СВОБОДА СЛОВА и ИНТЕРНЕТ.

(Статья ориентирована на рядового пользователя с минимальным уровнем IT – подготовки)

В рамках закона о свободном доступе к информации сейчас возможны проблемы с его выполнением. Часто задается вопрос - "что делать, если мне блокируют интернет?" Попытаюсь ответить общедоступным языком о механизмах такой блокировки и _индивидуальной_ возможности вернуть себе право свободного доступа к информации.

1) ФИЗИЧЕСКИЙ УРОВЕНЬ

Обмен информацией между точками "А" и "Б" возможно только в том случае, если физически существует некоторая среда, через которую эту информацию можно передать. Очевидно, если Вас отсоединили на физическом уровне (провайдер полностью отключил Вас от интернет или Wi-Fi - радиоканалы наглухо забили шумами) все ваши индивидуальные усилия будут безрезультативными.
Каким же образом рядовой пользователь может убедиться в наличие доступа в интернет. Для тех, кто использует Windows (а это основной массив рядовых пользователей) следует использовать встроенную программу ping:

1.1) Через меню "Пуск/Стандартные/Командная строка" запускаете окно Windows для запуска программ в ручном режиме (фактически Вы запускаете программу CMD)

1.2) В строке приглашения ввода набираете текст запуска программы ping. Например: ping facebook.com Далее нажимаем Enter и если интернет и узел facebook.com Вам доступны получаете ответ, который, как правило, содержит несколько повторяющихся строк следующего вида:

"Ответ от 173.252.110.27: число байтов=32 время=138mc TTL=83"

```
C:\>ping facebook.com

Обмен пакетами с facebook.com [173.252.110.27] по 32 байт:

Ответ от 173.252.110.27: число байт=32 время=138мс TTL=83
Ответ от 173.252.110.27: число байт=32 время=137мс TTL=83
Ответ от 173.252.110.27: число байт=32 время=150мс TTL=83
Ответ от 173.252.110.27: число байт=32 время=137мс TTL=83

Статистика Ping для 173.252.110.27:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 137мсек, Максимальное = 150 мсек, Среднее = 140 мсек
```

В этом ответе для нас важно следующее:

1.2.1) IP адрес узла facebook.com или 173.252.110.27 Внимание, такие адреса потребуются нам далее.
1.2.2) Время=138mc, которое отражает длительность прохождения информации между Вами и facebook.com. Это время может немного варьироваться в зависимости от загрузки глобальной сети.

1.2.3) Кроме того, следует обратить внимание на количество отправленных и полученных пакетов в статистике отчета ping. Если эти числа не совпадают, то связь с интернет неустойчивая (причина: шумы, значительная перегрузка сети).

Естественно у Вас возникает вопрос - а где взять имена узлов (например, facebook.com)? Ответ прост:

1.3) Запустите свой броузер и с помощью закладок обратитесь к некоторому сайту (например: http://www.gismeteo.ua/city/legacy/4944/).
Далее скопируйте для ping доменный адрес узла, то есть www.gismeteo.ua .
Выполняя ping www.gismeteo.ua Вы получите IP адрес 217.20.175.60 этого узла.
Теперь используйте в адресной строке броузера вместо имени www.gismeteo.ua IP - адрес 217.20.175.60 то есть:

http://217.20.175.60/city/legacy/4944/

и нажмите Enter. При нормальном доступе Вы увидите запрошенную Вами страницу с погодой в Киеве.

1.4) Если некоторый сайт с нейтральным контентом откликается в броузере как на обычный доменный адрес, так и на IP адрес, а вот сайты с интересным для Вас контентом не доступны посредством доменного адреса, то это явный признак проблем.

СОВЕТ - ЗАРАНЕЕ ЗАГОТОВЬТЕ IP адреса интересных для Вас узлов.

ВНИМАНИЕ. Если вы обнаружили, что на ping не реагирует ни один внешний узел, более того не отвечает узел Вашего провайдера, то это признак того, что у Вас технические неполадки с доступом. В этом случае следует проверить кабели, разъемы и так далее, уточнить у Вашего провайдера наличие технических проблем (это выясняется звонком по телефону), либо констатировать (и это очень печально) что Вас полностью отключил провайдер.

Все что написано в следующих разделах имеет смысл, только в том случае, если Ваш доступ ограничен только частично.

2) АДРЕСНЫЙ УРОВЕНЬ

Предположим, проверяя физическую доступность узлов интернет, мы обнаружили проблемную ситуацию 1.4. Такая ситуация возникает в цепочке по которой Ваш броузер взаимодействует с целевым сайтом. Эта цепочка работает следующим образом:

2.1. Броузер запрашивает доменный адрес целевого сайта и как результат запроса получает IP адрес этого сайта. После чего, в невидимом для Вас режиме, броузер посылает IP запросы на получение HTML - страницы и элементов этой страницы для их отображения на Вашем мониторе. Для преобразования доменного адреса в IP адрес применяется специальное программное или программно - аппаратное решение (DNS-сервер : http://ru.wikipedia.org/wiki/DNS-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80), с которым Вы выполняете взаимодействие, начиная от соединения с Вашим провайдером. Указанная проблемная ситуация возникает когда:

