Самоучитель

Денис Колисниченко

Анонимность и безопасность в ИНТЕРНЕТЕ

от «чайника» к пользователю

- Скрываем свое местонахождение и IP-адрес
- Посещаем заблокированные администратором сайты
- Шифруем передаваемые данные
- Защищаем почтовый ящик от спама и посторонних глаз
- Защищаем компьютер от вирусов и атак
- Защищаем домашнюю беспроводную сеть
- Шифруем данные на жестком диске
- Удаляем файлы без возможности восстановления
- Используем анонимные сети Tor, I2P, программы Comodo, TrueCrypt и др.

bhv

Денис Николаевич Колисниченко

Анонимность и безопасность в Интернете. От «чайника» к пользователю

Серия «Самоучитель (BHV)»

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=6982331
Анонимность и безопасность в Интернете. От "чайника" к пользователю: БХВ-Петербург; Санкт-Петербург; 2014
ISBN 978-5-9775-0363-1

Аннотация

Простым и понятным языком рассказано, как скрыть свое местонахождение и IP-адрес, используя анонимные сети Tor и I2P, посетить заблокированные администратором сайты, защитить личную переписку от посторонних глаз, избавиться от спама, зашифровать программой TrueCrypt данные, хранящиеся на жестком диске и передающиеся по сети. Отдельное внимание уделено защите домашней сети от нежданных гостей, от соседей, использующих чужую беспроводную сеть, выбору антивируса и брандмауэра (на примере Comodo Internet Security). Показано, как защитить свою страничку в социальной сети, удалить файлы без возможности восстановления и многое другое.

Для широкого круга пользователей

Содержание

Денис Колисниченко Анонимность и безопасность в Интернете. От "чайника" к пользователю

Введение

Стремление государства и некоторых коммерческих структур знать все о каждом человеке в последнее время начинает откровенно раздражать. Как правило, все прикрываются благородными целями: борьбой с мошенничеством, терроризмом и т. п. Известно, однако, что благими намерениями вымощена дорога в ад.

Изначально Интернет был "территорией свободы", единственным, пожалуй, местом с полной свободой слова, где каждый имел право высказать свое мнение. Сейчас же технический прогресс работает против этой самой свободы – опубликовал заметку в своем блоге – и жди звонка в дверь…

Впрочем законопослушным пользователям, может, и нечего бояться. Если забыть о свободе слова, конечно. Броди по Интернету, читай анекдоты, смотри фильмы. Но знай, что за каждым твоим шагом – наблюдают. И осознание этой истины реально бесит. В конце концов, у каждого есть право на тайну переписки и личной жизни. И реализовать его вам поможет эта книга, как раз и посвященная анонимной и безопасной (во всех смыслах этого слова) работе в Интернете.

Из *первой части* книги вы узнаете, как скрыть свой IP-адрес, как посетить сайт, заблокированный администратором сети, как зашифровать передаваемые по Сети данные, познакомитесь с двумя системами анонимизации трафика: Tor и I2P.

Вторая часть книги посвящена защите электронной почты. Сначала мы перекроем потоку спама путь в свой почтовый ящик, а затем разберемся, как защитить переписку. Будут рассмотрены безопасные соединения, передача писем через сеть Tor и, конечно же, криптография с открытым ключом (PGP).

Третья часть книги поможет вам защитить свой домашний компьютер и домашнюю сеть. В ней мы поговорим о выборе хорошего антивируса и брандмауэра (будут рассмотрены программа Comodo Internet Security и стандартный брандмауэр Windows 7), защитим домашнюю беспроводную сеть от вторжений (а любителей Интернета "на шару" оставим без такового), создадим хороший пароль и научимся шифровать данные на жестком диске с помощью утилиты TrueCrypt и стандартных средств Windows 7.

Ну, а *четвертая часть* книги поможет вам не рассекретить самого себя и подскажет, какие программы лучше всего использовать, если вы желаете остаться анонимным.

Не обойдите вниманием и *приложения*! В *первом* вы познакомитесь с программой AVZ и еще несколькими полезными утилитами, а во *втором* будет рассмотрена программа Traffic Inspector, которая весьма пригодится дома, поскольку позволяет блокировать доступ к Интернету по времени суток и по адресу, – ваши дети не смогут посетить заблокированные адреса или использовать Интернет ночью. К слову, возможности, предоставляемые этой программой (блокировка по адресу и времени), имеются во многих беспроводных маршрутизаторах, и если вы счастливый обладатель такового, можно обойтись и без этой программы. Однако в большинстве случаев дома всего лишь один компьютер и нет никакого маршрутизатора.

Читатели не любят длинных введений и часто таковые игнорируют. Поэтому считаю, что сейчас самое время перейти к чтению книги.

Часть I
Скрываем свое местонахождение и посещаем заблокированные сайты

Вся *первая часть* книги посвящена обеспечению вашей анонимности в Интернете. Вы узнаете, как скрыть свой IP-адрес и свое местонахождение, как скрыть от глаз администратора сети посещаемые вами сайты, как обойти черный список брандмауэра и посетить заблокированный сайт, как правильно удалить служебную информацию браузера и многое другое.

Глава 1. Как стать анонимным в Интернете?

1.1. Анонимность и вы

В последнее время Интернет становится все менее анонимным. С одной стороны – всевозможные ресурсы и вредоносные программы, собирающие различную информацию о пользователе: IP-адрес, имя, пол, возраст, место жительства, номер телефона. Такая информация может собираться как явно (вы ее сами указываете, заполняя на посещаемых сайтах различные формы-вопросники), так и неявно, когда она определяется на основании косвенных данных (например, ваше местонахождение при посещении того или иного сайта легко вычисляется по IP-адресу компьютера, с которого вы зашли в Интернет). Вся эта информация может собираться различными сайтами, например для показа вам рекламных объявлений, привязанных к вашему месту жительства, или в любых других целях. С другой стороны – силовые органы с оборудованием СОРМ (система оперативно-розыскных мероприятий), которое внедряется уже много лет.

Зачем нужна анонимность в Интернете обычному законопослушному пользователю?

> **Примечание**
> В побуждения незаконопослушных мы здесь углубляться не станем…

Причины у всех свои, но от них зависят способы достижения цели. В табл. 1.1 приводятся несколько типичных задач, которые рано или поздно приходится решать каждому интернет-пользователю.

Понимаю, что приведенные здесь способы решения поставленной задачи вам пока не ясны. Что ж, самое время разобраться со всеми этими заумными названиями: анонимайзеры, анонимные прокси-серверы и т. п.

Таблица 1.1. Причины сохранения анонимности в Интернете

Задача	Зачем?	Способы решения
Нужно разово скрыть свой IP-адрес	Вы просто не хотите, чтобы ваш IP-адрес "записал" сайт, который вы собираетесь посетить. Вторая причина — ради эксперимента. Например, вы создали свой сайт, скажем, на **http://narod.yandex.ru/**, установили на нем счетчик и теперь хотите проверить, работает он или нет. Если на сайт вы заходите со скрытого IP-адреса, значение счетчика останется неизменным. Когда же вы зайдете с использованием IP-адреса открытого, значение счетчика будет увеличено	Анонимные прокси-серверы Анонимайзеры
"Смена жительства"	Некоторые сайты разрешают доступ, если ваш IP-адрес относится к определенной стране. Пользователям других стран доступ на сайт запрещен	Анонимные прокси-серверы Распределенная сеть Tor
Постоянное анонимное посещение сайтов	Вероятно, вы или скрывающийся блоггер (в последнее время — это популярный род деятельности), или же просто не хотите, чтобы администратор (вашей офисной сети или сети провайдера) узнал, какие сайты вы посещаете	Распределенная сеть Tor Проект I2P
Нужно скрыть посещенные сайты от глаз коллег и родственников	У вас нет паранойи и вам все равно, следит ли за вами администратор, но вы просто не хотите, чтобы ваши родственники или коллеги узнали, на каких сайтах вы бываете	Не нужно никаких специальных средств, достаточно правильно очистить историю браузера или использовать режим приватного просмотра браузера Firefox. Об этом мы поговорим далее в этой главе
Нужно посетить заблокированный администратором сайт	"Злой" администратор закрыл доступ к Одноклассникам или ВКонтакте? Решение, как всегда, есть!	Распределенная сеть Tor
Зашифровать всю передаваемую вами информацию	Иногда анонимного посещения сайтов мало, важно, чтобы никто не узнал, какую информацию вы передавали этим сайтам (например, какие анкетные данные указывали)	Распределенная сеть Tor

1.2. Анонимайзеры: сокрытие IP-адреса

Представим, что вы собрались разово скрыть свой IP-адрес. Зачем это вам, мне дела нет. Снимаю с себя всякую ответственность, если ваши цели идут вразрез с существующим законодательством. Все мы помним, что Раскольников сделал с помощью топора, однако холодным оружием топор не считается…

Из личного опыта…

> В свое время анонимайзер помог мне в весьма неординарной ситуации. Все мы знаем, что пакеты, исходящие от нашего компьютера к компьютеру назначения (веб-серверу сайта, который мы хотим посетить), отправляются не напрямую, а проходят по определенному маршруту через некоторое количество маршрутизаторов. Так вот, один маршрутизатор на пути от моего компьютера к моему же сайту вышел из строя. В результате я не мог зайти на свой сайт, хотя он был вполне доступен, и на него могли зайти пользователи других провайдеров, пакеты которых проходили по иным маршрутам. Ждать пока маршрутизатор восстановят мне, разумеется, не хотелось, поэтому я и воспользовался анонимайзером, чтобы, во-первых, убедиться в доступности сайта, а, во-вторых, посмотреть, что же на нем творится.

Итак, что же представляет собой *анонимайзер* (anonymizer)? Это такой сайт в Интернете. Вы на него заходите, вводите в специальное поле адрес сайта, который хотите посетить анонимно, и вуаля – вы на сайте, но сайт записал в свои протоколы не ваш IP-адрес, а адрес анонимайзера. При переходе по ссылке также фиксируется IP-адрес анонимайзера – до тех пор, пока вы не закрыли окно (или вкладку) браузера, в котором изначально был открыт анонимайзер. Весьма удобно, а главное – просто.

Найти подходящий анонимайзер несложно – введите в Google запрос *анонимайзер* (или *anonymizer*), и будет найдено множество сайтов, предоставляющих такие услуги. Некоторые из них – бесплатные (они содержатся за счет размещаемой рекламы, которую вы вынуждены просматривать, пользуясь анонимайзером), за использование других придется заплатить.

Платный или бесплатный? Если вам просто надо анонимно посетить пару страничек, выбирайте бесплатный анонимайзер. А вот если вы хотите не просто посетить некий сайт, а еще и скачать оттуда какую-либо информацию, лучше выбрать платный. Дело в том, что бесплатные анонимайзеры часто ограничивают максимальный размер загружаемого объекта, – порой вам дадут скачать лишь 1–2 Мбайт, что по современным меркам откровенно мало. А вот платные разрешают скачивать файлы в несколько десятков и сотен мегабайт. Кроме того, некоторые платные анонимайзеры разрешают выбрать IP-адрес из диапазона адресов определенной страны (по выбору), что иногда полезно (см. табл. 1.1).

К достоинствам анонимайзеров можно отнести:

удобство и простоту использования – вам не понадобится устанавливать дополнительное программное обеспечение, не придется вносить изменения в параметры браузера или системы. Просто открыли сайт анонимайзера, ввели нужный URL, и ваш IP-адрес скрыт;

возможность блокировки баннеров – некоторые анонимайзеры для уменьшения количества ненужной информации, пропускаемой через их сервер, блокируют рекламные баннеры. Иногда эта функция становится доступной только после оплаты. К сожалению, большинство бесплатных анонимайзеров только добавляют свою дополнительную рекламу…

А вот недостатков у анонимайзеров очень много:

не выполняется шифрование передаваемых данных – да, с помощью анонимайзера вы можете скрыть свой IP-адрес – посещаемый вами сайт "запомнит" IP-адрес анонимайзера, но не ваш. Но от всевидящего ока администратора вам не скрыться. Он не только сможет легко вычислить, какие сайты вы посещали, но и при желании перехватит передаваемую информацию (например, анкетные данные, которые вы оставляли на сайте). Так что анонимайзеры не обеспечивают полной анонимности;

не всегда можно выбрать IP-адрес нужной страны – предположим, что анонимайзер находится в США. И если вы попытаетесь с его помощью зайти на сайт, который разрешает доступ пользователям только, скажем, из Германии, то у вас ничего не получится – ведь IP-

адрес будет американский. Ради справедливости нужно отметить, что некоторые анонимайзеры предлагают выбрать IP-адрес нужной страны, но это больше исключение, чем правило, да и не факт, что нужная вам страна окажется в списке;

не всегда скорость анонимного доступа будет высокой – тут все зависит от загрузки сервера анонимайзера и от того, как быстро пакеты от вашего компьютера передаются на сервер анонимайзера (то есть важна скорость передачи данных между вашим компьютером и сервером анонимайзера). Впрочем, все средства обеспечения анонимности снижают скорость соединения, и вы должны быть к этому готовы;

ограничение размера перекачиваемых файлов – об этом мы уже говорили, поэтому не вижу смысла повторяться, – не следует надеяться, что вы скачаете через анонимайзер пиратский фильм объемом в несколько гигабайт;

нет гарантий – никто не гарантирует, что анонимайзеры (а их огромное количество) не записывают адреса сайтов, которые вы посещаете, и не передают потом заинтересованным лицам…

Подытоживая отметим: анонимайзеры подойдут для сокрытия вашего IP-адреса – удаленный сайт не сможет его определить. Но для обеспечения полной анонимности они не подходят – администраторы смогут вычислить, какие сайты вы посещали, и даже посмотреть, какие данные вы передавали этим сайтам (поскольку анонимайзеры не производят шифрование данных).

Как администратор вычислит сайты, которые вы посещали? Очень просто. Анонимайзер перезаписывает все ссылки сайта, которые вы хотите посетить, добавляя в их начало свой адрес (чтобы ссылка была открыта не напрямую, а через анонимайзер). Я зашел на популярный анонимайзер **anonymouse.org** и через него – на свой сайт **www.dkws.org.ua**. В строке адреса браузера я увидел следующий URL (рис. 1.1):

http://anonymouse.org/cgi-bin/anon-www.cgi/http://www.dkws.org.ua/

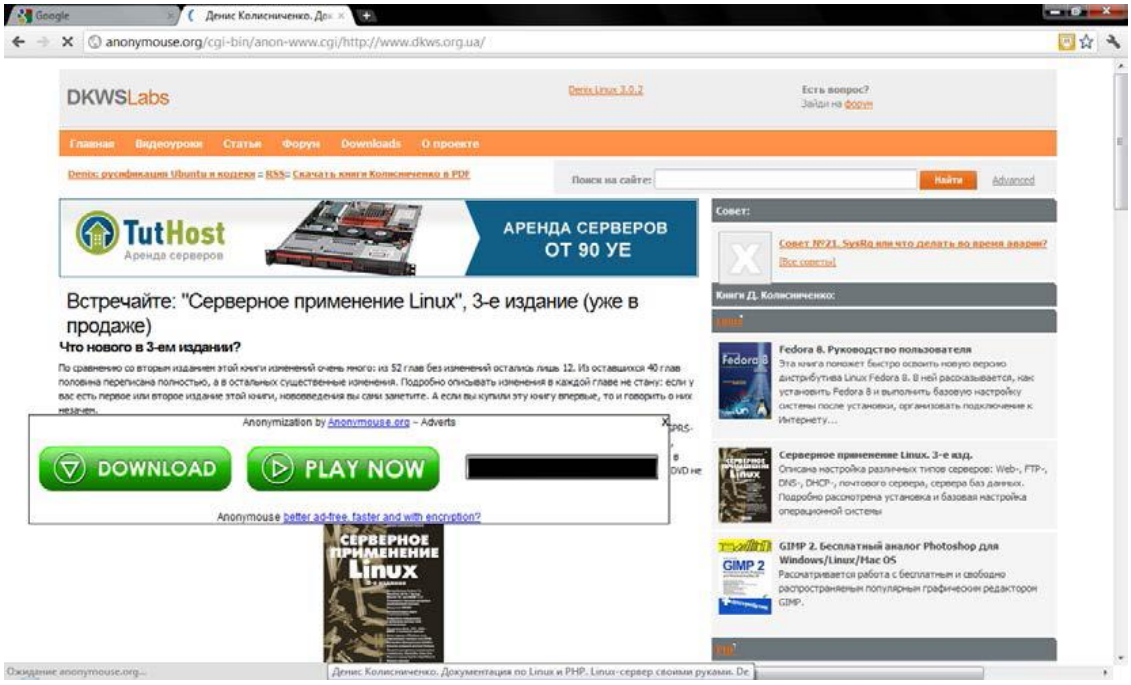

Рис. 1.1. *Просмотр сайта через* ***anonymouse.org****: анонимайзер добавил большой рекламный баннер*

Эта же строка попадет в журналы администратора вашей сети. Как видите, вычислить, какие сайты вы посещали, не составляет никакого труда. Более того, по таким ссылкам адми-

нистратор узнает, какие сайты вы посещали анонимно, и поймет, что к этим сайтам у вас есть повышенный интерес. Поверьте, ему будет о чем рассказать вашему начальству…

1.3. Анонимные прокси-серверы: сокрытие IP-адреса и местонахождения

С помощью анонимайзера скрывается не только ваш IP-адрес, но и ваше местонахождение, определяемое по IP-адресу. Но иногда нужно скрыть местонахождение более гибко, а именно – получить IP-адрес определенной страны. Как правило, к таким мерам прибегают пользователи, которым нужно посетить ограничиваемые сайты.

Из личного опыта…

Нет, никаких мыслей о взломе! Такая операция иногда бывает необходимой самым законопослушным пользователям. В 2009-ом году я столкнулся с анекдотической ситуацией. Крупнейший украинский провайдер "Укртелеком" использовал IP-адреса из диапазона лондонского провайдера. В результате, когда пользователи "Укртелекома" заходили на украинские сайты, их системы статистики считали, что пользователь пришел из Великобритании. А некоторые наши особо патриотические сайты ограничивают доступ всех зарубежных пользователей. Ну надо же – купил Интернет у крупнейшего национального провайдера, а вся страна считает тебя чужаком. Как сейчас обстоят дела у "Укртелекома" не интересовался, но в то время ситуация была вполне реальной.

Выбрать страну проживания можно с помощью анонимных *прокси-серверов*. Однако прежде, чем разбираться с анонимными прокси-серверами, поговорим сначала о прокси-серверах обычных.

1.3.1. Прокси-сервер – что это?

Итак, что такое прокси-сервер? Это узел сети, служащий для кэширования информации и ограничения доступа в сеть. Прокси-серверы устанавливаются как администраторами локальной сети для нужд ее самой, так и провайдерами Интернета для нужд всех их клиентов.

