать ваше поведение и интересы в Сети.
Почитать о его использовании и применении можно например тут: http://rutracker.org/forum/viewtopic.php?t=576626

Сразу уточню один момент. Данная сеть очень известна, в том числе благодаря СМИ, и уже была не раз скомпрометирована. Поэтому реальность попадание за использование Tor-а (особенно в том случае, вы будете являться одним из Tor-серверов в сети и через вас пойдет левый трафик) в места не столь отдаленные становиться и в нашей стране все реальнее. **Будьте бдительны**.

В прочем для ежедневного использования я бы мог посоветовать использовать **Tor Browser Bundle**. Скачать его можно по следующей ссылке: https://www.torproject.org/download/download-easy.html.en. На этом же сайте можно найти простое и понятное видео по его использованию, например здесь: https://www.torproject.org/projects/torbrowser.html.en. Раздел называется "Quick videos on how to use TBB". Знание английского, думаю, не потребуется.

“I2P”

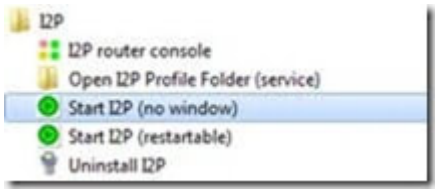


I2P «Проект Невидимый Интернет» - представляет собой анонимную, самоорганизующуюся, распределённую и опенсорсную децентрализованную сеть, которая в свою очередь представляет всего лишь связку туннелей, передающих зашифрованные данные через Интернет.

Дополнительно по этой теме можно почитать еще здесь:
http://lurkmore.to/I2P
http://ru.wikipedia.org/wiki/I2P
http://habrahabr.ru/post/97827/
http://habrahabr.ru/post/143516/

Для установки **“I2P”**.необходимо предварительно скачать среду **Java Runtime**: http://java.com/ru/download/index.jsp. На момент написания статьи, таковой была версия: jre 7 update 5 for windows. Скачиваем и устанавливаем.

Теперь скачиваем последнюю версию **I2P** здесь: http://www.i2p2.de/download и далее производим инсталляцию. На момент написания статьи, последней версией была i2p install 0.9 for windows. Установщик уже содержит и соответственно предлагает автоматом русский язык.

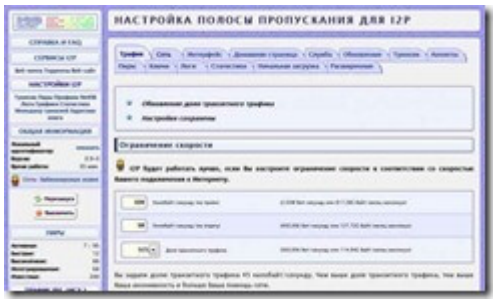


После установки в меню пуск появится папка I2P, в ней необходимо выбрать и запустить “Start I2P (no window)”.

Далее будет запущено окно браузера выбранного по-умолчанию. Картинка ниже.



Здесь нам рекомендуется зайти на страницу конфигурировании (http://127.0.0.1:7657/config), где будет необходимо указать скорость входящего/исходящего соединения и долю транзитного трафика, чем больше последний параметр, тем выше должны быть анонимность.



Далее нам необходимо зайди в окно настройки сети нашего браузера и указать следующие параметры:

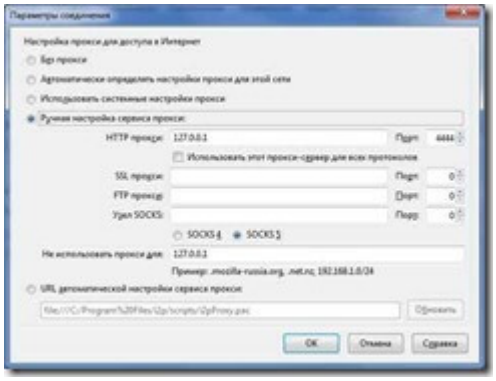
для использования HTTP proxy, адрес 127.0.0.1 порт 4444

для использования HTTPS Proxy, адрес 127.0.0.1 порт 4445

В интернета, на каждом сайте рекомендуют использовать строку:

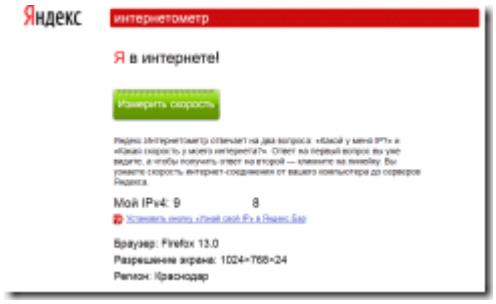
C:Program Filesi2pscriptsi2pProxy.pac

Ее использование мне дало возможность заходит на сайта с вида **.i2p, ничего более. Т.е. как такового прокси не сработало. Поэтому я использовал вариант HTTP proxy, адрес 127.0.0.1 порт 4444, как показано на картинке ниже.

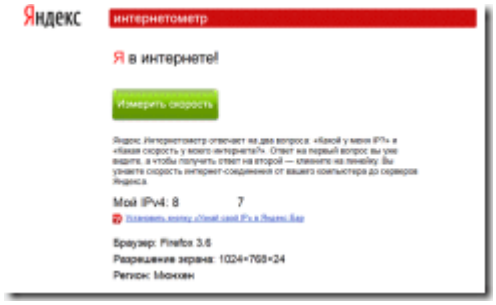


А теперь может увидеть результаты использования «Проекта Невидимый Интернет».

Итак. Вначале я вполне обаянный пользователь, находящийся где-то на территории города Краснодара. Сейчас можно определить: какой у меня браузер и какая версия, разрешение рабочего стола, мой ip-адрес, мой населенный пункт, моего провайдера и много другой информации.



Теперь включаем прокси. И вот я уже западно-европейский юзер, пытаюсь прощемиться на просторы интернета из города Мюнхена, столицы федеральной земли Баварии. Кстати, Google будет иметь зону de. Т.е. мы, практически, граждане Федеративной Республики Германия.



В завершении хочется отметить тот факт, что, несмотря немалую защищенность туннелей I2P, на территории СНГ эта система мало используется и весь трафик дружно топает за границу. Вывод очевиден. Скорость работы, зачастую, оставляет желать лучше. Поэтому на повседневную работу рекомендовать использование I2P достаточно сложно. Совет один: попробуйте экспериментальным путем выяснить насколько стабильно ведет себе система именно в вашем регионе.