2.2.1) В распределенном по узлам провайдеров сервисе DNS возникают сбои. Причины таких сбоев весьма разнообразны начиная от локальных ошибок на узлах отдельных провайдеров и завершая ошибками репликации или обмена DNS - информацией между серверами провайдеров. В этом случае можно перенастроить ссылку на DNS - сервер, используя в соединении с провайдером IP - адрес на устойчивом к нагрузкам узле. Например, ссылкой на Google:

> The Google Public DNS IP addresses (IPv4) are as follows:
> 8.8.8.8
> 8.8.4.4
> The Google Public DNS IPv6 addresses are as follows:
> 2001:4860:4860::8888
> 2001:4860:4860::8844
>
> Эти адреса, а также способ их использования вы можете уточнить по следующей ссылке:https://developers.google.com/speed/public-dns/docs/using?hl=ru
> Подробнее смотрите в приложениях 5.1, 5.2.

Однако для рядового пользователя эта операция достаточно сложная и такому пользователю лучше некоторое время подождать ибо, как правило, провайдеры применяют максимум усилий для устранения подобного рода сбоев. Следует подчеркнуть, что иногда такие сбои охватывают целые регионы (например: http://zn.ua/TECHNOLOGIES/v-kitae-proizoshel-krupneyshiy-v-istorii-interneta-sboy-137291_.html) и устраняются несколько дней. Однако в типичном случае на восстановление затрачивается от десятков минут до нескольких часов.

2.2.2) Совсем другой случай, когда провайдер осознанно устанавливает блокировку (фильтр) на отдельные доменные адреса или (чаще) группы адресов (например используется специально настроенный DNSBL - сервер
см. http://ru.wikipedia.org/wiki/DNSBL). Такая мера провайдера чувствительна для рядового пользователя, но малоэффективна в отношении пользователя с хорошей IT-подготовкой.
По этой причине, вместо DNS – фильтров, провайдеры устанавливают фильтрацию на конкретные IP адреса или группы таких адресов.
В таком случае для рядового пользователя остаются только инструменты перенаправления своих запросов через другие узлы в обход фильтров провайдера, причем возникает необходимость максимально маскировать такие запросы для фильтров провайдера.
Наиболее распространенными средствами для решения названной задачи являются анонимные (открытые) proxy - сервера (см. http://ru.wikipedia.org/wiki/Proxy_server), либо анонимные (открытые) VPN - сервера (см. http://ru.wikipedia.org/wiki/VPN). Открытыми называют сервера, к которым может получить доступ любой пользователь сети интернет. Об этих серверах поговорим ниже.

3) АНОНИМНЫЕ (ОТКРЫТЫЕ) PROXY и VPN СЕРВЕРА

Вначале разберемся, что это такое proxy - сервер или VPN - канал.

3.1) ОТКРЫТЫЙ PROXY - СЕРВЕР.

Функцию такого сервера проще всего определить как некоторый сервис, который выполняет преобразование IP - адресов в двух направлениях, временно запоминая связь соединения для однозначного движения информации от пользователя в сеть и обратно.

Если провайдер не заблокировал IP адрес узла, который предоставляет возможность такого преобразования, то пользователь имеет возможность, установив proxy – соединение, обойти установленный провайдером фильтр целевого IP адреса. Это происходит следующим образом:

3.1.1) Рядовой пользователь в броузере запрашивает WEB-сайт узла с анонимным proxy - сервером. Получив WEB-страницу этого сайта, он вводит в некоторое поле этой страницы доменный адрес WEB-сайта, который его интересует.

3.1.2) Proxy - сервер выполняет преобразование доменного адреса запрошенной Вами страницы в IP адрес с помощью своего DNS - сервера (то есть в обход всех фильтров блокирующего провайдера) и отправляет Ваш запрос от имени собственного IP адреса.

3.1.3) Получая ответ от целевого сервера (получая целевую страницу) proxy - сервер переадресует информацию на Ваш IP адрес, причем отправляя Вашу страницу от своего имени. В этом смысле, для провайдера, установившего
блокировку, Ваш броузер работает только с WEB-сайтом на который им не установлены ограничения (если это действительно так).

Как легко догадаться, что доменные и IP адреса таких proxy-серверов легко отслеживаются при их публичном распространении, а следовательно те, кто имеет виляние на провайдеров, могут обязать эти адреса внести в список блокируемых для конечных пользователей. Сегодня уже широко известным
proxy - сервером такого типа является http://hidemyass.com/proxy/

Кроме того, существуют списки бесплатных proxy - серверов с несколько другими правилами взаимодействия, который можно найти по доменному адресу http://hideme.ru/proxy-list/ В таких списках (а их можно нагуглить), как правило, отражается время последней проверки их доступности.

3.2) VPN - КАНАЛ.