Имя или IP-адрес прокси-сервера можно занести в настройки браузера. В результате браузер будет обращаться к какому-либо узлу сети не напрямую, а через прокси-сервер (то есть запрос будет передаваться сначала на прокси-сервер). А прокси-сервер уже может запросить имя пользователя и пароль (если такое поведение задал администратор прокси) и только потом предоставить пользователю доступ к узлу.

Некоторые ленивые администраторы самодельных локальных сетей применяют прокси для ограничения доступа своих пользователей к Интернету, поскольку более сложные методы им реализовывать неохота (или экономически нецелесообразно).

Однако большинство прокси-серверов используются не для аутентификации, а для кэширования страниц. Браузер обращается к прокси-серверу и передает адрес страницы, которую хочет просмотреть пользователь. Если такая страница имеется в кэше прокси-сервера (а это возможно, если эту страницу недавно кто-то из пользователей сети уже просматривал), то прокси-сервер сразу передает ее пользователю. В результате обращение к удаленному узлу даже не производится, что снижает нагрузку на интернет-канал, экономит деньги, ресурсы удаленного узла и повышает скорость доступа к Интернету. Одно дело передать данные по локальной сети, где скорость соединения доходит до 1000 Мбит/с (в случае с Gigabit Ethernet), другое дело – передать данные по интернет-каналу, где скорость доступа

порой ниже 5 Мбит/с (ну, лично я избалован своим провайдером с его скоростью 50 Мбит/с, а вот сосед неудачно выбрал провайдера и довольствуется скоростью всего 2 Мбит/с).

Дальнейшее развитие прокси-серверов – *прозрачные прокси-серверы*. Суть их заключается в том, что весь веб-трафик с помощью правил брандмауэра сети перенаправляется на прокси-сервер, в результате чего ускоряется доступ к прокэшированным страницам и устраняется необходимость настраивать отдельно каждый клиентский компьютер (точнее, каждый браузер на каждом клиентском компьютере).

1.3.2. Настраиваем анонимный прокси-сервер

Теперь вернемся к рассмотрению *анонимных прокси-серверов*. Как правило, анонимный прокси-сервер – это обычный прокси-сервер, но неправильно настроенный. Администраторы таких серверов забывают запретить доступ к своему серверу чужим узлам. Впрочем, есть и публичные (открытые) прокси, которые намеренно разрешают доступ всем желающим.

Для обеспечения анонимности вам нужно просто указать IP-адрес такого прокси-сервера в настройках браузера.

Где достать адрес анонимного прокси? Списки таких адресов публикуются на различных ресурсах – например, на **http://www.cooleasy.com/**. Там вы найдете IP-адреса прокси-серверов из разных стран (рис. 1.2). Дополнительные IP-адреса можно найти по запросу *Free proxy*. Еще один полезный сайт: **http://spys.ru/aproxy/**.

Рис. 1.2. *Списки анонимных прокси*

Примечание

Кстати, на сайте **www.cooleasy.com** есть и собственный анонимайзер: **http://www.cooleasy.com/webproxy/**.

Найдя заветный IP-адрес, пропишите его в настройках браузера.

В Internet Explorer для этого нужно выполнить следующие действия:

1. Выберите команду меню **Сервис | Свойства обозревателя**.
2. Перейдите на вкладку **Подключения** (рис. 1.3).

3. Нажмите кнопку **Настройка сети**. В открывшемся окне (рис. 1.4) установите флажок **Использовать прокси-сервер для локальных подключений (не применяется для коммутируемых или VPN-подключений)**.

4. Введите IP-адрес прокси-сервера и его порт. Обычно порт указывается в списке прокси в отдельной колонке или через двоеточие – например, 192.168.2.100:3128

(здесь 3128 – номер порта). Стандартные номера портов для прокси: 80, 3128, 8080.

5. Для установки разных прокси для различных сетевых ресурсов (HTTP, FTP и т. д.) нажмите кнопку **Дополнительно** и введите соответствующие адреса (рис. 1.5)

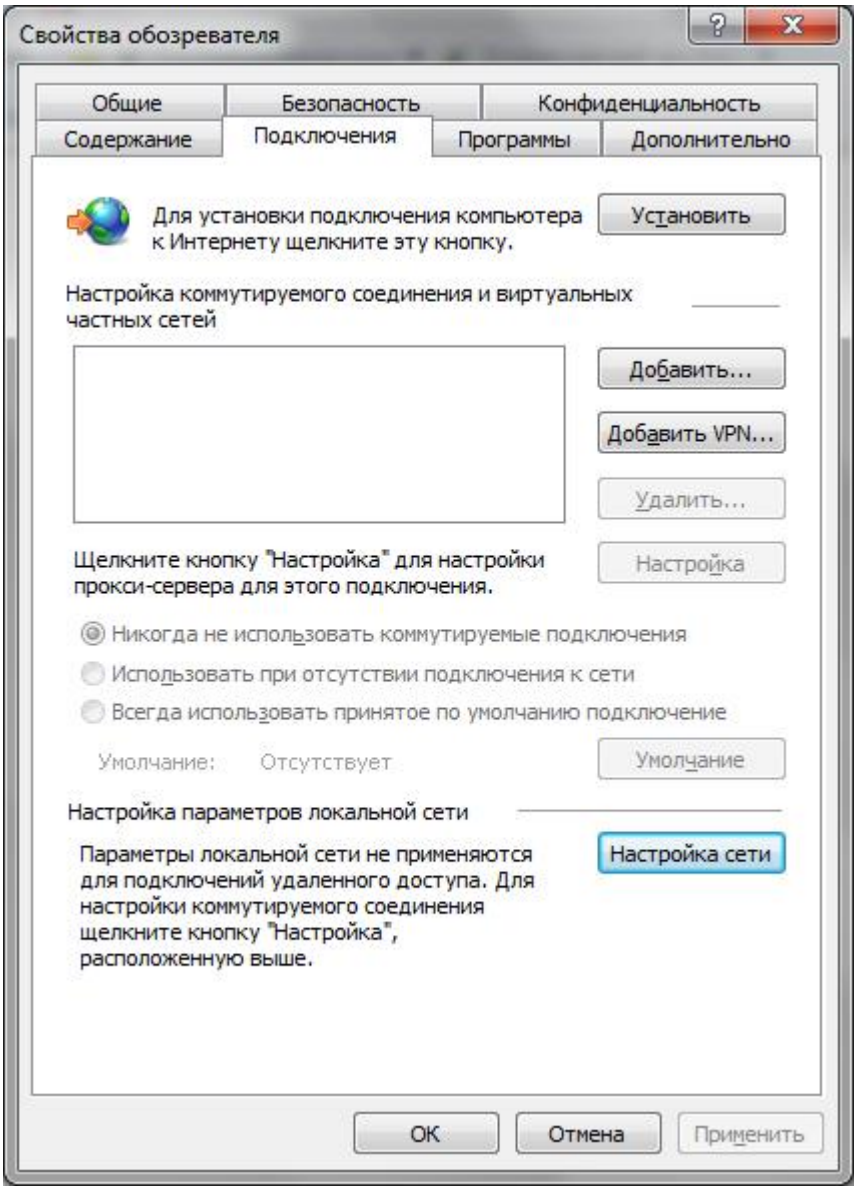

Рис. 1.3. *Свойства обозревателя: вкладка* ***Подключения***

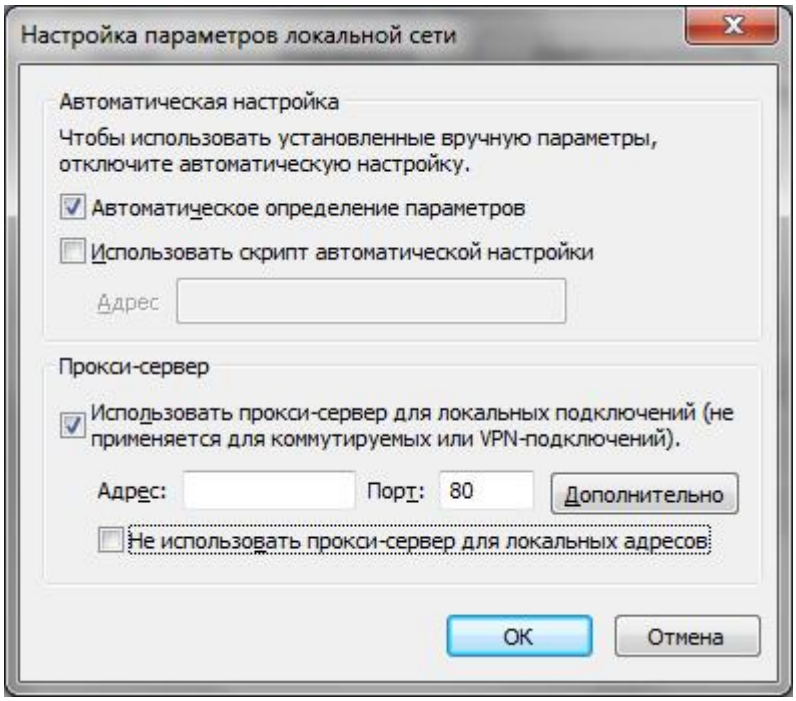

Рис. 1.4. *Окно настройки параметров локальной сети*

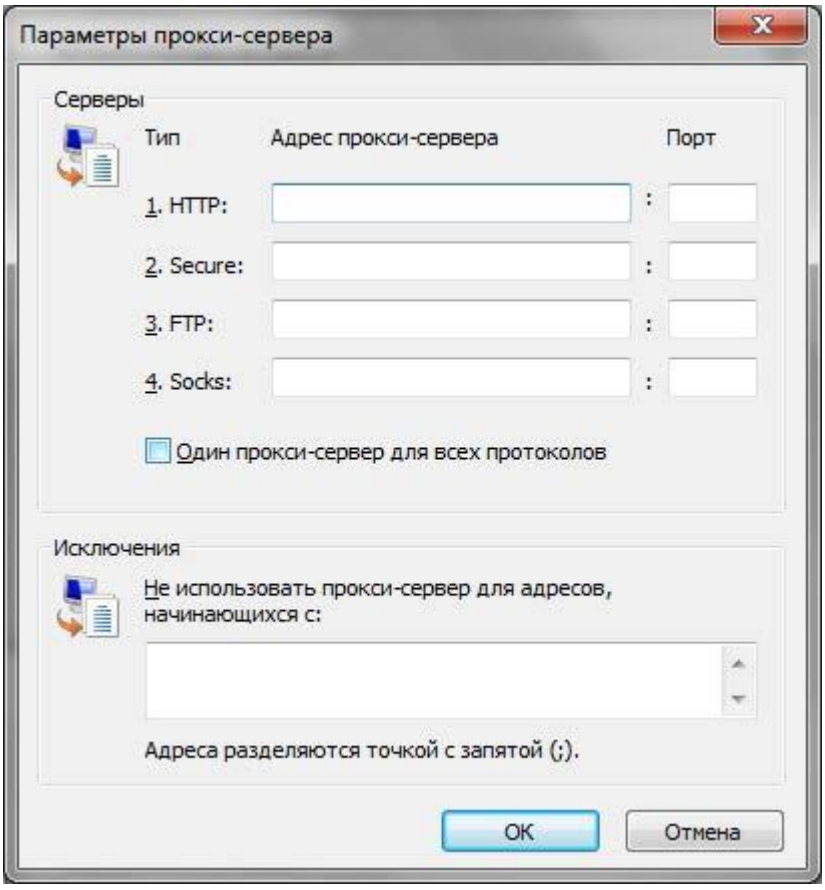

Рис. 1.5. *Окно параметров прокси-сервера*

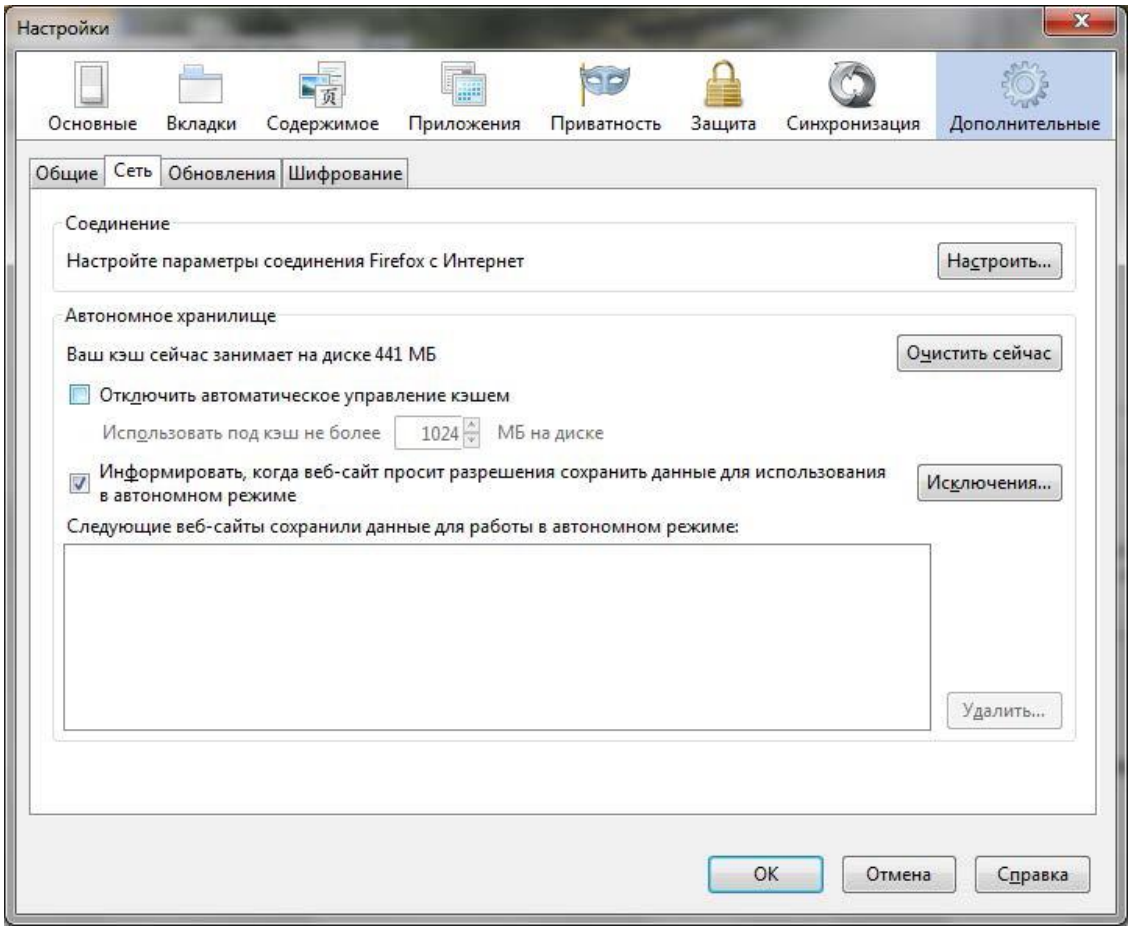

Рис. 1.6. *Окно настроек Firefox*

В Google Chrome последовательность действий будет иной:

1. Нажмите кнопку вызова страницы настроек (с изображением гаечного ключа).
2. Из открывшегося окна выберите команду **Параметры**.
3. Перейдите в раздел **Расширенные**, нажмите кнопку **Изменить настройки прокси-сервера**.
4. Откроется уже знакомое окно (см. рис. 1.5) параметров браузера IE (браузер Google Chrome использует некоторые настройки IE). Далее последовательность действий такая же, как и для IE.

Если у вас Firefox:

1. Выберите команду меню **Firefox | Настройки | Настройки**.
2. Перейдите на вкладку **Сеть** (рис. 1.6).
3. Нажмите кнопку **Настроить**. В открывшемся окне (рис. 1.7) выберите **Ручная настройка сервиса прокси** и введите в поле **HTTP прокси** IP-адрес проксисервера и его порт.

Пользователям браузера Opera нужно выполнить следующие действия:

1. Выбрать команду **Opera | Настройки | Общие настройки**.
2. Перейти на вкладку **Расширенные**, затем – в раздел **Сеть** (рис. 1.8).
3. Нажать кнопку **Прокси-серверы**.
4. В открывшемся окне выбрать **Конфигурировать прокси-сервер вручную** и ввести в поле **HTTP** адрес прокси-сервера, а в поле **Порт** – его порт (рис. 1.9).

