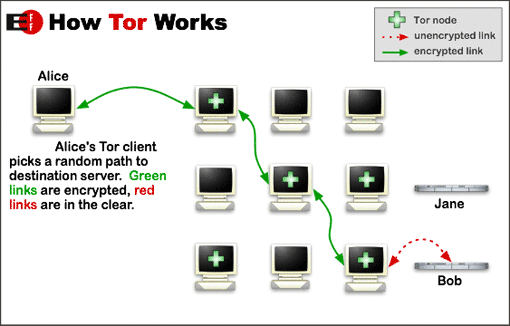
Работа с браузером TOR

Для начала скачайте и установите браузер - <https://www.torproject.org/>

Пользователи сети Tor запускают «луковый» прокси-сервер на своей машине, который подключается к серверам Tor, периодически образуя цепочку сквозь сеть Tor, которая использует многоуровневое шифрование. Каждый пакет данных, попадающий в систему, проходит через три различных прокси-сервера — узла, которые выбираются случайным образом. Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьего узла, потом для второго и в конце, для первого. Когда первый узел получает пакет, он расшифровывает «верхний» слой шифра (аналогия с тем, как чистят луковицу) и узнаёт, куда отправить пакет дальше. Второй и третий сервер поступают аналогичным образом. В то же время, программное обеспечение «лукового» прокси-сервера предоставляет SOCKS-интерфейс. Программы, работающие по SOCKS-интерфейсу, могут быть настроены на работу через сеть Tor, который, мультиплексируя трафик, направляет его через виртуальную цепочку Tor и обеспечивает анонимный веб-сёрфинг в сети.

Внутри сети Tor трафик перенаправляется от одного маршрутизатора к другому и окончательно достигает точки выхода, из которой чистый (нешифрованный) пакет данных уже доходит до изначального адреса получателя (сервера). Трафик от получателя обратно направляется в точку выхода сети Tor.



## Преимущества Tor

### Удобный для пользователя

Браузер Tor подобен большинству браузеров, которыми вы пользовались прежде. Он доступен для многих людей и обладает дружелюбным интерфейсом, что делает его простым и удобным в использовании.

### Бесплатный

Браузер Tor бесплатен для скачивания и использования. Более продвинутые пользователи могут скачать проект с открытым исходным кодом и внести требуемые изменения в исходный код.

Обеспечивает безопасность вашей конфиденциальности

Tor защищает вашу конфиденциальность, не раскрывая ваш IP-адрес на посещаемых вами сайтах. Любой человек, будь то журналист, представитель политической оппозиции или среднестатистический гражданин, может использовать эту платформу, чтобы защитить свою информацию от чрезмерно ограничивающих свободу правительств или крупных корпораций.

## Минусы

### Низкая скорость

Поскольку трафик проходит через множество ретрансляторов, то зачастую можно наблюдать задержку в отображении контента. В частности, фото и виде могут иметь проблемы с загрузкой. Чем больше пользователей, которые не размещают ретранслятор, тем медленнее работает вся цепочка.

### Блокировка веб-служб

Многие крупные веб-сервисы блокируют доступ к Tor. При посещении такие сайты возвращают сообщение об ошибке, например, 404. Другие разрешают доступ, но включают на сайте целый лабиринт [капчей (CAPTCHA)](https://www.cloudav.ru/mediacenter/security/captcha-future/), в которых необходимо ввести проверочный код.

### Проблемы с законом

Браузер Tor может использоваться каждым. Если кто-то занимается незаконной деятельностью, а вы являетесь конечным ретранслятором, то весь трафик такого пользователя будет приводить к вам. Спецслужбы очень настороженно относятся к пользователям Tor, а потому внимательно следят за ними. Просто в силу того, что вы являетесь пользователем Tor, вы можете быть помечены как потенциальный преступник, а потому все ваши действия будут отслеживаться.

Что нужно посмотреть в Tore:

1) Попробуйте зайти на сайты, недоступные из других браузеров. Есть ли те, которые заблокированы даже через Tor?

2) Попробуйте авторизоваться в самых популярных интернет сервисах (вк, facebook, youtube и прочее), если возникнут проблемы - описать их. Также сравните эти сервисы с разными уровнями безопасности (найдёте в настройках Tor’a “Приватность и защита”). Опишите разницу.

3) Сравните скорость интернета в обычном браузере и в Торе. Желательно несколько раз. Сделайте выводы.

4) Попробуйте найти сайты с доменом .onion через обычный браузер. После опробуйте их в Tor’е. Найдите полезный сайт с подобным доменом и кратко опишите его.