VPN - канал, как инструмент, разрабатывался для объединения посредством интернет отдельных корпоративных локальных сетей (разбросанных по всему миру) в единую локальную сеть.
При этом в качестве основной задачи, ставилась задача защиты информации (бизнес - информации) от ее перехвата в среде интернет. Таким образом, защита информации определила структуру решения этой задачи в виде специальных кодирующих / декодирующих средств, как на стороне источника, так и на стороне приемника.
Кроме шифрования информации VPN (Virtual Private Network) - канал выполняет еще одну важную функцию. Для ее понимания необходимо понимать, что информация в сетях передается пакетами (порциями) организация которых включает заголовок (или адреса доставки и характеристики пакета), собственно данные, а также трейлер (хвост), который содержит информацию для контроля целостности пакета и исправления ошибок. В VPN - передающая сторона шифрует исходный пакет из локальной сети (либо одиночной машинки), потом одевает на зашифрованный пакет новый заголовок с IP-адресами доставки пакета в сети интернет, а приемная сторона соответственно снимает такой транспортный заголовок и трейлер, дешифрует информацию и, тем самым, восстанавливает исходный пакет. Такой восстановленный исходный пакет, попадая в удаленный сегмент внутренней, локальной сети, достигает внутреннего адресата и (в этом смысле) неотличим от других внутренних пакетов.

Другими словами это очень похоже на доставку грузов сторонними перевозчиками (интернет транспортом) в прочно запечатанных контейнерах (зашифрованных пакетах). Как правило, для работы с VPN – каналом используются дополнительное программное или аппаратно – программное обеспечение. Для пользовательской стороны чаще всего используются специальные драйверы или сервисы (например http://openvpn.net/).
В старших версиях Windows, а также многих других операционных системах уже появились встроенные возможности. О том, как такие возможности можно использовать, обстоятельно описано в следующей статье:
http://av.3dn.ru/publ/kompjuternaja_bezopasnost/kak_obezopasit_sebja_v_otkrytykh_setjakh_wi_fi_s_pomoshhju_vpn/4-1-0-31 .

При солидной защите содержимого пользовательской информации, VPN – канал (в том числе и к открытому VPN – серверу) остается беззащитным в части его возможной блокировки в точке подключения к провайдеру. Как и в случае с proxy, у провайдера остается возможность отслеживать IP адреса таких VPN – серверов (особенно при их публичном распространении) и соответственно устанавливать фильтры.
Однако, если Вам удалось договориться о VPN – канале с некоторым частным узлом (лучше с узлом в зарубежной бизнес – сети), Вы получаете предельно надежный доступ равноценный доступу вашего партнера.

3.3) Tor

(The Onion Router http://ru.wikipedia.org/wiki/Tor) — свободное программное обеспечение для реализации второго поколения так называемой «луковой маршрутизации».
Tor – это система прокси-серверов (по некоторым данным и VPN – каналов), позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. Анонимность в сети Tor достигается благодаря тому, что подключение к тому или иному ресурсу идет через цепочку промежуточных серверов. Таким образом, определить IP-адрес и местоположение использующего Tor человека становится довольно сложно. Благодаря своей анонимности Tor пользуется популярностью у интернет - активистов, хакеров, а также пользователей, живущих в странах, контролирующих и фильтрующих интернет - трафик. Как и рассмотренные ранее, Tor остается беззащитным в части его возможной блокировки в точке подключения к провайдеру. Клиентскую часть Tor можно скачать с сайта: https://www.torproject.org/download/download-easy.html.en
Подробнее о Tor смотрите в приложениях 5.3, 5.4. Для рядового пользователя рекомендуется использование Tor Browser Bundle (приложение 5.4).

4) РЕЗЮМЕ.

Все что человек построил, человек может и сломать. Только не следует забывать, что в нашем случае это справедливо для всех сторон. Таким образом, если Вам приходится отстаивать свои права на свободу слова в интернет, Вы должны осознавать, что отстаивание своих прав это процесс, требующий заметных усилий.

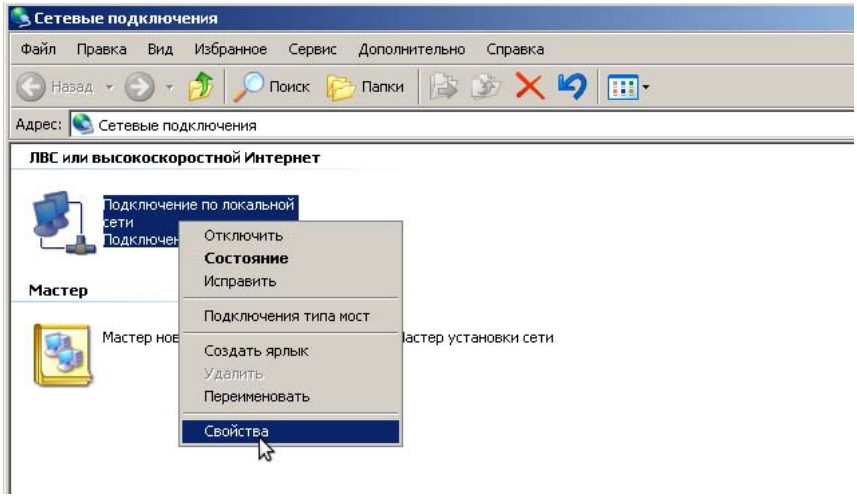
5) ПРИЛОЖЕНИЯ.