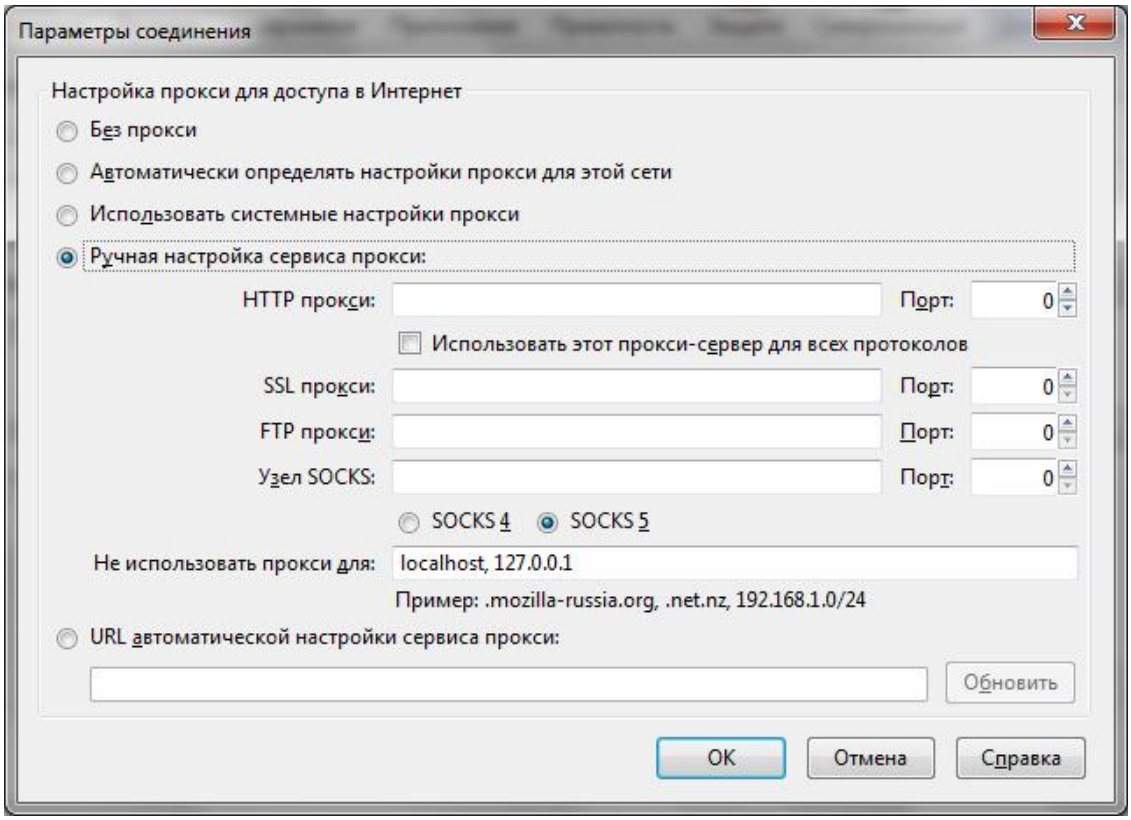

Рис. 1.7. *Параметры соединения*

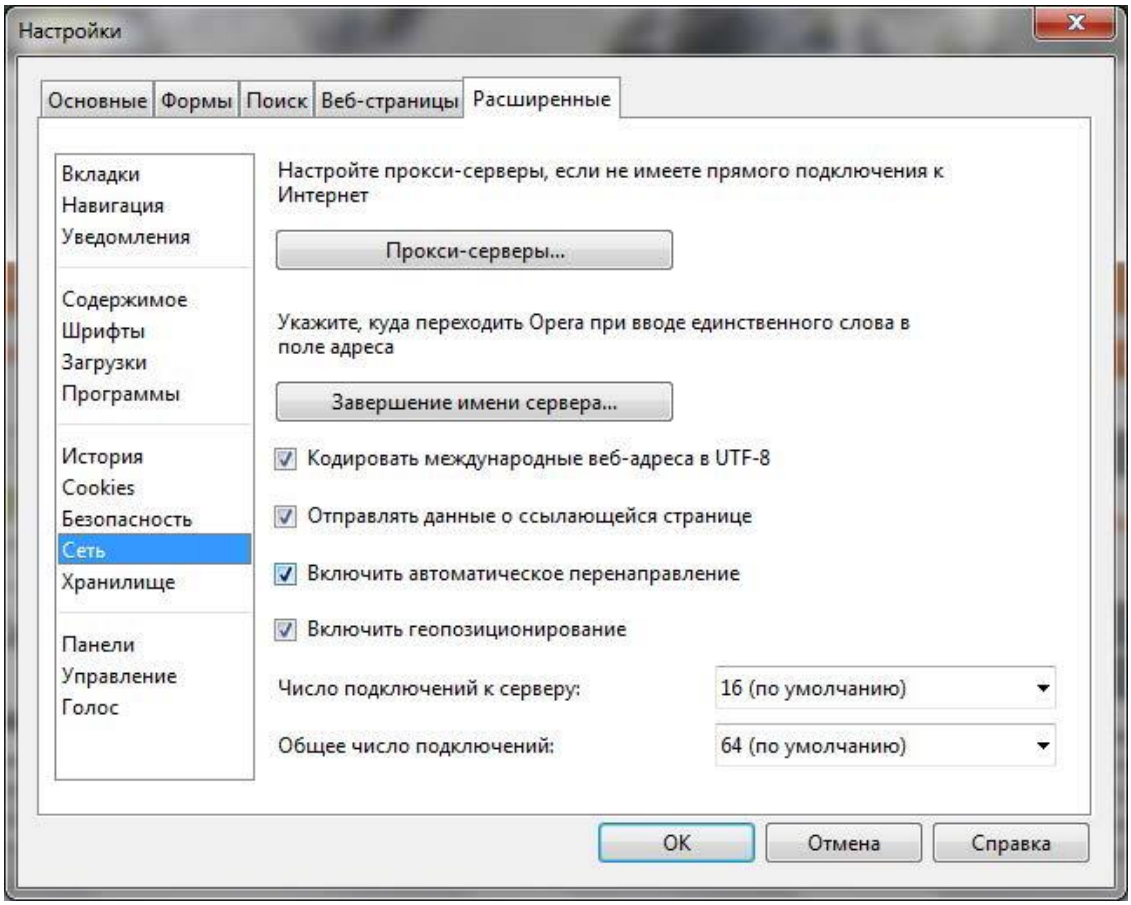

Рис. 1.8. *Настройки браузера Opera*

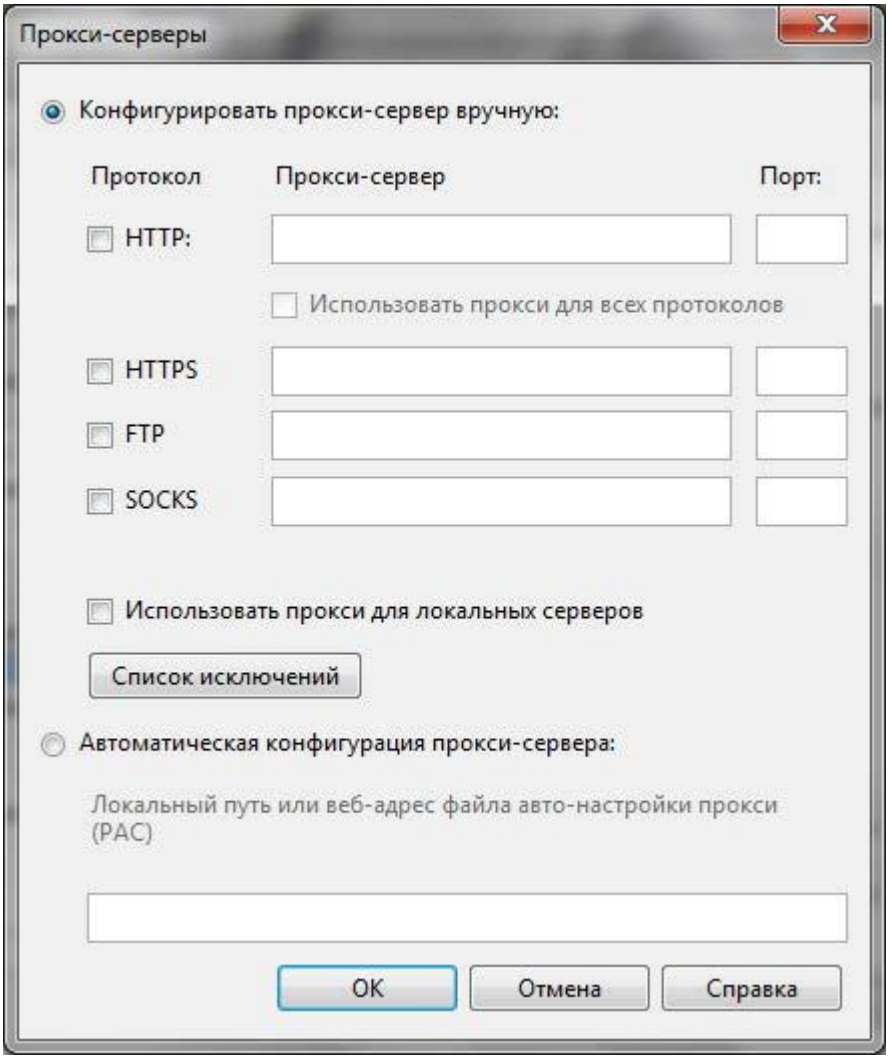

Рис. 1.9. *Параметры прокси-сервера*

1.3.3. Достоинства и недостатки анонимных прокси-серверов

Особых преимуществ перед анонимайзерами у анонимных прокси-серверов нет, если не считать того, что вы можете выбрать анонимный прокси с нужным вам IP-адресом. А вот недостатков достаточно:

непостоянство – как уже отмечалось, некоторые анонимные прокси-серверы это плохо настроенные обычные. Когда администратор поймет, что его прокси используется в качестве публичного (анонимного), он закроет доступ, и вы больше не сможете использовать привычный IP-адрес;

низкая скорость доступа – подобрать анонимный прокси с высокой скоростью доступа не всегда получается;

не все анонимные прокси являются в полном смысле слова анонимными – некоторые из них передают узлу в заголовках запроса ваш IP-адрес. К тому же нет никакой гарантии, что такие прокси не ведут журнал посещений и не пересылают эту информацию третьим лицам;

данные передаются по незашифрованному каналу – стало быть существует возможность перехватить передаваемые вами данные. Некоторые анонимные прокси шифруют соединения, но они, как правило, требуют оплаты.

Неоднозначно и с объемом передаваемых данных – некоторые прокси могут ограничивать его, а некоторые – нет. Если прокси является публичным из-за ошибки администратора, передача больших объемов информации может быть замечена администратором…

1.4. Локальная анонимность

Часто пользователям бывает все равно, следит ли за ними грозный администратор или кто-либо еще. Главное, чтобы коллеги по работе или родственники не видели, какие сайты посещались с их локального компьютера.

Просто очистить историю посещений мало, ведь остаются еще и "косвенные улики" – при загрузке страниц их копии и копии изображений и других объектов, внедренных в страницу, сохраняются в локальном кэше браузера. Проанализировав этот кэш, а также состав Cookies и сохраненные пароли, можно узнать, на каких сайтах вы бывали и какие страницы посещали.

Разберемся, как правильно очистить приватные данные браузера. Начнем с Google Chrome:

1. Нажмите комбинацию клавиш <Ctrl>+<Shift>+<Delete>.

2. В открывшемся окне (рис. 1.10) установите все флажки и нажмите кнопку **Удалить данные о просмотренных страницах**.

В браузере Firefox перед посещением подозрительных сайтов лучше всего выбрать команду **Firefox | Начать приватный просмотр** (рис. 1.11). Это оптимальное решение, поскольку удаление информации о просмотренных страницах может вызвать подозрение и некоторые неудобства – ведь будет удалена вся история, все пароли. А в режиме приватного просмотра история, пароли и другие "улики" не сохраняются. Однако не путайте режим приватного просмотра с анонимностью – просто браузер не будет сохранять историю посещений и другие служебные данные, но удаленный узел сможет получить ваш IP-адрес.

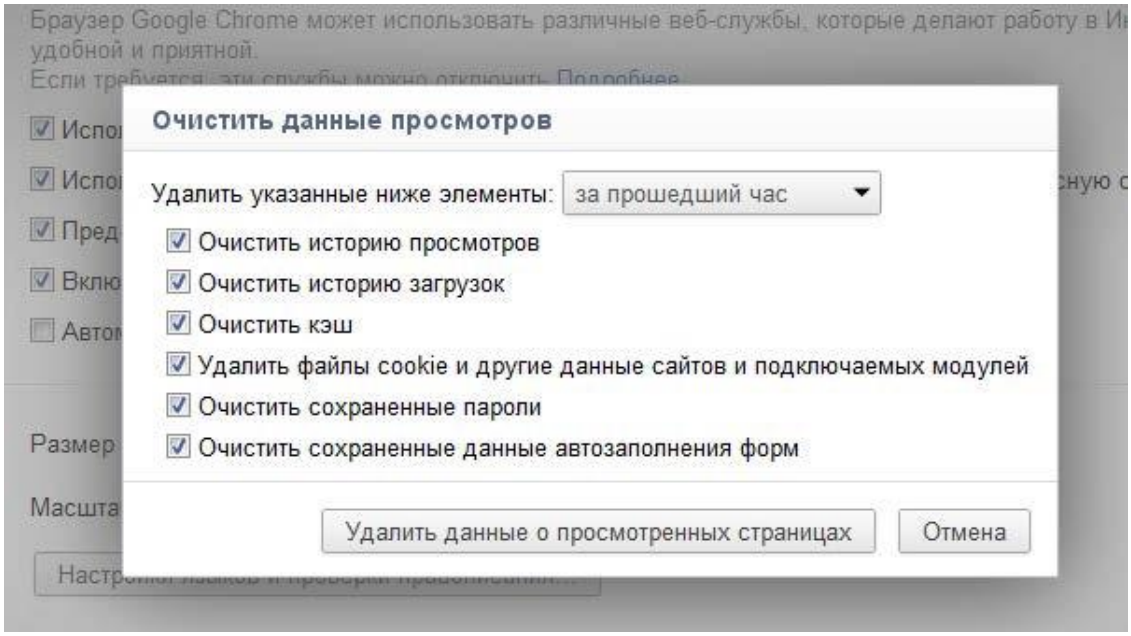

Рис. 1.10. *Заметаем следы в Google Chrome*

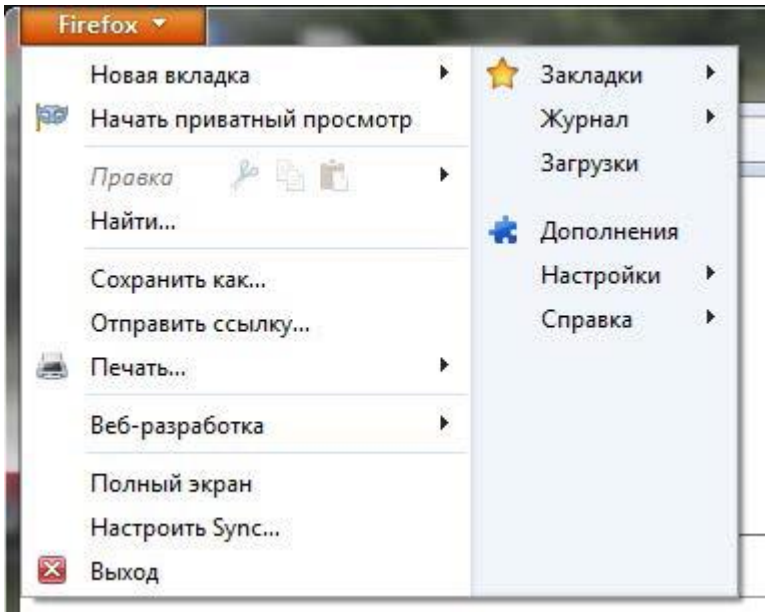

Рис. 1.11. *Режим приватного просмотра в Firefox*

В браузере Opera нужно перейти на вкладку **Расширенные** уже знакомого окна настроек (см. рис. 1.8), затем – в раздел **История**. А там нажать обе кнопки **Очистить** (рис. 1.12).

В Internet Explorer откройте окно **Свойства обозревателя** и на вкладке **Общие** (рис. 1.13) нажмите кнопку **Удалить**. В открывшемся окне (рис. 1.14) установите все флажки и нажмите кнопку **Удалить**.

