# Обходим Великий Российский Файрвол

Часть 1 из 5

**В России официально установлена цензура Интернета. Но контролировать Интернет не так просто, как это может показаться с первого взгляда.**


**I2P** — анонимная оверлейная сеть, использующая принцип чесночной маршрутизации, исходные коды которой распространяются на условиях нескольких свободных лицензий. В отличии от Tor, который в первую очередь направлен на доступ к сайтам обычного интернета (хотя в нем и существуют скрытые сервисы, аналогичные ипсайтам в I2P, а в I2P можно получить доступ к внешнему Интернету, используя аутпрокси), основной целью I2P является доступ именно к скрытым ресурсам — ипсайтам. Ипсайт от обычного вебсайта отличает только его нахождение в сети I2P.

> **!** Никогда не используйте анонимные сети с настройками, которые позволяют использовать Интернет в одном браузере в обход самой сети. В этом случае будет достаточно вставить любое изображение из внешнего Интернета, чтобы получить ваш реальный IP-адрес.

## Установка

Для установки посетите `http://i2p2.de` или установите пакет с помощью пакетного менеджера вашего дистрибутива.

## Использование

> **!** Не используйте аутпрокси для передачи конфиденциальных данных, владелец аутпрокси видит трафик нешифрованным.

После установки настройте свой браузер на использование HTTP-прокси 127.0.0.1:4444 и посетите страницу `http://127.0.0.1:7657`. Перед вами консоль маршрутизатора I2P — место, из которого можно управлять всеми настройками I2P.
Для начала перейдите в меню «Настройки I2P» (`http://127.0.0.1:7657/config`) и установите ограничения скорости в соответствии со скоростью вашего интернета.
Остальные настройки можно оставить по умолчанию. Подождите некоторое время для полноценной интеграции с сетью, после чего вы сможете полноценно пользоваться сетью. Роутер желательно не выключать, так как при его перезапуске потребуется придется повторить этот процесс.
В I2P отсутствуют корневые DNS-сервера, копия адресной книги хранится на каждом роутере. На `http://rus.i2p` вы можете найти дополнительный список подписок, который можно добавить в susidns.

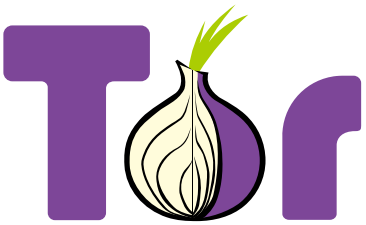
## Некоторые ипсайты

1. `http://forum.i2p` — главный форум, есть рускоязычный раздел.
2. `http://rus.i2p` — русская I2P-вики.
3. `http://pastethis.i2p` — pastebin-подобный ресурс.
4. `http://flibusta.i2p` — зеркало Флибусты, крупной библиотеки электронных книг.
5. `http://tracker.rus.i2p` — русский торрент-трекер в I2P.

# Обходим Великий Российский Файрвол

Часть 2 из 5

**В России официально установлена цензура Интернета. Но контролировать Интернет не так просто, как это может показаться с первого взгляда.**



**Tor** — анонимная оверлейная сеть, использующая принцип луковой маршрутизации, исходные коды которой распространяются на условиях лицензии BSD.
**Луковая маршрутизация** — технология анонимного обмена информацией, использующая многократное шифрование и пересылку через цепочки узлов. Каждый луковый маршрутизатор в цепочке удаляет слой шифрования и пересылает сообщение дальше, согласно полученным инструкциям, где все повторится. И так до тех пор, пока сообщение не достигнет адресата. Такое название технология получила из-за сходства данного процесса с очисткой луковицы.

> **!** Никогда не используйте анонимные сети с настройками, которые позволяют использовать Интернет в одном браузере в обход самой сети. В этом случае будет достаточно вставить любое изображение из внешнего Интернета, чтобы получить ваш реальный IP-адрес.

## Установка

Для установки посетите `https://torproject.org` или установите пакет с помощью пакетного менеджера вашего дистрибутива.

## Использование

> **!** Не забывайте, что при использовании обычного Интернета через Tor, последняя нода в цепочке (exit-нода) видит трафик нешифрованным.

Самым простым способом использования Tor является установка Tor Browser Bundle. Просто скачайте его с `https://torproject.org/projects/torbrowser.html`, распакуйте и запустите.
Вы также можете установить Tor и задать в настройках приложений, которые вы хотите через него использовать, адрес socks5-прокси 127.0.0.1:9050.
Для использования приложений через Tor, не имеющих настроек прокси, скачайте torsocks — `https://code.google.com/p/torsocks`.