5.1) ПУБЛИЧНЫЕ DNS. (Статья 1. Для рядовых пользователей)

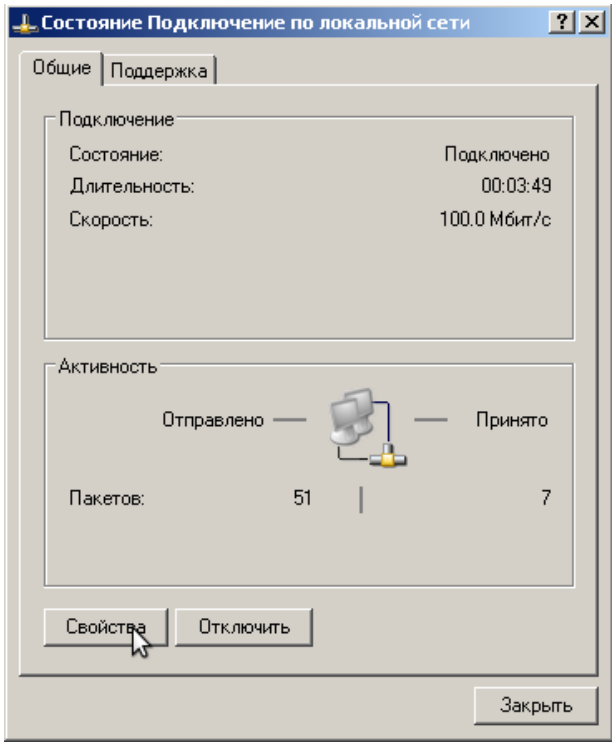
Источник : http://beget.ru/art_public_dns

Случаются ситуации, когда у Вашего интернет - провайдера очень долго обновляется кеш DNS-серверов, и недавно купленный домен не работает. Такое также может произойти, если Вы изменяли настройки DNS для уже существующего домена.
В этом случае совсем не обязательно ждать несколько суток. Можно начать использовать альтернативный публичный DNS-сервер взамен того, который предоставляет интернет - провайдер. Сейчас мы расскажем, как это можно сделать.

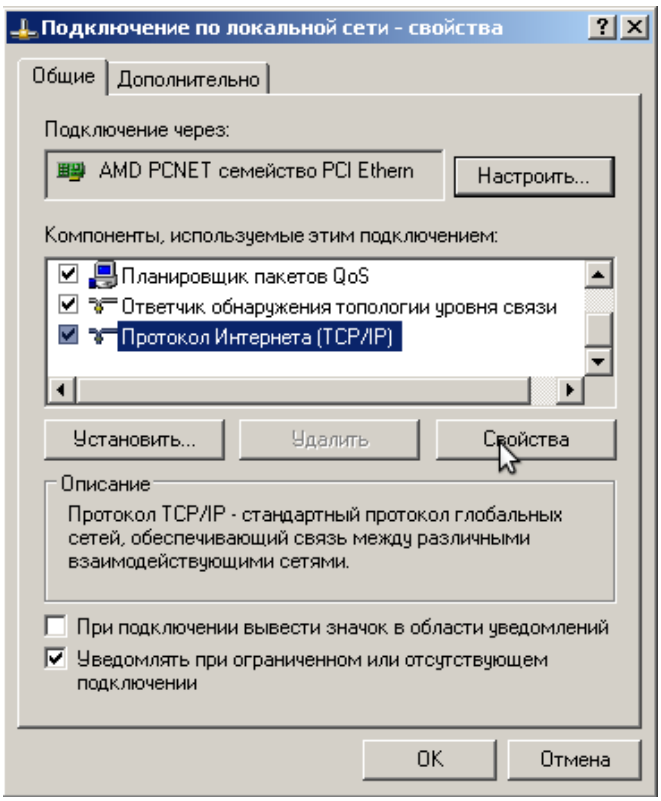
Для того, чтобы указать вашей ОС использовать альтернативный DNS-сервер в ОС Windows, необходимо открыть *Панель управления -> Сетевые подключения*, где щелкнуть правой кнопкой мыши на вашем сетевом подключении и в контекстном меню выбрать пункт *Свойств*:



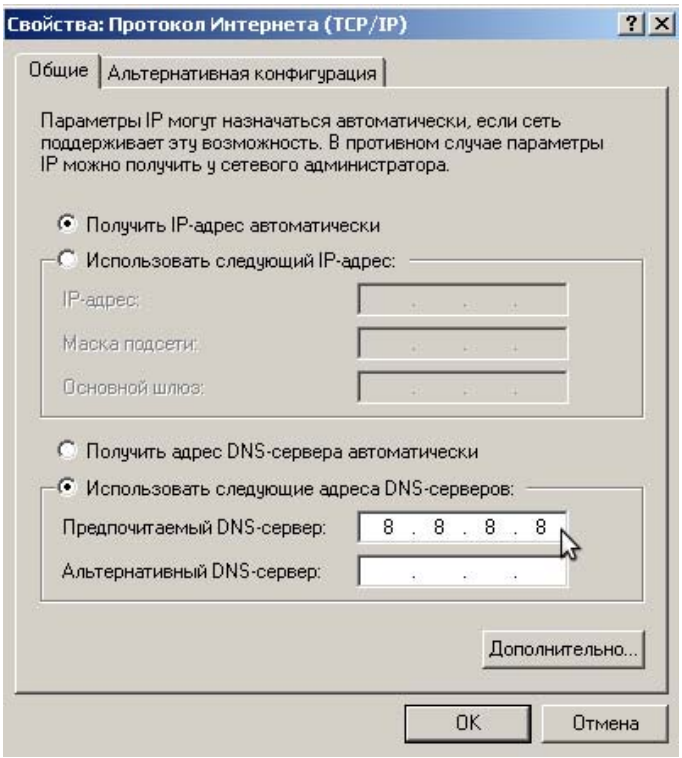
Откроется окно свойств сетевого подключения. Далее Вам необходимо нажать на кнопку *Свойства*:



В появившемся диалоге Вам нужно найти и выделить в списке протоколов *Протокол Интернета (TCP/IP)*, и нажать на кнопку *Дополнительно*:



Наконец откроется нужный нам диалог. Поставьте в нижней части радиокнопку в положение *Использовать следующие адреса DNS серверов*. После чего впишите нужные Вам адреса DNS. В нашем примере мы используем публичные DNS сервера Google. Они предоставляют два сервера, их IP: 8.8.8.8 и 8.8.4.4. Поэтому в этом случае необходимо ввести только один адрес. После ввода сохраните все изменения. С этого момента ваша ОС будет использовать другой DNS сервер.



Вы можете использовать любой другой публичный DNS сервер, который Вам известен. Например, это могут быть сервера OpenDNS. Их IP адреса:
208.67.222.222
208.67.220.220
После сохранения Вам надо перезапустить браузер и проверить работу Вашего сайта.

5.2) ПУБЛИЧНЫЕ DNS (Статья 2. Для IT-специалистов).

Для IT-специалистов будет может оказаться полезной следующая информация:
Источник: http://compnetworking.about.com/od/dns_domainnamesystem/tp/top-free-internet-dns-servers.htm

Google Public DNS
Google operates the world's largest public DNS service. Launched in December 2009, it supports many billions of DNS queries per day, much of the volume generated from clients outside the U.S. Google Public DNS utilizes servers at IP addresses 8.8.8.8 and 8.8.4.4. The company developed this service as one of its corporate initiatives to make the Internet more accessible and easier for everyone to use, making it a logical choice for users worldwide.
OpenDNS
The oldest of all services on this list, OpenDNS also supports billions of DNS queries per day via its servers operating on 208.67.222.222 and 208.67.220.220. In addition to its basic name resolution service, OpenDNS Home Solutions provides free Web site filtering of adult content (called FamilyShield) and URL spell correction with accompanying installed software. The company also sells various security products to businesses. Those looking for an alternative to Google products and a service that works well outside the U.S. also tend to like OpenDNS.
Norton DNS for Home
Security software company Symantec began offering its free Norton DNS in 2010. The package works similarly to OpenDNS FamilyShield. Utility programs that automatically configure the DNS server addresses 198.153.192.50 and 198.153.194.50 and set up basic content filtering exist for Windows, Mac OS X and Android. Those already using OpenDNS or Google Public DNS but dissatisfied with those service can try Norton DNS to see how it compares.
Comodo Secure DNS
In addition to its free DNS service, Comodo is known for the Antivirus package it sells along with other software products. Access the Comodo DNS servers at 8.26.56.26 and 8.20.247.20.
DNS Advantage
A company called Neustar manages both the free DNS Advantage service as well as the commercial (not free) UltraDNS system. Enter the DNS server addresses 156.154.70.1 and 156.154.71.1 to use DNS Advantage.
Verizon / Level 3 Communications
U.S Internet provider Verizon maintains public DNS servers that can be used by both subscribers and non-subscribers. Verizon's servers (sometimes identified as "Level 3 Communications" or as "Genuity" / "gtei.net") appear at 4.2.2.1 through 4.2.2.6.
ScrubIT
Addresses 67.138.54.100 and 207.225.209.66 belong to the ScrubIT free public DNS servers. Designed to automatically block pornographic and other undesirable Web sites, ScrubIT made its debut in 2007 and received mixed reviews for its aggressive filtering policies. The product has since been discontinued.

5.3) Tor: Overview (ОБЗОР)

(Фрагментарный перевод. Источник: https://www.torproject.org/about/overview.html#ru)

Tor был первоначально разработан, реализован и развернут как проект лук - маршрутизации третьего поколения лаборатории военно-морских исследований США (onion routing project of the U.S. Naval Research Laboratory). Изначально он использовался для защиты правительственной связи. Сегодня он используется для удовлетворения самых разнообразных целей нормальных людей, военных, журналистов, сотрудников правоохранительных органов, активистов, и так далее.