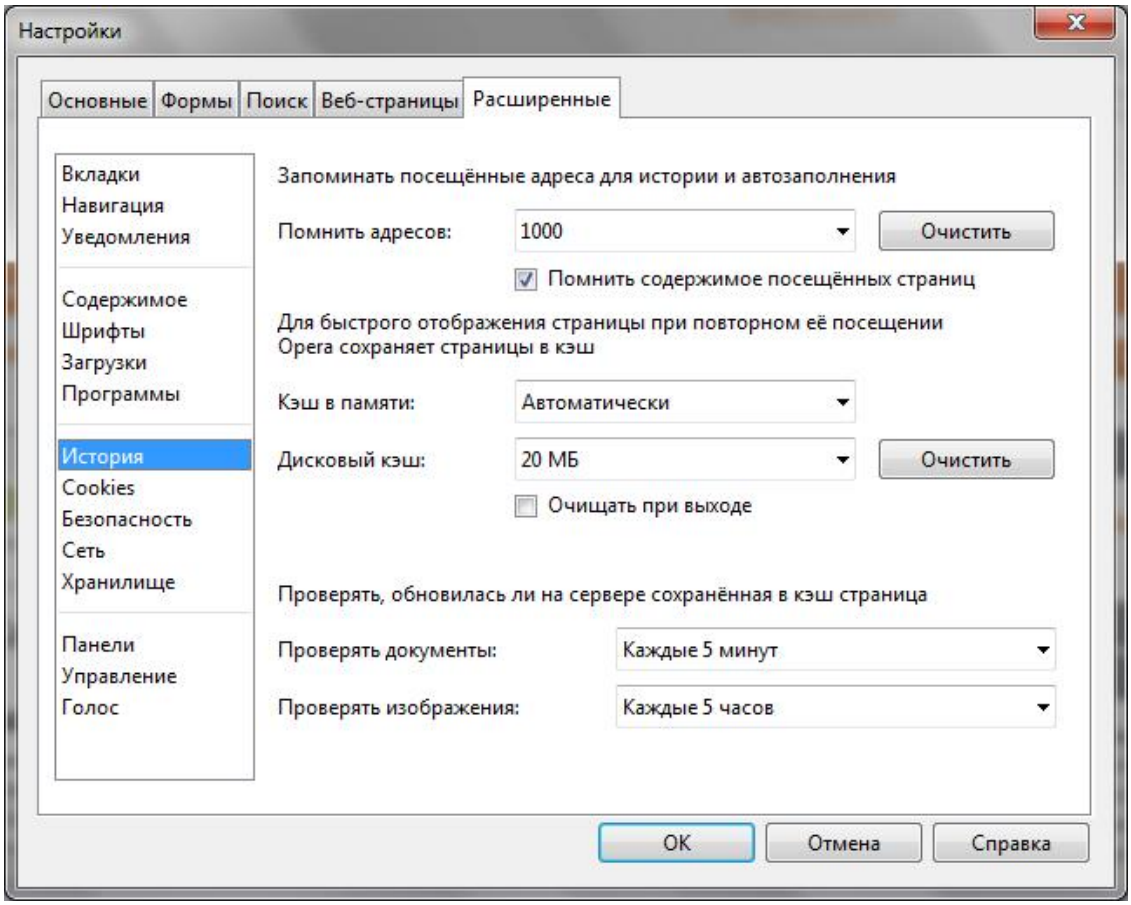

Рис. 1.12. *Заметаем следы в Opera*

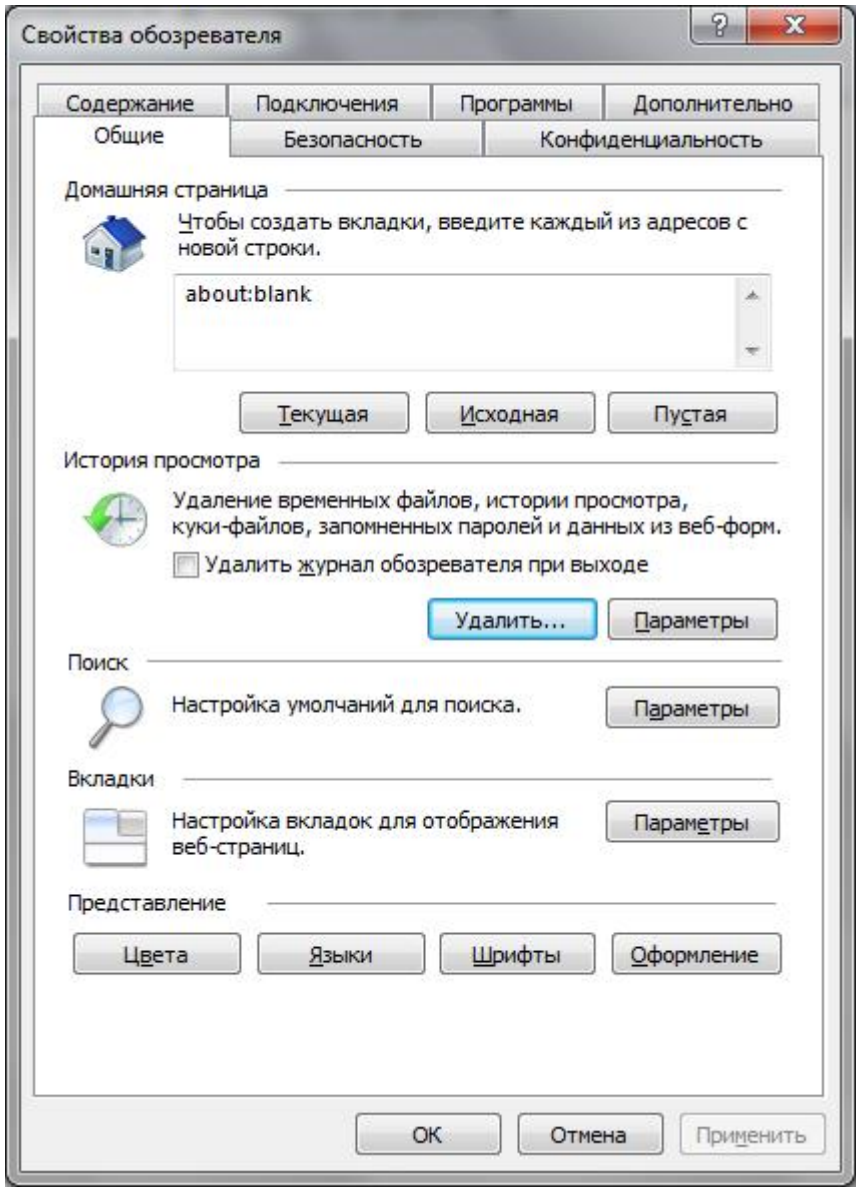

Рис. 1.13. *Свойства обозревателя Internet Explorer*

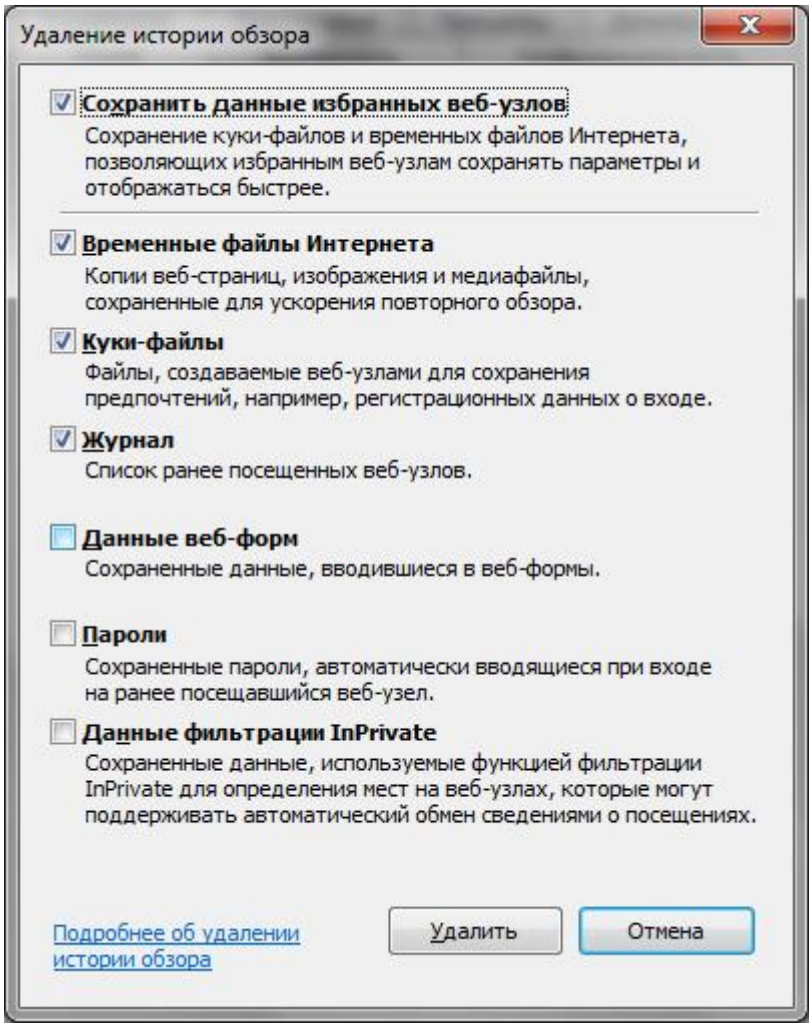

Рис. 1.14. *Удаляем историю обзора*

Примечание

И тем не менее, даже если вы удалите временные файлы (кэш браузера), Cookies, сохраненные пароли и другие служебные данные, сохраняемые браузером, это не обеспечит вам истинной анонимности, поскольку по журналам провайдера заинтересованные и имеющие соответствующие полномочия службы могут легко восстановить всю историю вашей работы в Интернете. Поэтому читаем дальше…

1.5. Что еще нужно знать об анонимности в Интернете?

Перечислим ряд источников информации, из-за которых анонимность пользователя подвергается угрозам.

Служебные данные, сохраняемые браузером. Мы только что узнали, как от них избавиться.

Журналы удаленного узла. Администратор такого узла, проанализировав свои журналы, сможет узнать, кто посещал его сайт и какие файлы он загружал. Как ускользнуть от внимания администратора удаленного узла, мы уже тоже знаем – нужно использовать анонимные прокси-серверы или анонимайзеры. В этом случае в журнал удаленного узла будет записан не ваш IP-адрес, а IP-адрес анонимного прокси.

Журналы шлюза провайдера. Администратор вашего интернет-провайдера при желании легко определит, какие страницы вы посещали и какие файлы загружали, – ведь вся эта информация проходит через его сервер. Замести следы поможет программа Tor, которая будет рассмотрена в *главе 2*.

Примечание

Существуют способы рассекречивания цепочек Tor – это вы тоже должны понимать. Однако цель должна оправдывать средства, учитывая необходимые для рассекречивания цепочки ресурсы. Если вы ничего не "натворили", а просто не хотите, чтобы кто-то узнал, какие сайты вы посещаете, никто не будет специально предпринимать какие-либо действия, чтобы лишить вас анонимности.

Перехват трафика. Находясь в одной сети с "жертвой", злоумышленник может легко перехватить передающиеся по сети данные, увидеть кто и какие сайты загружает, даже прочитать вашу переписку в "аське" или по емейлу. И для этого не нужно быть "крутым хакером" – в Интернете можно легко найти и скачать утилиты, делающие всю "грязную работу" по перехвату и организации информации. Злоумышленнику достаточно просто запустить программу и подождать. Сами понимаете, для этого особыми знаниями и навыками обладать не нужно.

Внимание!

Не верите? Найдите одну из таких программ (например, GiveMeTo или LanDetective Internet Monitor) и убедитесь сами. Многие столь же "полезные" программы можно скачать с сайта **http://www.spyarsenal.com/download.html**. Пусть вам и не требуется перехватывать чей-то трафик, но попробовать такие программы в действии нужно, чтобы самому убедиться, что это реально. Основной здесь принцип такой: предупрежден – значит вооружен (потом не говорите, что я вас не предупреждал). Избежать перехвата трафика можно с помощью той же программы Tor. Точнее, ваш трафик все равно будет перехвачен, но толку злоумышленнику от перехваченных данных не будет, поскольку они будут зашифрованы программой Tor.

Итак, в *главе 2* мы поговорим о том, как посетить заблокированные администратором сайты, а также как зашифровать передаваемые вами данные. Да, вы все правильно поняли – речь пойдет о программе Tor.

1.6. Анонимность и закон

Здесь я постараюсь объяснить читателю, что все действия, описываемые далее в этой книге, – абсолютно законны, дабы ко мне не было никаких претензий (мол, рассказываете, как совершать незаконные действия, или побуждаете к совершению таковых).

В следующих двух главах будут рассмотрены системы анонимизации и шифрования трафика. Но законно ли использование таких систем в Российской Федерации? Некоторые пользователи боятся использовать программное обеспечение подобного рода, поскольку не знают, какие последствия могут быть и чего ожидать от нашего любимого государства.

Внимание!

Перед тем, как продолжить, сразу хочу вас предупредить: я не юрист, никогда им не был и, судя по всему, вряд ли уже им стану. Все, что будет написано далее, – это результат моего собственного анализа и компиляции всевозможных законов и кодексов (знать законы обязан

каждый, поскольку незнание этих самых законов никаким чудодейственным образом не освобождает от ответственности за их нарушение). Поэтому, если вы найдете здесь какие-либо неточности, буду рад выслушать ваши комментарии. Связаться со мной можно через издательство (**mail@bhv.ru**) или напрямую на сайте **www.dkws.org.ua** (пользователь **den**).

Первым делом определимся, чем являются программы шифрования и анонимизации трафика вроде Tor и I2P. Это сетевые приложения, использующие шифрование при передаче данных по сети. В законодательстве ничего не сказано об анонимизации, поэтому будем считать эти программы приложениями, использующими *алгоритмы стойкого шифрования*.

Мы используем наши приложения бесплатно и сами не получаем от их использования никакой выгоды, поскольку на их основе не оказываем никаких коммерческих услуг. И действительно – не будем же мы шифровать трафик соседа, пусть сам себе установит Tor и использует на здоровье.

Теперь обратимся к следующим правовым актам:

Конституция РФ, ст. 23 (декларирует в том числе право на личную неприкосновенность и тайну переписки).

Федеральный закон об информации, информационных технологиях и защите информации № 149-ФЗ.

Начнем с 23-й статьи Конституции РФ:

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Прочитаем внимательно гарантируемые права применительно к нашим проблемам. Выходит, что системы анонимизации и шифрования трафика стоят на страже конституционных прав человека – они технически обеспечивают ваше право на тайну переписки.

Если кто-то запрещает вам использовать подобное программное обеспечение, значит, он нарушает ваши непосредственные конституционные права. Этот кто-то должен ознакомить вас с судебным постановлением, где прямым текстом указан запрет на использование средств защиты данных. Другими словами, если тот или иной администратор с синдромом Наполеона пытается вам запретить использовать средства анонимизации трафика (а как же, ведь он не сможет посмотреть, какие сайты вы посещаете, – тем самым вы ограничиваете его властное чувство), можете смело подать на него в суд.

Что же касается контролирующих органов (не буду перечислять, их очень много на постсоветском пространстве), они могут утверждать, что защиту личных данных гарантирует государство и оно же регулирует право доступа к ним этих самых контролирующих органов. С другой стороны, нигде в Конституции прямо не сказано, что гражданин не имеет право предпринимать самостоятельные действия по защите своей частной жизни.

Настало время обратиться к Федеральному закону № 149-ФЗ. Весь текст закона я приводить здесь не стану, а ограничусь лишь той его частью, которая относится к нашей ситуации (вот фрагмент из ст. 6):

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Получается вот какая картина. Согласно п. 4 ст. 6 Федерального закона № 149-ФЗ *вы можете предпринимать меры по защите информации* и защищать свои права в случае незаконного получения информации – ведь попытка узнать, какие сайты вы посещаете, это и есть незаконное получение информации, поскольку разрешения на получение такой информации, скорее всего, у администратора или еще кого-то нет.

Требование не использовать средства анонимизации и шифрования трафика может быть расценено как нарушение п. 8 ст. 9 Федерального закона № 149-ФЗ:

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

На основании перечисленных правовых актов использование средств анонимизации и шифрования трафика не является незаконным в РФ. Конечно, если у вас возникнут проблемы с использованием подобного ПО, обратитесь к квалифицированному юристу – может, появились дополнительные правовые акты, регулирующие использование программ для шифрования информации. В нашей стране юридическая сфера – крайне динамичная, и все в ней меняется еще быстрее, чем в мире ИТ. А если учесть, что одни законы противоречат другим…

Глава 2. Tor: заметаем следы. Как просто и эффективно скрыть свой IP-адрес

2.1. Как работает Tor? Заходим в Одноклассники на работе

В *главе 1* мы разобрались, как с помощью анонимных прокси-серверов и анонимайзеров скрыть свой IP-адрес. Но, как было показано, оба эти метода не предоставляют нужной степени анонимности.

Усложним поставленную задачу: теперь нам нужно не только скрыть свой IP-адрес от удаленного узла, но и полностью "замаскироваться" – чтобы администратор нашей сети или кто-то еще не смогли определить, какие узлы мы посещаем, и чтобы никто не смог "подслушать" передаваемые нами данные.

Именно для решения таких задач и была создана *распределенная сеть Tor*. Tor (аббревиатура от The Onion Router) – это свободное (то есть свободно распространяемое и абсолютно бесплатное) программное обеспечение, использующееся для анонимизации трафика.

> **Примечание**
>
> Поскольку исходный код Tor открыт всем желающим, любой пользователь может проконтролировать Tor на наличие/отсутствие "черного хода", специально созданного для спецслужб или еще кого-то. На данный момент Tor не скомпрометировал себя – его репутация незапятнанна.

Сеть Tor обеспечивает надежную анонимизацию и защищает пользователя от слежки как за посетителями конкретного сайта, так и за всей активностью самого пользователя. К тому же все передаваемые пользователем данные шифруются, что исключает их прослушивание.

Вкратце принцип работы Tor заключается в следующем: при передаче данных от узла А (ваш компьютер) к узлу Б (удаленный сайт) и обратно данные передаются в зашифрованном виде через цепочку промежуточных узлов сети.

Отсюда следует еще одно преимущество использования Tor, которое наверняка оценят пользователи корпоративных сетей. Поскольку узел (нод, от англ. *node*) А обращается к узлу Б не напрямую, а через промежуточные узлы, то это позволяет обойти "черный список" брандмауэра сети.

Рассмотрим конкретный пример. Предположим у вас в офисе "злой" администратор заблокировал доступ сотрудников к социальной сети, к тем же Одноклассникам (наверное, это самая популярная сеть на наших просторах, хотя есть и не менее популярные: ВКонтакте, Мой мир, Facebook и др.). Сайт **www.odnoklassniki.ru** и будет узлом Б, ваш рабочий компьютер – это узел А.

Вы запускаете программу Tor и вводите адрес узла Б. Передаваемые вами данные (в данном случае – адрес узла) будут зашифрованы и переданы первому узлу в цепочке – назовем его узел В, затем данные в том же зашифрованном виде будут переданы узлу Г и т. д. Так будет продолжаться, пока данные не получит последний узел цепочки (скажем, узел Т), который и передаст ваш запрос конечному узлу – Б. Понятно, что на последнем участке (от узла Т к узлу Б) данные будут незашифрованы, поскольку узел Б не поддерживает открытые ключи сети Tor (если бы это было так, то весь Интернет был бы анонимным).

Посмотрите на рис. 2.1 – на нем изображен процесс передачи данных между вашим и удаленным компьютерами через сеть Tor. Проанализировав его можно сделать следующие выводы:

администратор вашей сети (или администратор провайдера) не сможет узнать, какие данные вы передаете, поскольку данные передаются в зашифрованном виде;

администратор вашей сети не сможет узнать, какой узел вы посещаете, поскольку вместо интересующего вас узла (**www.odnoklassniki.ru**, **www.vkontakte.ru** и т. п.) ваш узел формально будет обращаться к одному из узлов сети Tor – ничем не примечательному узлу с непонятным доменным именем. Тем более, что при каждом новом подключении к Tor первый узел цепочки будет другим;

если администратор сети заблокировал доступ к интересующему вас узлу (**www.odnoklassniki.ru**, **www.vkontakte.ru** и т. п.) на брандмауэре, вы сможете обойти это ограничение, поскольку фактически ваш компьютер подключается к совершенно другому узлу (к узлу цепочки Tor). Запрещать доступ к этому узлу нет смысла, т. к. при следующем подключении к Tor или при принудительной смене цепочки узел входа в Tor будет изменен;

удаленный узел "увидит" только IP-адрес последнего узла цепочки, ваш IP-адрес будет скрыт;

теоретически перехват данных возможен на последнем участке пути – от последнего узла цепочки Tor до удаленного узла. Но для этого нужно отследить всю цепочку Tor, что технически сделать очень сложно, поскольку она может состоять из десятков узлов. Если же получить доступ к удаленному узлу, то все равно нельзя будет понять, кто есть кто, поскольку для этого нужно знать как минимум точку входа и точку выхода сети Tor.

При подключении к сети Tor для вашего компьютера определяется точка входа (выбирается случайный узел из сотен тысяч узлов Tor), "тоннель" и точка выхода – то есть строится цепочка. В процессе работы с сетью иногда возникает необходимость сменить цепочку – это можно сделать без перезагрузки программного обеспечения (позже будет показано, как), что делает работу с сетью максимально комфортной.