## Некоторые скрытые сервисы

1. `http://dppmfxaacucguzpc.onion` — TorDir, каталог скрытых сервисов.
2. `http://jhiwjjlqpyawmpjx.onion` — TorMail, электронная почта в Tor.
3. `http://silkroadvb5piz3r.onion` — Silk Road, анонимная торговая площадка, принимающая оплату в Bitcoin.
4. `http://4eiruntyxxbgfv7o.onion/pm` — TorPM, сервис обмена сообщениями.
5. `http://c4wcxidkfhvmzhw6.onion` — PrivacyBox, сервис анонимных контактных форм.

# Обходим Великий Российский Файрвол

Часть 3 из 5

**В России официально установлена цензура Интернета. Но контролировать Интернет не так просто, как это может показаться с первого взгляда.**

**VPN** — технология, позволяющая создавать сети поверх существующего Интернет-подключения. Из-за высокой скорости работы, простоты настройки и шифрования трафика от клиента до VPN-провайдера часто используется как средство сокрытия реального IP-адреса при доступе в Интернет. VPN-провайдеры обычно предоставляют свои услуги на платной основе.
**SSH** — протокол, созданный для безопасной передачи данных. Часто используется для удаленного управления другими компьютерами, но может использоваться и для создания туннелей.
**SSH-туннель** — туннель, созданный с помощью SSH-соединения и используемый для передачи данных. Существуют организации, предоставляющие SSH-туннелирование на платной основе.

## Использование

> ! Не забывайте, что хозяин VPN-сервиса или SSH-туннеля видит трафик нешифрованным.

При использовании VPN, следуйте инструкциям, полученным от вашего VPN-провайдера.
SSH-туннели настраиваются так:

```
ssh –D localhost:port login@address
```

port — порт, трафик на который будет пропускаться через SSH-туннель.
login — ваш логин на удаленном сервере.
address — адрес удаленного сервера.
После этого установите в приложениях, трафик которых вы хотите туннелировать, например, в браузере, адрес SOCKS-прокси localhost с портом, который вы указали в предыдущем шаге.

## Некоторые VPN-провайдеры

1. `https://ipredator.se`
2. `https://kebrum.com`
3. `https://relakks.com`
4. `https://vpntunnel.se`
5. `http://ivacy.com`

## Некоторые провайдеры SSH-туннелей

1. `https://tunnelr.com`
2. `http://torvpn.com`
3. `http://vpnsecure.me`
4. `http://guardster.com`
5. `http://anonyproz.com`

# Обходим Великий Российский Файрвол

Часть 4 из 5

**В России официально установлена цензура Интернета. Но контролировать Интернет не так просто, как это может показаться с первого взгляда.**

**JonDo** (**JonDonym**, также **Java Anon Proxy** или **JAP**) — программное обеспечение, представляющее доступ к цепочке прокси-серверов.

## Установка

Для установки посетите `https://anonymous-proxy-servers.net` или установите пакет с помощью пакетного менеджера вашего дистрибутива.

## Использование

> **!** Не забывайте, что хозяева выходных нод видят трафик нешифрованным.

JonDo напоминает Tor, но в отличии от Tor, где каждый доброволец может поднять как промежуточный сервер, так и exit-ноду, JonDo опирается на помощь отдельных организаций. Однако, Tor может использоваться в цепочке JonDo, для этого достаточно добавить адрес socks5-прокси Tor. Бесплатная версия позволяет проксировать только HTTP и HTTPS трафик, в платной версии доступно все, а также нелимитирована скорость.
Для использования запустите JonDo и настройте браузер на использование прокси-сервера 127.0.0.1:4001.

## Недостатки

1. В бесплатной версии можно проксировать только HTTP и HTTPS.
2. В бесплатной версии скорость ограничена до 30–50 кБит/с.
3. В бесплатной версии размер передаваемого файла ограничен 2 МБ.
4. Число нод очень сильно ограничено.

# Обходим Великий Российский Файрвол

Часть 5 из 5

**В России официально установлена цензура Интернета. Но контролировать Интернет не так просто, как это может показаться с первого взгляда.**

**Прокси-сервер** — сервер, который позволяет пропускать через себя пользовательский трафик.
**Веб-прокси** — веб-страница, которая позволяет пользователю получить контент с заданного адреса через себя.

## Использование

> **!** Не забывайте, что хозяева прокси-серверов и анонимайзеров видят трафик нешифрованным.

> **!** Некоторые прокси-сервера передают заголовок X-Forwarded-For с реальным IP-адресом клиента.

В случае использования прокси, просто задайте его адрес в настройках браузера и других приложений, которые вы хотите использовать через прокси.
В случае использования веб-прокси, перейдите на его страницу и введите адрес сайта, который вы хотете посетить.

## Списки открытых прокси

1. `http://xroxy.com`
2. `https://hidemyass.com/proxy-list`
3. `http://freeproxy.ch`
4. `http://proxylists.net`
5. `http://nntime.com`

## Некоторые веб-прокси

1. `https://hidemyass.com`
2. `http://anonymouse.org`
3. `http://hide.pl`
4. `http://hideme.ru`
5. `http://guardster.com/free/`