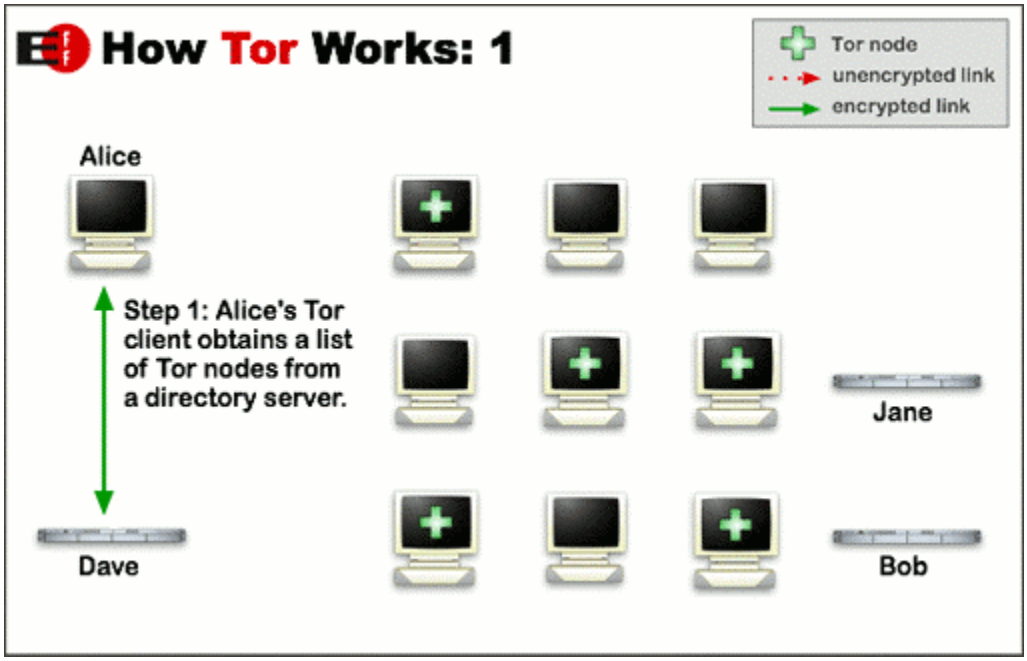
Tor является сетью виртуальных туннелей, которые позволяют отдельным пользователям и группам людей улучшить свою приватность и безопасность в сети. Tor обеспечивает основу для широкого спектра приложений , которые позволяют организациям и частным лицам обмениваться информацией через публичные сети, не раскрывая их личную жизнь.

Обычные пользователи применяют Tor чтобы не дать возможность отслеживания их подключений к сайтам новостей, службам мгновенного обмена сообщениями, и т.п., в условиях когда они блокируются интернет-провайдерами. Скрытые сервисы Tor позволяют пользователям посещать WEB-сайты и другие ресурсы не раскрывая свое местоположение. Отдельные лица также используют Tor для социально-проблемных связей: WEB - форумы для жертв насилия и оскорблений или людей с болезнями. Корпорации используют Tor как безопасный способ проведения конкурентного анализа и для защиты важных путей поставок от наблюдателей. Они также используют его для замены традиционных VPN, которые не скрывает от злоумышленника точное количество и временные промежутки сеанса связи.

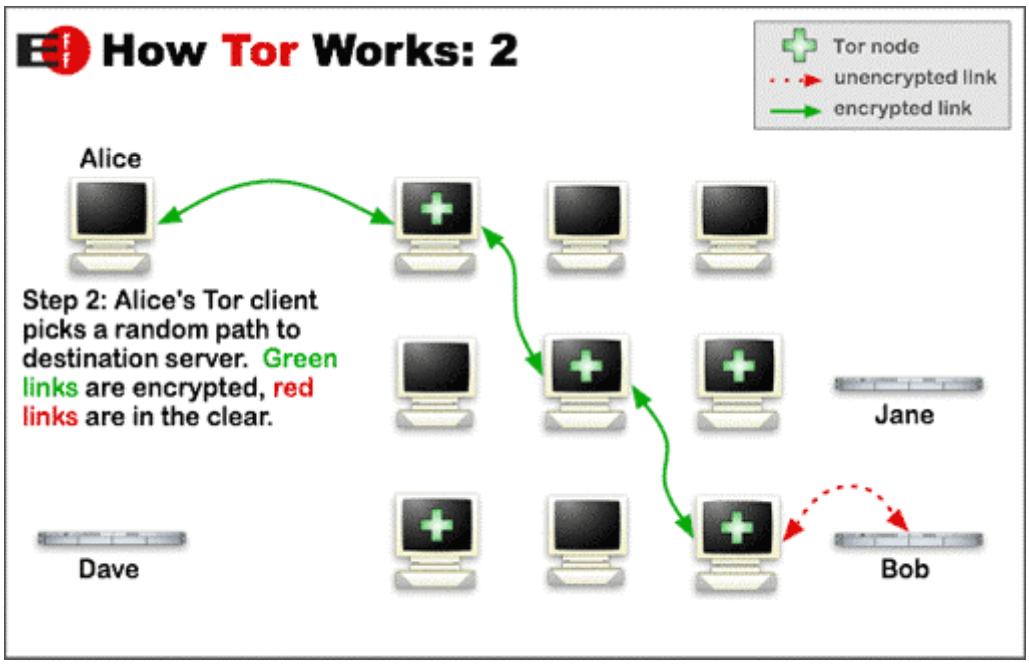
Филиал ВМС США использует Tor для сбора разведывательных данных, а одно подразделение использовало Tor во время своего развертывания на Ближнем Востоке. Правоохранительные органы используют Tor для посещения WEB - сайтов, не оставляя IP адреса.