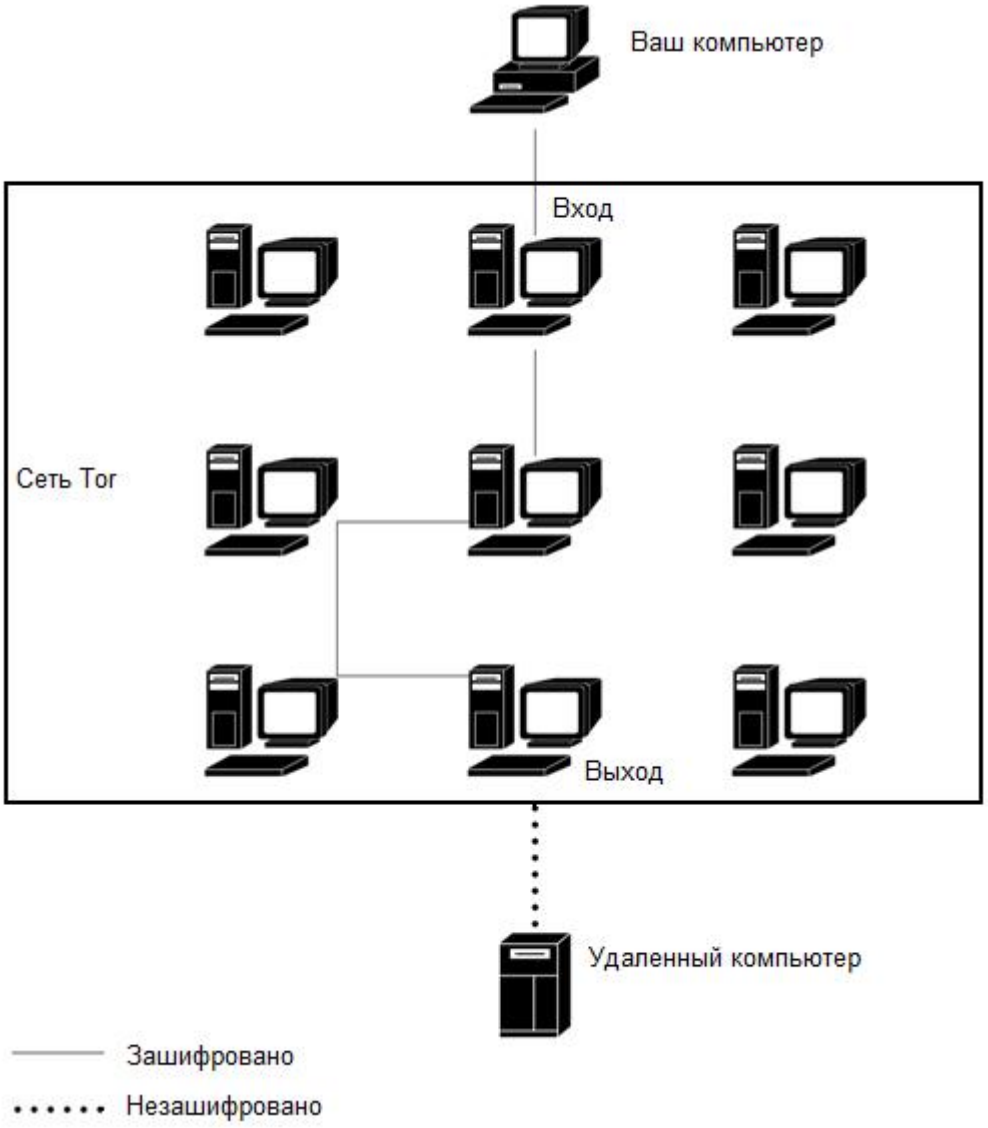

Рис. 2.1. *Передача данных через распределенную сеть Tor*

Смена цепочки может понадобиться в двух случаях:

когда нужно сменить конечный IP-адрес (например, чтобы получить IP-адрес, относящийся к определенной стране или городу);

когда полученная цепочка оказалась довольно медленной. Скорость передачи информации зависит от каналов передачи данных от одного узла цепочки к другому, поэтому сгенерированная цепочка может оказаться нерасторопной. Вы же можете создать другую цепочку – вдруг она окажется быстрее?

> **Примечание**
>
> Несколько лет назад Tor работала довольно медленно – иногда приходилось даже отключать картинки, чтобы дождаться загрузки странички. Сейчас с производительностью все нормально, и нет прямой необходимости отключать загрузку картинок.

Дополнительную информацию о сети Tor вы можете получить по адресу: **http://tor.cybermirror.org/faq.html.ru**.

В *главе 3* мы поговорим о другом проекте для анонимизации трафика – I2P. В отличие от Tor, в I2P возможна полная анонимность, но при условии, что оба участника обмена

трафиком подключены к I2P. Забегая вперед, отмечу, что сеть I2P идеально подходит для "шпионов", желающих общаться тайно, но не для посещения заблокированных сайтов или смены IP-адреса.

2.2. Tor или анонимные прокси-серверы и анонимайзеры. Кто кого?

Если вам понятен принцип работы Tor, то ее преимущества тоже должны быть ясны, но на всякий случай сравним Tor с анонимными прокси-серверами и анонимайзерами:

анонимайзеры и анонимные прокси не шифруют передаваемые данные, поэтому администратору вашей сети (или сети провайдера) будет легко вычислить, какие сайты вы посещали и какие данные передавали. Сеть Tor шифрует всю передаваемую информацию, поэтому даже если кто-то перехватывает данные, передающиеся по вашему каналу связи, он получит только бессмысленные наборы байтов. Однако за все нужно платить – Tor работает медленнее, чем анонимайзеры, хотя быстрее, чем некоторые анонимные прокси;

некоторые анонимные прокси-серверы на самом деле таковыми не являются, поскольку сообщают ваш IP-адрес удаленному узлу в заголовках HTTP-запроса. Без специальной проверки (а для этого вам нужно приобрести свой сервер или хотя бы купить хостинг и написать сценарий, анализирующий заголовки HTTP-запросов от анонимного прокси) нельзя узнать, является ли прокси-сервер действительно анонимным. При использовании Tor скрыт не только ваш IP-адрес (от внимания администратора удаленного узла), но и адрес назначения (от внимания администратора вашей сети);

при использовании анонимного прокси-сервера проследить цепочку довольно просто – в ней будет всего три элемента: ваш компьютер, анонимный прокси и удаленный компьютер. Ваша анонимность, по сути, зависит только от одного псевдоанонимного прокси-сервера. А вдруг этот анонимный прокси передает информацию заинтересованным лицам? При использовании Tor вы доверяете передаваемые данные нескольким случайным серверам, которые выбраны из тысяч доступных узлов сети Tor. Многие эти узлы представляют собой обычные домашние компьютеры (позже я расскажу, как стать волонтером сети Tor и как помочь сделать Интернет действительно анонимным). Чтобы отследить передаваемые данные, ваш противник (пусть это будет тот самый злой администратор сети) должен контролировать все эти случайно выбранные узлы, разбросанные по всему миру. Сами понимаете, что вероятность такого контроля ничтожно мала;

некоторые анонимные прокси (или анонимайзеры) предлагают зашифрованный обмен данными (между вами и прокси), но такие серверы, как правило, платные. Сеть Tor абсолютно бесплатна, и при этом использование Tor ни к чему вас не обязывает – вы можете быть как обычным клиентом, так и узлом сети Tor, – режим работы выбирается по вашему желанию;

анонимные прокси обычно поддерживают только HTTP-трафик, а сеть Tor теоретически можно настроить на поддержку любого TCP-соединения;

Tor, в отличие от других подобных систем (имею в виду JAP[1]) и некоторых анонимных прокси, ни разу себя не скомпрометировала и имеет незапятнанную репутацию – ведь ее исходный код открыт, и любой желающий может с ним ознакомиться. А вот разработчики JAP были пойманы на добавлении "черного хода" по запросу спецслужб.

[1] Программа JAP – одна из программ, обеспечивающих анонимность в Интернете. Она скрывает реальный IP-адрес, перемешивая данные всех пользователей JAP с помощью микс-прокси до тех пор, пока отследить реальный адрес станет невозможно.

2.3. Критика Tor и скандалы вокруг этой сети

Некоторые специалисты критикуют Tor, поскольку она может использоваться для организации преступных действий. Ряд стран даже объявили войну Tor – например, в 2006 году спецслужбы Германии захватили шесть компьютеров, работающих узлами сети Tor, а в 2007 году немецкая полиция арестовала владельца одного из узлов сети Tor, поскольку через его узел неизвестный отправил ложное сообщение о теракте. В 2009 году в Китае были заблокированы до 80 % IP-адресов публичных серверов Tor.

Однако возможность применения в преступных целях не делает Tor оружием злоумышленников. Наоборот, они предпочитают использовать другие методы: spyware, вирусы, взлом прокси-серверов, использование краденых мобильных телефонов и т. п. Злоумышленник может украсть мобильный телефон, выйти в Интернет, передать провокационное сообщение, а затем выбросить телефон в реку, зачем ему сложности с Tor?

Сеть Tor в большинстве случаев используется законопослушными пользователями, пытающимися обойти ограничения брандмауэра родной сети, а также не желающими, чтобы за ними следили.

Не нужно думать, что Tor – это панацея, и если вы используете эту сеть, то на 100 % анонимны. Нет. Вас все же могут рассекретить. Методы различны: от клавиатурного шпиона, установленного на вашем компьютере, до создания выходного сервера Tor, который будет перехватывать весь трафик. Если ваш трафик будет выходить из сети Tor через этот сервер, то он может быть перехвачен злоумышленником.

> **Из истории вопроса…**
>
> В 2007 году национальная полиция Швеции арестовала эксперта по компьютерной безопасности Дена Эгерстада (Dan Egerstad), поскольку он неправомерно получил доступ к компьютерной информации. Эгерстад создал пять выходных серверов Tor и перехватывал незашифрованный трафик, в результате чего получил пароли к электронной почте посольств, государственных организаций, правоохранительных органов разных стран и т. п.

Подробнее об этом и других интересных фактах вы сможете прочитать на страничке Википедии (не вижу смысла приводить эту информацию в книге, если вы можете прочитать ее бесплатно): **http://ru.wikipedia.org/wiki/Tor**. Настоятельно рекомендую на досуге посетить приведенную ссылку – вы узнаете много интересных фактов о сети Tor, а мы тем временем перейдем к практике – к использованию Tor.

> **Совет**
>
> Вас мучает совесть, что в случае использования Tor вы тем самым поспособствуете распространению кибер-преступности? Тогда перейдите по следующей ссылке, и все сомнения исчезнут: **http://tor.cybermirror.org/faq-abuse.html.ru**.

2.4. Установка и использование Tor

2.4.1. Быстро, просто и портабельно: Tor на флешке

Программное обеспечение Tor можно сравнить со швейцарскими часами – последние можно покупать только в фирменном магазине, чтобы не нарваться на подделку. Также и

Tor следует скачивать только с официального сайта по адресу: **https://www.torproject.org/** (рис. 2.2).

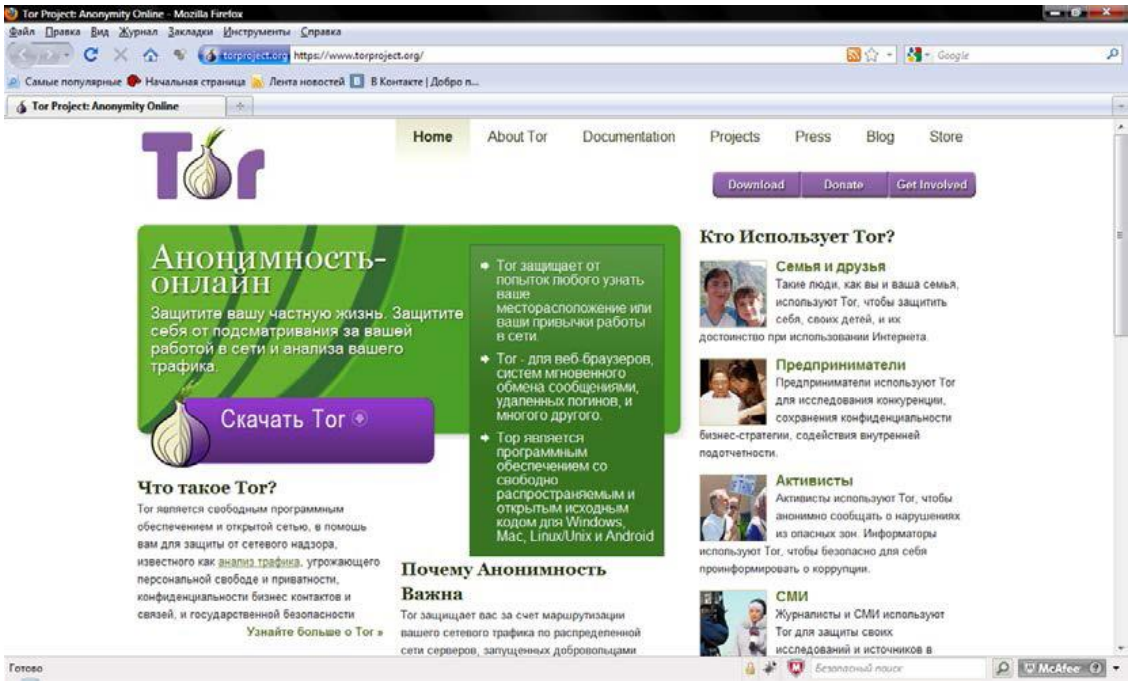

Рис. 2.2. *Официальный сайт Tor*

Не рекомендую загружать программное обеспечение Tor из всевозможных каталогов программ – в него могут быть встроены "черные ходы"; кроме того, такое "нефирменное" программное обеспечение может быть модифицировано злоумышленниками для передачи информации (ваших паролей, электронных писем и т. п.) третьим лицам. Помните, что исходный код Tor доступен каждому, и это основное ее преимущество, но и основной недостаток тоже. Ведь каждый может скачать и модифицировать комплект Tor, а затем выложить на своем сайте, якобы с благими намерениями (типа, комплект Tor с браузером Firefox, в котором установлены дополнительные плагины). А вы, загрузив и установив такую модифицированную версию Tor, получите систему, которая будет передавать злоумышленнику всю информацию о вас. Поэтому идем на официальный сайт и скачиваем все там.

Надо отметить, что тут существуют варианты:

можно скачать уже преднастроенный комплект программного обеспечения – вам надо будет запустить только одну программу, немного подождать, пока осуществится подключение к сети Tor, и вы готовы к работе,

а можно скачать все необходимое по отдельности и настраивать привязку компонентов вручную.

Мы будем ориентироваться на уже готовый комплект, поскольку так меньше вероятность допустить при настройке ошибку, из-за которой анонимность не будет обеспечиваться.

Рассмотрим состав готового комплекта:

Tor – сердце системы анонимизации трафика. Эта программа строит цепочки, по которым должны передаваться ваши данные, пропускает через них данные и получает ответы. Программа Tor, по сути, является прокси-сервером и работает аналогично прокси-серверу SOCKS, локальные соединения принимаются на порт 9050. Благодаря этому на работу через Tor можно настроить практически любую программу;

Vidalia – панель управления программой Tor, используется для настройки Tor и наблюдения за его работой;

Provioxy – анонимизирующий HTTP/HTTPS прокси-сервер. Приложение является надстройкой над Tor и улучшает защиту в программах, использующих протоколы HTTP и HTTPS (обычно это браузеры). Эта программа использует тот же порт 9050;

плагин Torbutton – специальный плагин для браузера Firefox, включающий и выключающий анонимизацию трафика. При включении анонимизации трафика выключаются все плагины, по которым можно вычислить ваш реальный IP-адрес, а именно: Java, Flash, ActiveX, RealPlayer, Quicktime, Adobe PDF и некоторые другие. Да, видео на Youtube анонимно вы не посмотрите.

По адресу **https://www.torproject.org/download/download.html.ru** вы можете скачать два уже настроенных комплекта программного обеспечения:

пакет Tor Browser – включает в себя описанное ранее программное обеспечение и английскую версию браузера Mozilla Firefox. Использовать другие браузеры, особенно с закрытым исходным кодом, не рекомендуется, поскольку нет никакой гарантии, что они не передают конфиденциальную информацию третьим лицам. Браузер Firefox, включаемый в состав пакета Tor Browser, проверяется разработчиками Tor (да и исходный код Firefox открыт для всех желающих), что исключает возможность установки "черного хода". Подробнее о выборе браузера мы поговорим в *главе 12*;

> **Примечание**
>
> В главе 12 также будет показано, как настроить проприетарные ICQ-клиенты (программы QIP и ICQ) для работы через распределенную сеть Tor.

пакет Tor Browser Instant Messaging Bundle – содержит не только браузер, но и клиент мгновенного обмена сообщениями. В качестве такого клиента используется программа Pidgin, поэтому теперь ваши беседы в ICQ, Jabber и других службах мгновенного обмена сообщениями будут защищены от прослушки. Подробнее о Pidgin можно прочитать по адресу **http://ru.wikipedia.org/wiki/Pidgin**.

> **Примечание**
>
> К сожалению, в настоящее время пакет Tor Browser Instant Messaging Bundle временно не распространяется из-за ошибки в Pidgin, сводящей на нет все старания программы Tor анонимизировать трафик. В скором времени эта проблема будет устранена, и пакет снова станет доступным для загрузки (может быть, даже к моменту выхода этой книги из печати).

Преимущества преднастроенного пакета очевидны. Во-первых, вам не придется ничего настраивать, следовательно, вы не сможете совершить ошибку. Во-вторых, вы можете распаковать загруженный архив прямо на флешку, и комплект программ для анонимизации трафика будет всегда с вами. А это значит, что вы можете не бояться заходить в Интернет с чужих компьютеров – при условии, что на компьютере не установлен клавиатурный шпион, никто не перехватит ваши данные.

Настройка Tor вручную может понадобиться в двух случаях: если у вас уже есть настроенный браузер Firefox, или же вам нужно настроить другую сетевую программу (которая не является браузером или клиентом обмена сообщениями) на работу через Tor.

Первый случай неактуален. Пусть на вашем компьютере имеется Firefox с уже установленными плагинами. Но ведь при включении режима анонимизации трафика (плагин Torbutton) большинство полезных плагинов (как уже отмечалось ранее) будут отключены. Однако Torbutton не может знать обо всех плагинах, потенциально способных передавать ваш IP-адрес третьей стороне, поэтому из соображений безопасности свой браузер использовать не рекомендуется. Лучше использовать "чистый" браузер, входящий в комплект Tor Browser.

Второй случай актуален при настройке сторонних программ. Но опять-таки, вам никто не мешает загрузить пакет Tor Browser и использовать его компоненты для анонимизации трафика сторонней программы. Далее будет показано, как настроить почтовый клиент Thunderbird *(см. разд. 2.4.3)* и программу интернет-телефонии Skype *(см. разд. 2.4.4)* на использование Tor.

Прямая ссылка на загрузку последней версии Tor Browser выглядит так:

https://www.torproject.org/dist/torbrowser/tor-browser-2.2.32-3_ru.exe

Однако я вам советую воспользоваться кнопкой **Download** на официальном сайте Tor – вы будете уверены, что загружаете самую последнюю версию Tor Browser.

Запустите загруженный файл (это самораспаковывающийся архив), и все, что вам нужно сделать, – это указать каталог, в который следует распаковать Tor (рис. 2.3). Пакет Tor Browser для Windows может работать в Windows 7, Windows Vista и Windows XP.

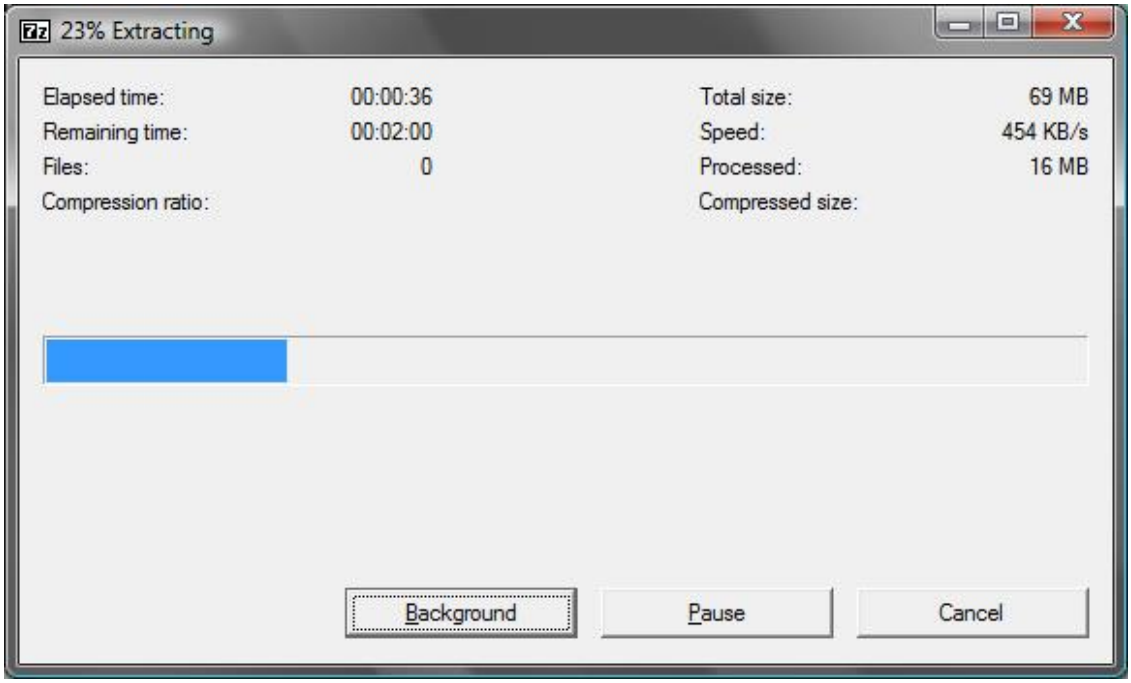

Рис. 2.3. *Распаковка Tor Browser*

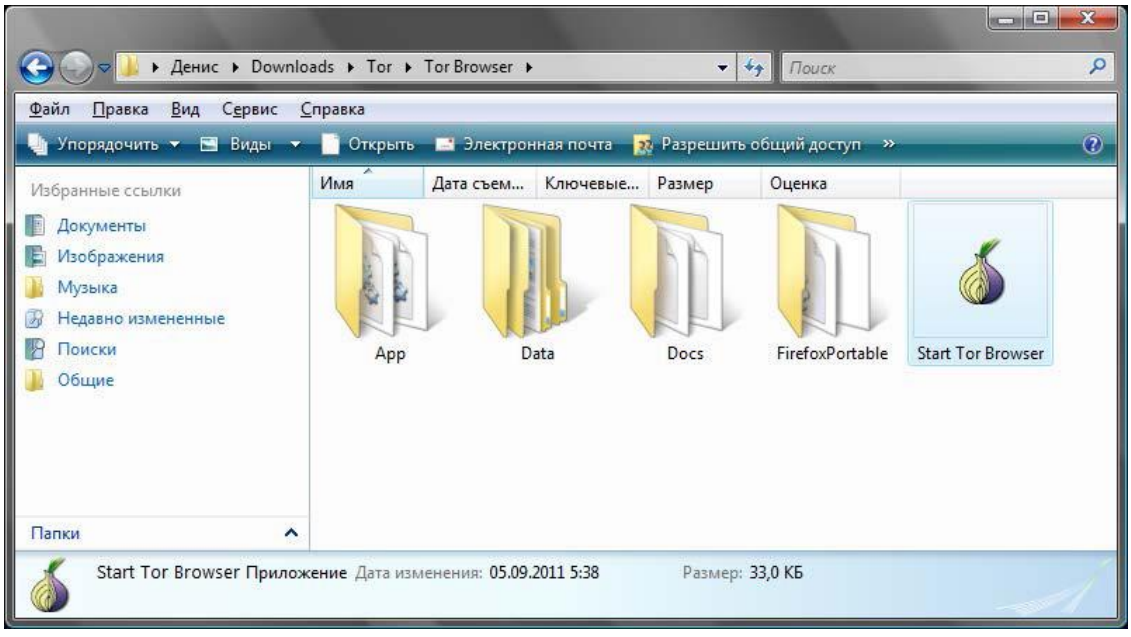

Рис. 2.4. *Запустите программу Start Tor Browser.exe*

Перейдите в каталог, в который вы распаковали Tor Browser, и запустите программу Start Tor Browser.exe (рис. 2.4).

Откроется окно панели управления Vidalia – придется немного подождать, пока будет выполнено подключение к сети Tor (рис. 2.5). Установив соединение, Vidalia запустит браузер Firefox, входящий в комплект Tor Browser. Для проверки состояния подключения к сети браузер обратится к сценарию **https://check.torproject.org/?lang=en-US&small=1**, который сообщит статус соединения (рис. 2.6). Как можно видеть, соединение с сетью Tor установлено, и теперь вы анонимны. Сценарий проверки состояния соединения сообщает также и ваш новый IP-адрес, в данном случае это: 192.251.226.205.

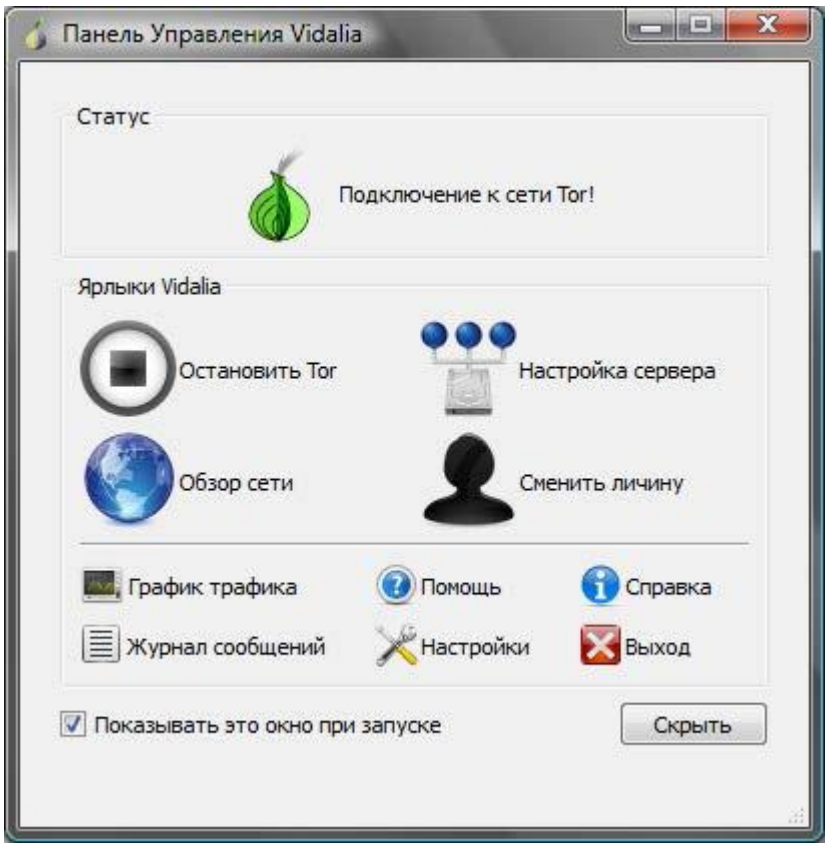

Рис. 2.5. *Панель управления Vidalia*

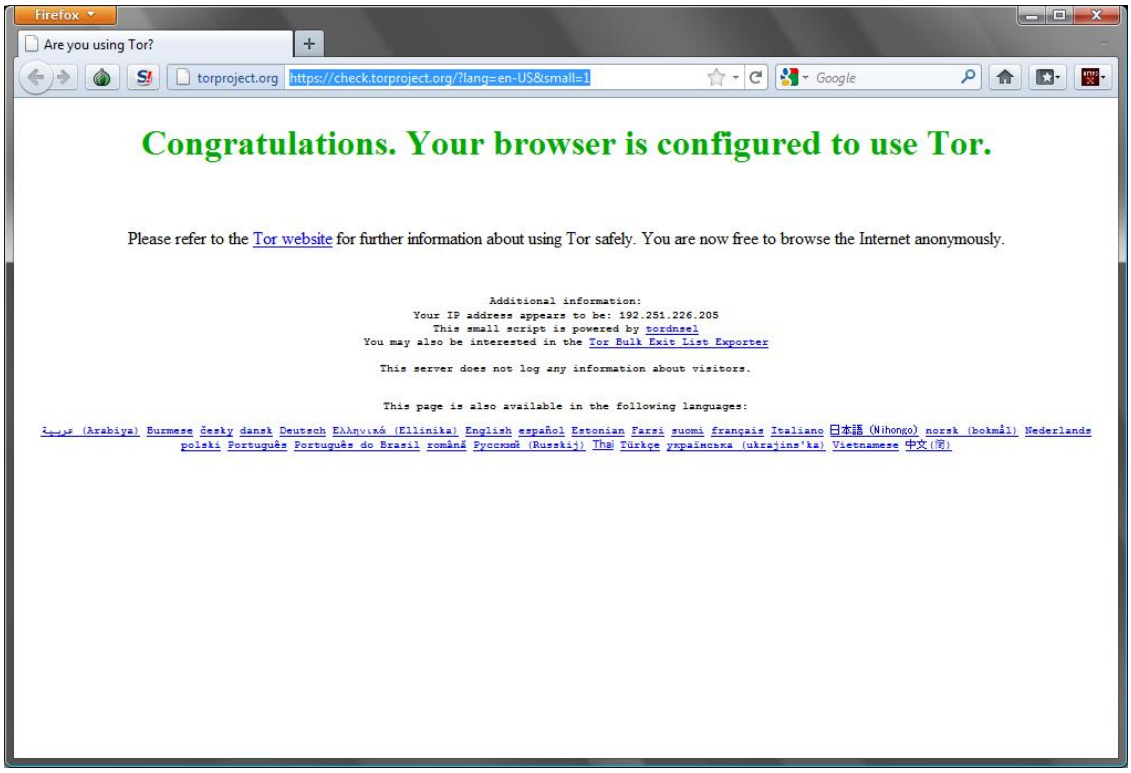

Рис. 2.6. *Браузер Firefox: соединение с Tor установлено*

Рис. 2.7. *Tor включен*

Проконтролировать, работает ли Tor, можно и по-другому – в процессе анонимного серфинга. Для этого подведите указатель мыши к кнопке с изображением логотипа Tor (рис. 2.7) – всплывающая подсказка покажет состояние подключения к Tor. Если нажать на эту кнопку, откроется меню. В нем, помимо других команд, будет присутствовать команда **Настройки**, позволяющая настроить плагин Torbutton.

> **Внимание!**
>
> Будьте осторожны – в большинстве случае настройки Torbutton изменять не требуется, а неправильные параметры могут привести к потере анонимности. Тем не менее в следующем разделе мы с некоторыми настройками познакомимся.

Что делать дальше? Просто вводите адрес желаемого узла и наслаждайтесь анонимным серфингом. Скорость соединения зависит от узла, к которому вы подключаетесь, и от сгенерированной цепочки.

2.4.2. Панель управления Vidalia

Настало время рассмотреть панель управления Vidalia, изображенную на рис. 2.5. В окне Vidalia вы найдете следующие кнопки:

Остановить Tor – служит для останова Tor, затем эту же кнопку можно использовать для запуска Tor. В большинстве случаев перезапускать Tor не нужно, а если вы желаете сменить IP-адрес и всю цепочку, лучше нажать кнопку **Сменить личину**;

Обзор сети – позволяет визуально оценить созданную цепочку (рис. 2.8);

Настройка сервера (она же **Настройки**) – вызывает окно настроек, его мы рассмотрим чуть позже;

Сменить личину – раньше (в предыдущих версиях Vidalia) эта кнопка называлась **Сменить цепочку**, зачем нужно было ее переименовывать, я не знаю. Изменение цепочки позволяет изменить список узлов, через которые будет происходить обмен данными, и сменить конечный IP-адрес;

График трафика – небольшое окошко, показывающее, какой объем информации был получен и передан через сеть Tor;

Помощь – открывает окно справки;

Справка – показывает информацию о версии Vidalia и Tor. Хотя правильнее бы эту кнопку назвать **О программе**.

Выход – завершает работу Tor и закрывает окна Vidalia и Firefox.

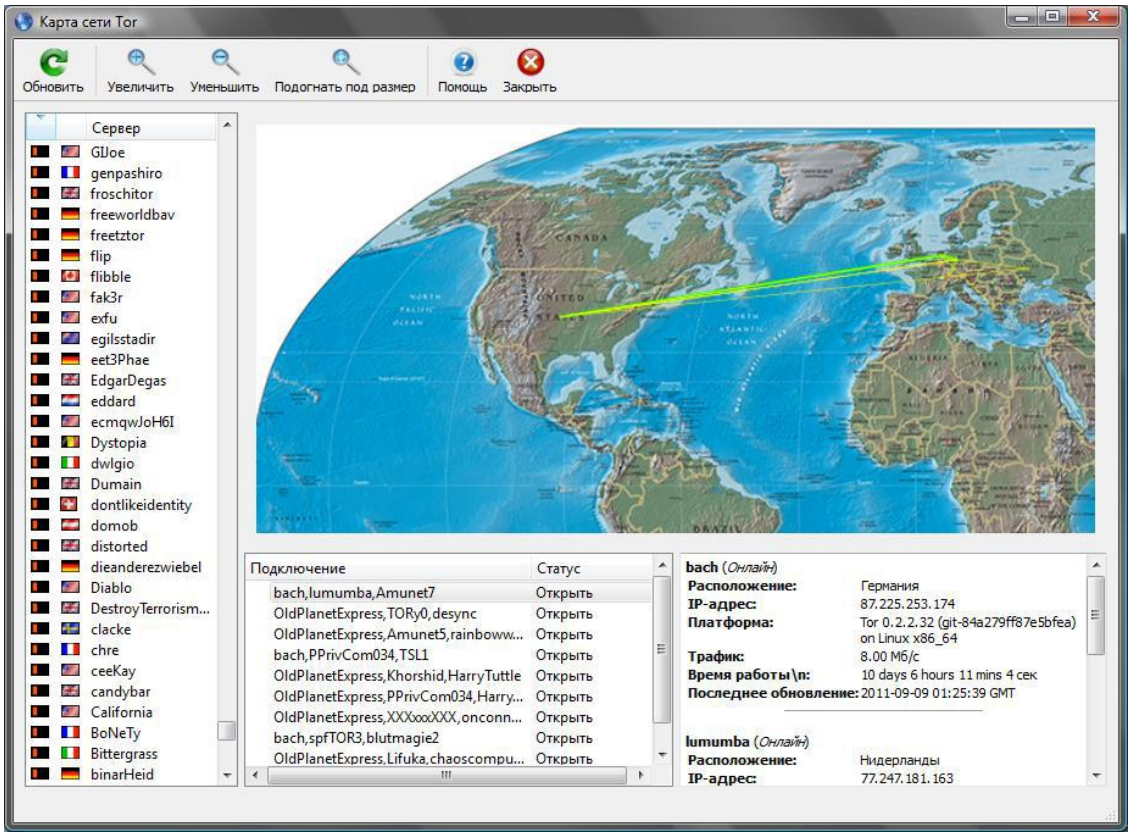

Рис. 2.8. *Цепочка Tor на карте мира*

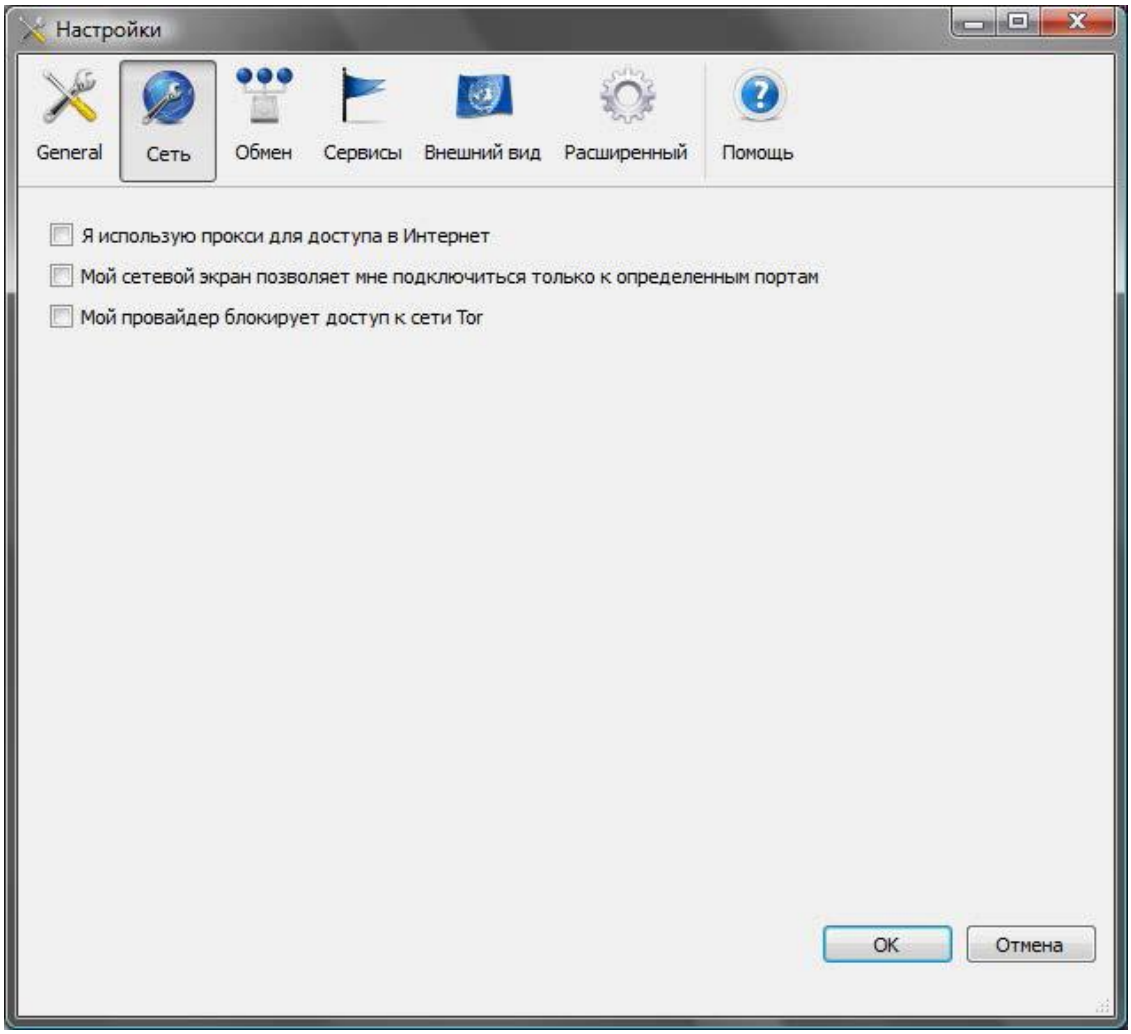

Рис. 2.9. *Параметры раздела* ***Сеть***

Нажмите кнопку **Настройки**. Не все настройки Tor важны. Наиболее важные настройки находятся в разделах **Сеть** и **Обмен**. Начнем с первого раздела (рис. 2.9):

 # Я использую прокси для доступа в Интернет – если доступ к Интернету осуществляется через прокси-сервер, который вы обычно указывали в настройках браузера, включите этот параметр и укажите параметры прокси: имя узла, порт, имя пользователя и пароль (если нужно);

 # Мой сетевой экран позволяет мне подключиться только к определенным портам – используется для обхода брандмауэра. После включения этого параметра появится поле, в котором надо ввести разрешенные порты через запятую. В этой строке не должно быть пробелов. Пример: 80,443,3128;

 # Мой провайдер блокирует доступ к сети Tor – некоторые провайдеры блокируют доступ к Tor. В этом случае включите параметр и укажите мосты, через которые будет осуществляться доступ к Tor (рис. 2.10). Список мостов доступен по адресу **https://bridges.torproject.org**. Можно также нажать кнопку **Найти мосты** для автоматического поиска мостов Tor. Однако провайдер может тоже воспользоваться этой функцией и заблокировать полученные узлы… Так что гарантий, что Tor у вас заработает в случае блокировки провайдером, никаких нет.