Для понимания работы Tor следует ответить на вопрос - как работает анализ потока данных в интернет? Пакеты данных в интернете состоят из двух частей: полезная нагрузка данных и заголовок, используемый для маршрутизации. Полезная нагрузка данные все время отправки, что является ли сообщение электронной почты , WEB - страница, аудио-файл. Даже если вы шифруете пересылаемые Вами данные, анализ трафика позволит узнать очень много о том, что Вы делаете, и, вероятно, что вы говорите. Это потому, что анализ нацелен на заголовок и позволяет узнать источник, приемник , размер, и так далее. Очень простую форму анализа потока данных можно реализовать где-то между отправителем и получателем в сети, просматривая заголовки. Однако есть и более мощные техники такого надзора. Многие заинтересованные стороны наблюдают за несколькими сегментами интернета и используют продвинутые статистические методы, чтобы проследить характерные сеансы связи разных организаций и частных лиц. Шифрование в таких случаях бессмысленно, так как оно лишь скрывает содержание интернет - трафика, а не заголовки.
Tor помогает уменьшить риск и простого и продвинутого анализа трафика, раскидывая ваши сеансы связи через несколько узлов в интернете, так что ни один из промежуточных узелов не может привязать вас к месту положения и назначения. Идея состоит в том, чтобы построить временный извилистый маршрут для обмена информацией, а затем периодически выполнять уничтожение следов этого маршрута. Вместо того, чтобы идти по прямому пути от отправителя к получателю, пакеты данных в сети Tor выбирают случайные маршруты через несколько серверов, которые скрывают ваши следы так, ни один наблюдатель в любой точке не может сказать, откуда данные пришли и куда они собираются.

Первым шагом (наиболее уязвимым) при подключении Tor к сети является обращение к Tor – серверу для получения списка промежуточных серверов через которые он может начать построение маршрута (см. рис. Works: 1).

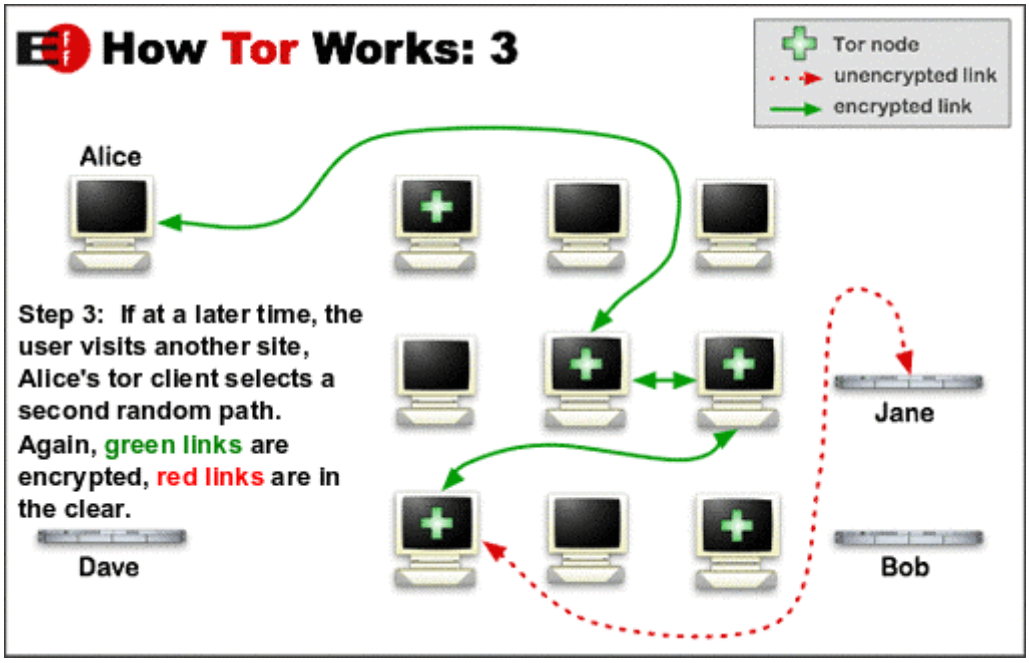


Далее, чтобы создать приватный путь с помощью Tor, программа пользователя (или клиент) последовательно строит цепочки зашифрованных соединений с серверами сети. Цепочка вырастает по одному прыжку за раз, и каждый участвующий сервер знает только то, от какого сервера он получил данные и какому серверу эти данные он передает. Ни один из серверов не знает полный путь, по которому будут идти пакеты данных. Клиент определяет отдельный набор ключей шифрования для каждого прыжка вдоль цепи, чтобы каждый прыжок невозможно было проследить (см. рис. Works: 2).



Как только цепочка была создана, становится возможным обмен могими видами данных. Так как каждый сервер видит не больше одного шага в цепи, ни сторонний наблюдатель,

ни анализ трафика не могут четко связать получателя и отправителя. Tor работает только для потоков TCP, а также может использоваться любым приложением с помощью SOCKS. Для большей эффективности, программное обеспечение Tor использует конкретную цепочку маршрута не более десяти минут (или около того). После этого новым запросам предоставляется новая цепочка, чтобы не связывать ваши предыдущие действия с новыми действиями (см. рис. Works: 3).



Однако Tor не может самостоятельно решить все проблемы анонимности. Он нацелен только на защиту процесса передачи данных. Для повышения эффективности Вы должны использовать специфичные программные продукты (и специфичные протоколы например https). Для рядового пользователя наиболее удобно использовать Tor Browser Bundle, который удобно обеспечивает работу с WEB – ресурсами в интернете .