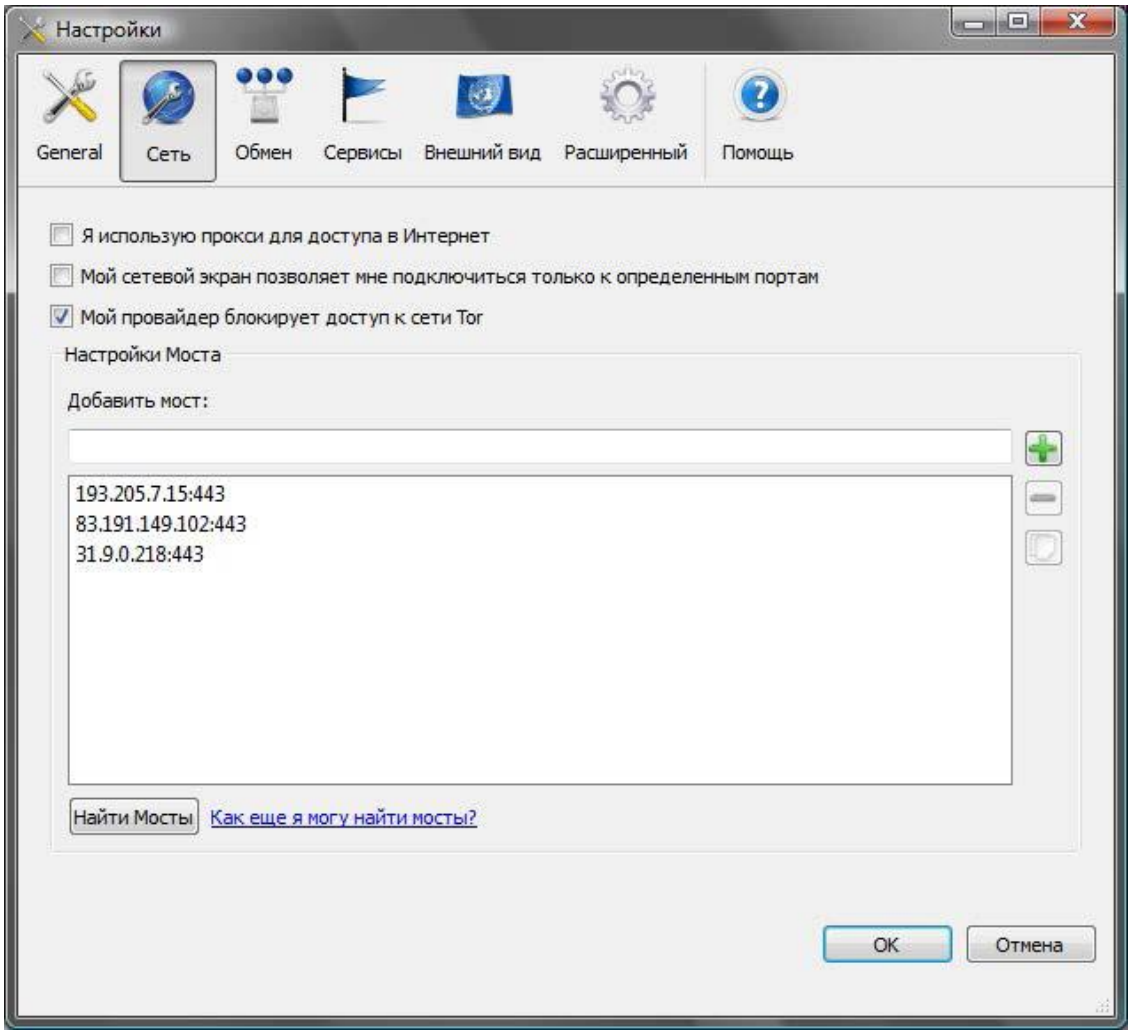

Рис. 2.10. *Добавление мостов Tor*

В разделе **Обмен** (рис. 2.11) вы можете выбрать режим работы Tor:

 # Режим работы только как клиент – используется по умолчанию, вы подключаетесь к Tor и используете ее ресурсы, но не предоставляете ничего взамен;

 # Серверный трафик сети Tor – вы можете превратиться из простого обывателя в узел сети Tor. Для этого выберите этот режим работы и на вкладке **Основные настройки** введите информацию о себе – ваш псевдоним (поле **Ник**) и адрес электронной посты;

на вкладке **Пределы полосы пропускания** вы можете установить предел использования вашего канала связи, иначе Tor узурпирует весь ваш интернет-канал;

вкладка **Правила выхода** позволяет определить ресурсы Интернета, к которым другие пользователи Tor смогут получить доступ через ваш компьютер (сайты, безопасные сайты, почта, мгновенные сообщения и др.);

 # Помочь заблокированным пользователям получить доступ к сети Tor – если в предыдущем случае вы становитесь просто сервером (нодом) сети Tor, то в этом вы превращаетесь в мост, через который другие пользователи будут заходить в Tor.

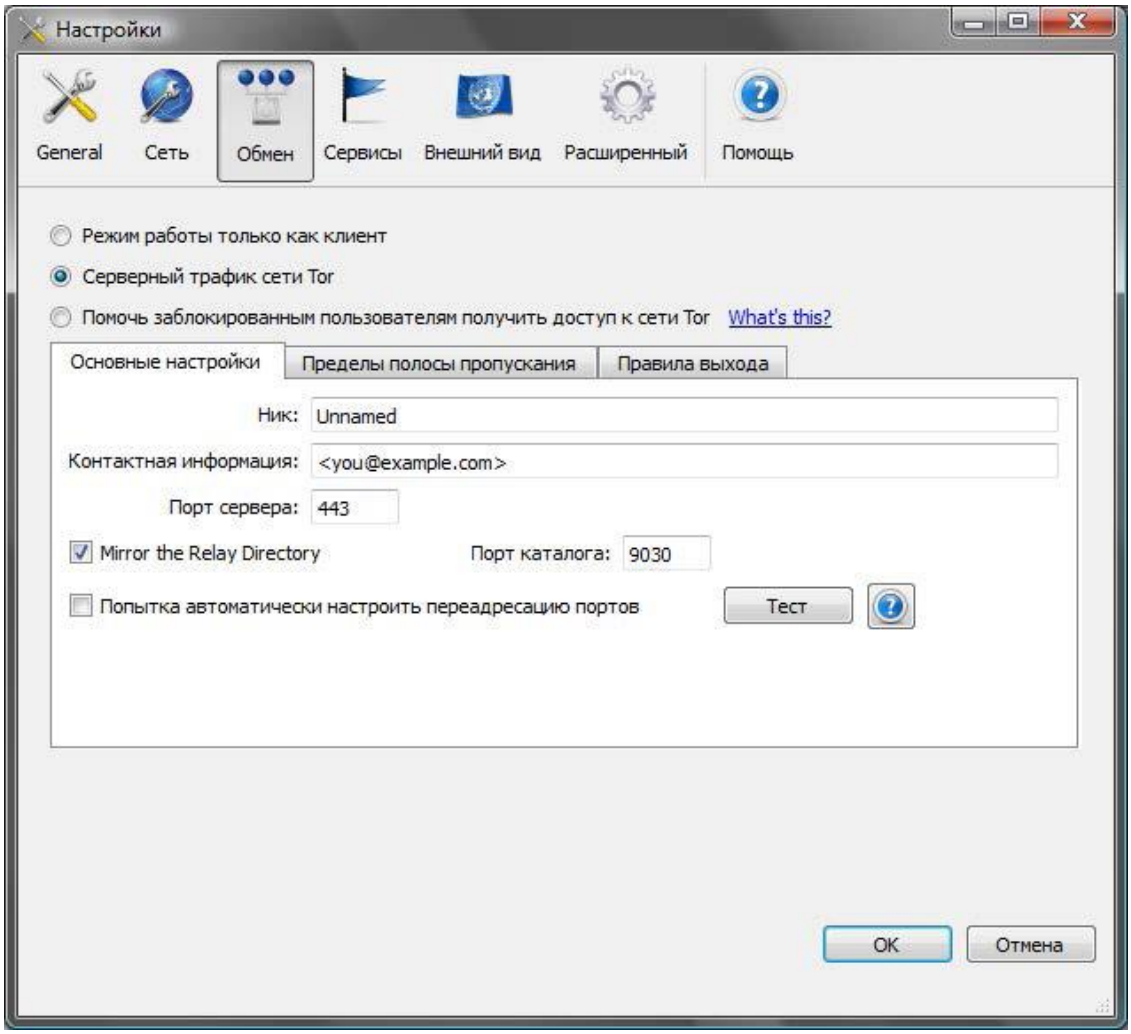

Рис. 2.11. *Параметры раздела* ***Обмен***

Помогать или не помогать сети Tor? С одной стороны, она безвозмездно помогает вам. С другой стороны, если кто-либо из пользователей совершит противоправное действие, а ваш узел окажется точкой выхода, подозрение падет на вас. Так что, если вы решили стать волонтером, то:

 # Ограничьте пропускную полосу – не нужно, чтобы Tor забирал весь интернет-канал, вам ведь тоже нужно;

на вкладке **Правила выхода** отключите параметры **Получать почту** и **Прочие сервисы** – так, по крайней мере, ваш компьютер не будет использоваться для рассылки спама.

Осталось рассмотреть еще один вопрос, а именно – выбор узлов выхода, что важно, если вы хотите заполучить на выходе IP-адрес определенной страны. В подкаталоге Data\Tor каталога установки пакета Tor Browser находится конфигурационный файл torrc. Откройте его и добавьте две строки:

EntryNodes $fingerprint,$fingerprint….

ExitNodes $fingerprint,$fingerprint….

Первый параметр задает список входных узлов, а второй – выходных. Вместо переменной $fingerprint вы можете задать:

идентификатор узла в сети Tor (его можно узнать с помощью карты);

IP-адрес узла (но нужно быть точно уверенным, что он является сервером сети Tor, это тоже можно узнать с помощью карты);

ISO-код страны, например, {de} для Германии, {ru} для России и т. д. Для определения кода страны вам пригодится следующая ссылка: **http://www.perfekt.ru/dict/cc.html**.

Примечание

Разработчики Tor не рекомендуют использовать параметры EntryNodes и ExitNodes (это плохо влияет на анонимность), но вы можете поступать так в крайних случаях – когда нужно заполучить цепочку с жестко заданными входными и выходными узлами.

2.4.3. Настройка почтового клиента Mozilla Thunderbird

Рассмотрим настройку почтового клиента для работы с сетью Tor на примере программы Mozilla Thunderbird. Выполните следующие действия:

1. Запустите Tor и с помощью Vidalia убедитесь, что подключены к сети Tor.
2. Запустите Mozilla Thunderbird
3. Выберите команду **Инструменты | Настройки**.
4. Перейдите в раздел **Дополнительно**, далее – на вкладку **Сеть и дисковое пространство** (рис. 2.12).
5. Нажмите кнопку **Соединение**. В открывшемся окне установите параметры так, как показано на рис. 2.13.

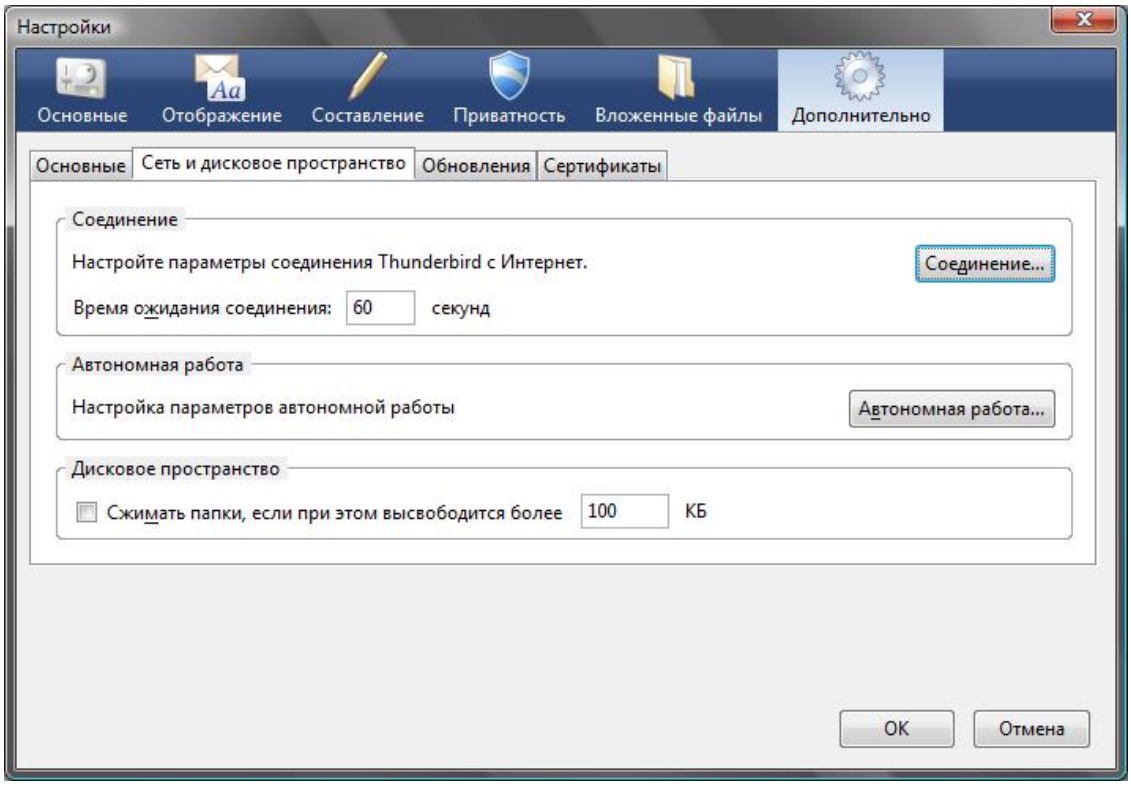

Рис. 2.12. *Настройки Mozilla Thunderbird: вкладка* ***Сеть и дисковое пространство***

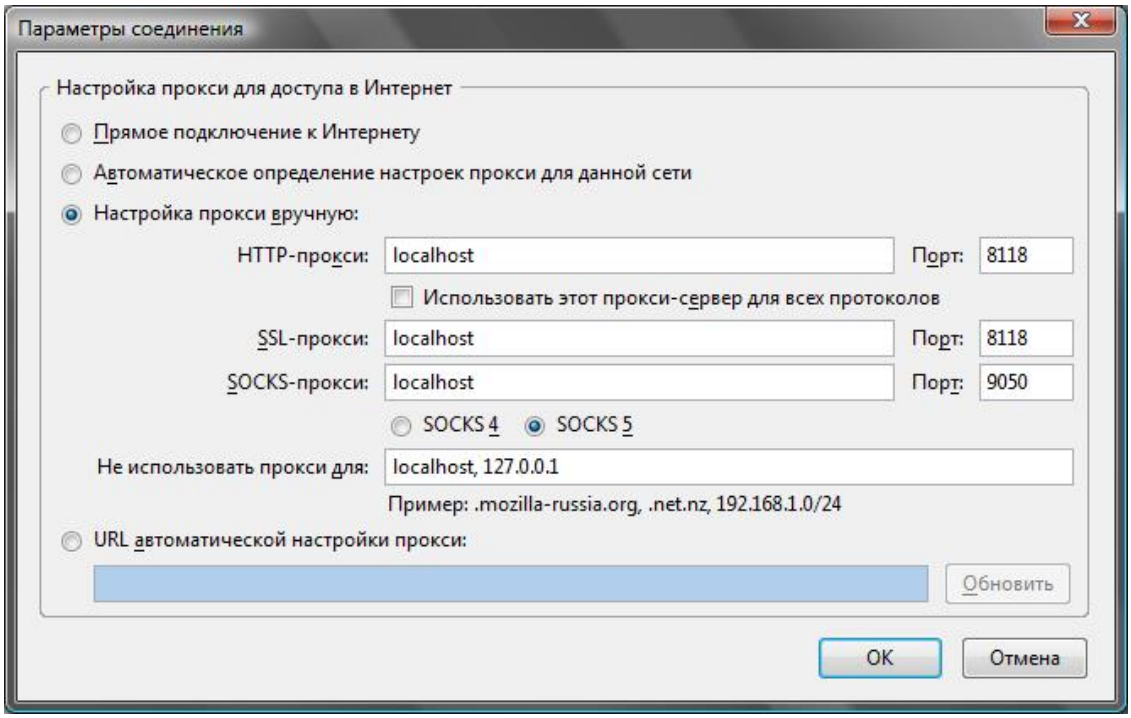

Рис. 2.13. *Параметры прокси-сервера: настройка на использование Tor*

2.4.4. Настройка программы интернет-телефонии Skype

Популярную программу интернет-телефонии Skype тоже можно настроить на использование Tor. Для этого выполните команду **Инструменты | Настройки**, перейдите в раздел **Дополнительно | Соединение** и установите параметры так, как показано на рис. 2.14.

Вот только со Skype есть одна проблема. Вообще-то Skype – программа с закрытым исходным кодом. Алгоритмы шифрования Skype весьма надежны (до сих пор пока никто не расшифровал их), и теоретически можно использовать Skype и без Tor. Конечно, она будет прекрасно работать и через Tor, но я сомневаюсь, что в этом есть смысл, поскольку после приобретения компании Skype компанией Microsoft поползли слухи о том, что прослушка Skype спецслужбами вполне возможна.

Правда это или нет, знают только спецслужбы, но на всякий случай ознакомьтесь со следующей ссылкой и сделайте соответствующие выводы: **http://dkws.net/archives/2017**. В любом случае никто не даст вам гарантий, что завтра в коде Skype не появится (если уже не появился) "черный ход" для спецслужб или еще кого-то.