5.4)Tor Browser Bundle

Загрузить Tor Browser Bundle: http://www.comss.ru/page.php?id=760

Tor Browser Bundle позволяет использовать Tor на операционной системе Windows без инсталляции какого-либо дополнительного программного обеспечения. Оно может быть использовано с флеш-носителя USB, поставляется с преднастроенным веб-браузером Firefox и является независимым.
Если у вас проблемы из-за вашего IP адреса, такие как: нет возможности скачать что-то с файлообменника, или просто нельзя где-то зарегистрироваться с местным IP. Tor Browser Bundle вам в помощь.

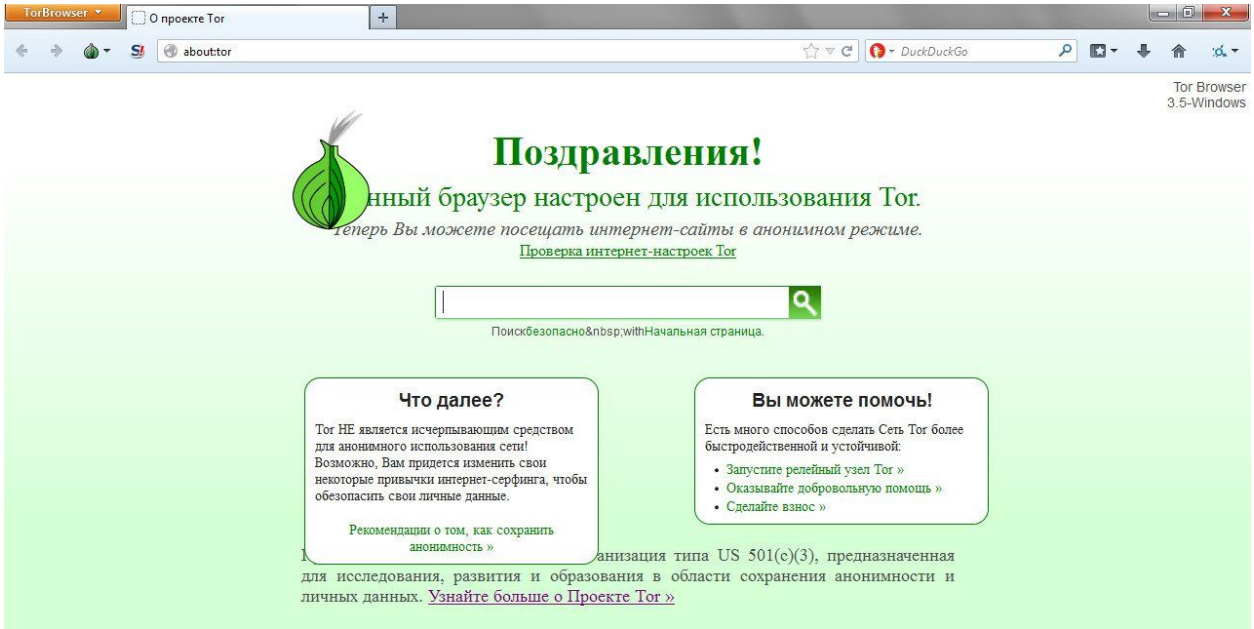
Программное обеспечение Tor обеспечивает защиту за счет маршрутизации вашего трафика по распределенной сети серверов, запущенных добровольцами со всего мира: оно не допускает наблюдения за вашим Интернет соединением и получения информации о том, какие сайты вы посещаете, оно не открывает посещаемым вами сайтам информацию о вашем физическом расположении, и позволяет посещать заблокированные сайты.

Содержимое комплекта:
Разработчик: The Tor Project
Лицензия: Freeware (**бесплатно**)

Версия:	3.5.1 [Windows / RU]
Обновлено:	2014-01-25
Система:	8.1 / 8 / 7 / Vista / XP 32|64-bit
Интерфейс:	русский
Категория:	Браузеры и плагины
Размер:	23.3 MB

Использование:

Когда извлечение файлов закончено, откройте папку Tor Browser из директории, в которую вы сохранили файлы. Дважды щелкните по приложению «Start Tor Browser.exe». Вскоре появится окно Vidalia.
Как только Tor запустится, автоматически откроется окно Firefox. Через Tor будут проходить только веб страницы, посещаемые с использованием входящего в установочный пакет браузера Firefox. На другие веб браузеры, например, Internet Explorer, действие Tor не будет распространяться. Прежде, чем посещать какие-либо страницы, убедитесь, что в браузере в правом нижнем углу написано "Tor включен". Чтобы уменьшить риск, не запускайте стандартный Firefox во время использования Browser Bundle, а также перед началом закрывайте все открытые ранее окна стандартного браузера Firefox.
По окончании работы в Интернете, закройте все открытые окна Firefox. Из соображений безопасности список посещенных вами веб страниц и все cookies будут удалены. Вместе с Tor Browser Bundle автоматически будут закрыты Vidalia и Tor.
Помните, что Tor анонимизирует источник вашего трафика и шифрует весь трафик внутри сети Tor, но он не может зашифровать трафик между сетью Tor и адресом назначения. Если вы передаёте ценную информацию, вы должны уделять вопросам безопасности столько же внимания, как и при работе через стандартное Интернет соединение — используйте HTTPS или другой способ конечного шифрования и аутентификации.



На рисунке приведен внешний вид стартовой станицы