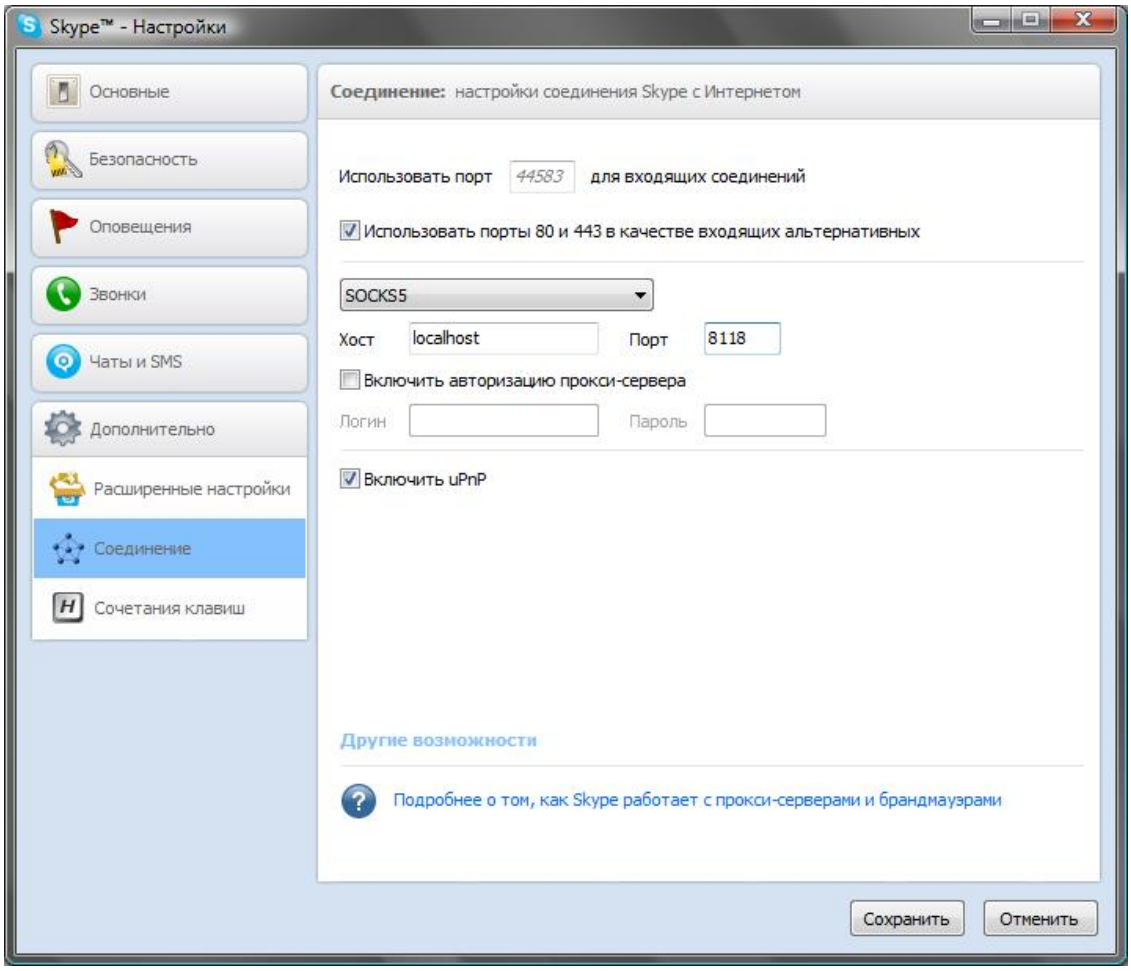

Рис. 2.14. *Настраиваем Skype на использование Tor*

2.4.5. Настройка FTP-клиента FileZilla

Чтобы не создавать лишнюю нагрузку на сеть Tor, рекомендуется не передавать через нее по FTP огромные файлы. Но все же Tor использовать для обмена файлов по протоколу FTP можно – ведь когда обновляешь свой сайт, в большинстве случаев размер каждого из передаваемых файлов составляет всего несколько килобайтов и редко доходит до мегабайта. Конечно, ISO-образы дистрибутивов операционных систем лучше через Tor не выкладывать (большие объемы трафика снижают производительность всей сети – потом не удивляйтесь, что Tor работает медленно). Впрочем, я не утверждаю, что через Tor нельзя передать, скажем, ISO-образ размером 650 Мбайт или даже 4 Гбайт. Технически такая возможность есть, но перед тем, как начать передачу, ознакомьтесь с *разд. 2.7*. А вот для передачи небольших файлов Tor вполне сгодится.

Для настройки FileZilla на использование Tor выполните команду меню **Редактирование | Настройка**. В открывшемся окне перейдите в раздел **Базовый прокси** (рис. 12.15), установите тип прокси **SOCKS5**, введите в поле **Хост прокси** имя прокси – *localhost* и порт *9050*. Не забудьте нажать **OK** для сохранения настроек.

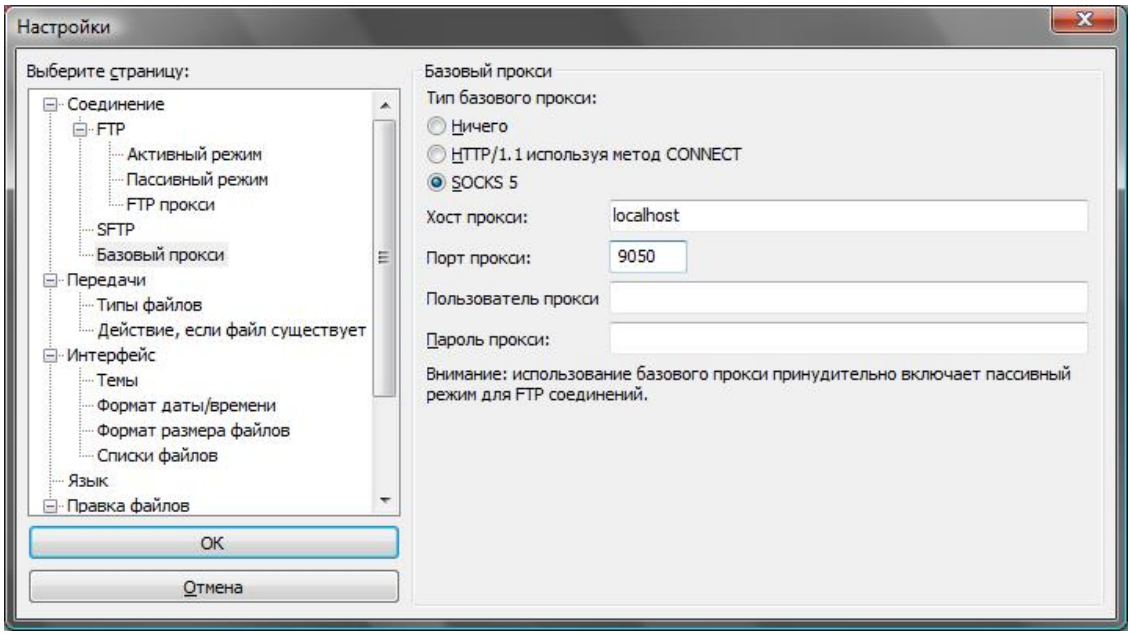

Рис. 12.15. *Настройка FTP-клиента FileZilla на использование Tor*

2.4.6. Настройка браузера Opera

Проприетарные браузеры (Opera относится к их числу) не рекомендуется использовать для обеспечения анонимности. Почему? Ответ на этот вопрос вы узнаете из *главы 12*. Но если сильно хочется "торифицировать" Opera, то все возможно.

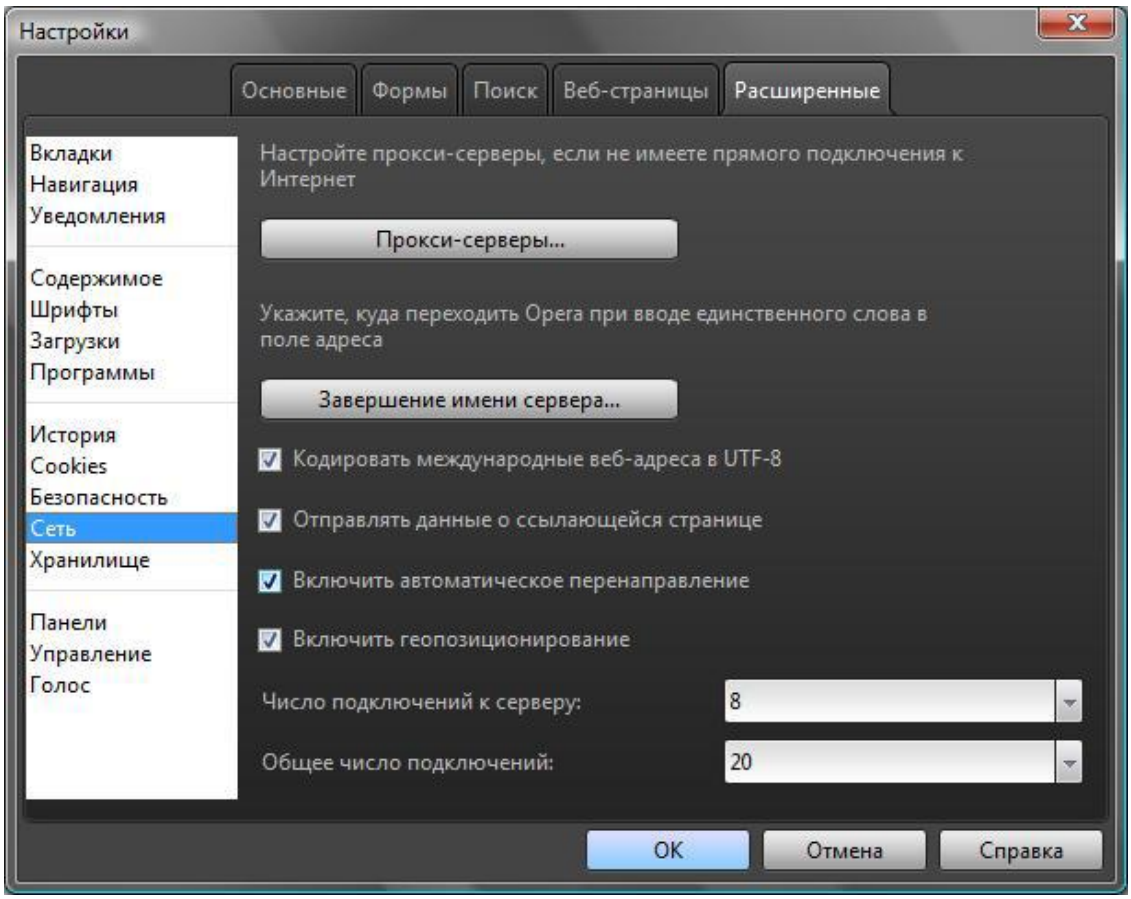

Рис. 2.16. *Сетевые параметры Opera*

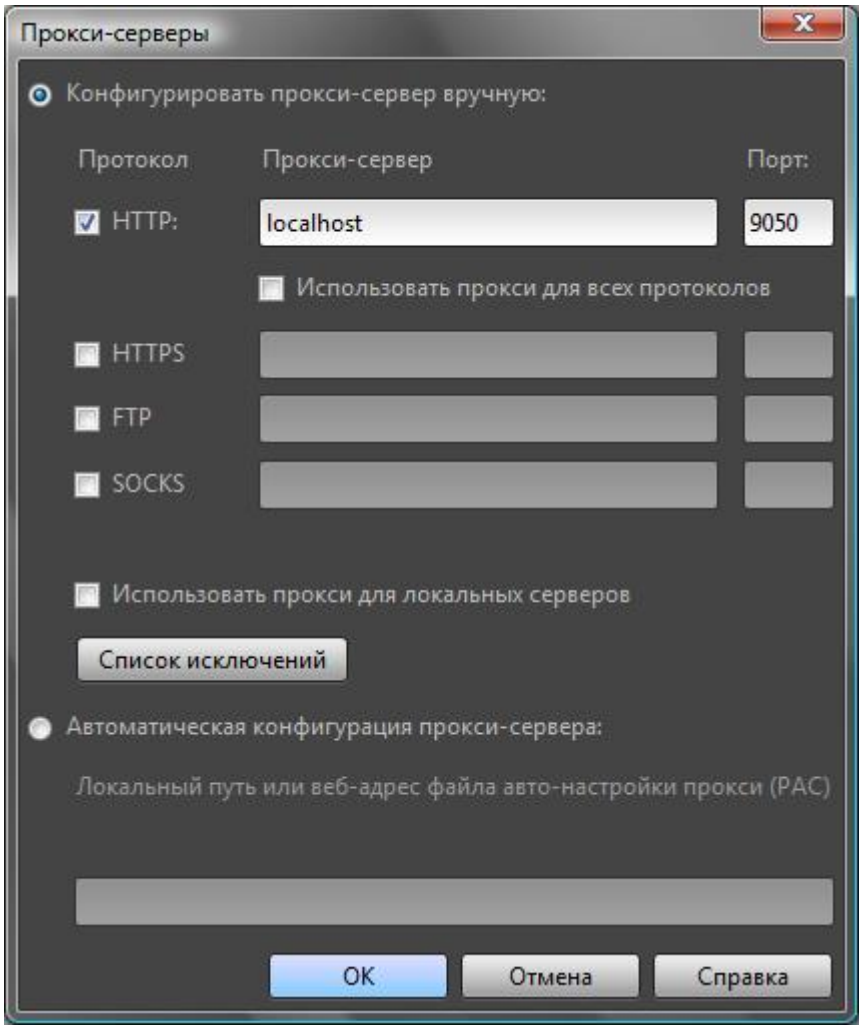

Рис. 2.17. *Параметры прокси-сервера: настройка на Tor*

Запустите браузер и выполните команду меню **Opera | Настройки | Общие настройки**. Перейдите на вкладку **Расширенные** в раздел **Сеть** (рис. 2.16). Нажмите кнопку **Прокси-серверы** и в открывшемся окне (рис. 2.17) укажите имя прокси-сервера localhost и его порт 9050.

После этого вы можете использовать Opera через Tor. Конечно, нужно убедиться, что Tor запущена (ранее было сказано, как это сделать).

2.5. Когда Tor бессильна. Дополнительные расширения для Firefox

Не нужно думать, что если вы установили Tor, то теперь полностью анонимны. Начинающие пользователи часто допускают ряд ошибок, которые приводят к их рассекречиванию. При использовании Tor нужно помнить следующее:

Tor защищает те программы, которые работают через нее. Если вы установили Tor Browser, но не настраивали на работу через Tor остальные сетевые программы (другие браузеры, ICQ, Skype и т. д.), то о никакой анонимности можно и не мечтать. Наиболее частая ошибка пользователей заключается в следующем. Пользователь устанавливает и запускает Tor Browser, а затем запускает другой браузер (а не тот, который запускается с помощью

Vidalia), например, Opera или Internet Explorer, и думает, что его трафик анонимизирован. Но это не так, поскольку эти браузеры не настроены на использование Tor;

разработчики Tor рекомендуют использовать браузер Firefox с плагином Torbutton. Этот плагин отслеживает статус сети Tor и отключает потенциально опасные плагины (Flash, ActiveX, Java и т. п.). В настройках Torbutton вы можете запретить отключение плагинов, но в этом случае Tor не гарантирует анонимность. Порой различные плагины могут идти в обход Tor и передавать приватную информацию. Лучше всего использовать два браузера, например Google Chrome для обычной работы в Интернете и Tor Browser (Firefox с Torbutton) – для анонимной работы;

следует быть очень осторожными с Cookies. Лучше всего отключить Cookies в настройках браузера, а еще лучше установить расширения NoScript и CookieSafe или Permit Cookies, которые еще больше повысят анонимность;

помните, что Tor шифрует трафик от вас до сети Tor и внутри самой сети, но между точкой выхода и конечным узлом трафик не шифруется. Если есть возможность, подключайтесь к конечному узлу по протоколу HTTPS. К сожалению, не все сайты поддерживают безопасные соединения;

не используйте BitTorrent через Tor. Если есть необходимость анонимно обращаться к трекерам, используйте TAILS (**http://tails.boum.org/**).

2.6. Ограничения и недостатки сети Tor

Tor – не безупречна. У всего есть свои недостатки, вот недостатки Tor:

некоторые интернет-ресурсы запрещают доступ из анонимной сети Tor;

скорость доступа к интернет-ресурсам через Tor существенно ниже, чем напрямую, но это плата за анонимность;

хотя Tor можно настроить для работы с любым TCP-соединением, ряд портов закрыты в выходной политике Tor, поэтому некоторые действия через Tor выполнить нельзя. Очень часто закрывается порт 25 – отправить почту не получится. Делается это специально, дабы компьютеры не использовались для рассылки спама;

некоторые сайты блокируют доступ пользователей из других стран. Если выходной IP-адрес будет принадлежать другой стране, зайти на сайт у вас не получится. Отчасти можно решить проблему, выбрав выходной узел в нужной стране, но это создает небольшие неудобства.

2.7. Этика использования сети Tor

При использовании Tor придерживайтесь следующих правил:

не используйте Tor для действий, не требующих анонимности: онлайн-игры, интернет-радио, онлайн-видео, загрузка больших файлов. Все эти действия создают ненужную и бесполезную нагрузку на сеть Tor, ей трудно справиться с такой нагрузкой;

не используйте Tor для нанесения вреда сайтам, рассылки спама и других вредоносных действий. Иначе у администраторов разных ресурсов появятся причины закрыть доступ из сети Tor, и она станет бесполезной. Этим вы повредите пользователям всего мира, которым действительно нужна анонимность.

Глава 3. Сеть I2P – альтернатива Tor

3.1. Что такое I2P?

В *главе 2* мы познакомились с распределенной сетью Tor, позволяющей зашифровать и анонимизировать трафик. Здесь будет рассмотрен другой проект анонимизации – I2P (Invisible Internet Project, проект "Невидимый Интернет"). I2P – это так называемая *оверлейная* сеть, то есть работающая поверх обычного Интернета. Получается, что I2P – как бы сеть над сетью.

Сеть I2P обеспечивает функционирование внутри себя многих сетевых служб: сайтов (технология eepsite), почты, систем мгновенного обмена сообщениями и даже торрент-трекеров (BitTorrent, EDonkey, Kad, Gnutella и др.). А для последних I2P – просто рай, до сих пор не понимаю, почему все торрент-трекеры не перекочевали еще в I2P. Скорее всего потому, что многие пользователи не знают об I2P и не понимают, как в ней работать. Вот сейчас этот пробел в ваших знаниях мы и восполним, а уж использовать I2P или нет – решайте сами.

3.1.1. Преимущества I2P

Итак, чем же I2P полезна обычным пользователям? Начнем с торрент-трекеров. Загружая фильм (программу, музыкальную композицию и т. п.) с торрент-трекера (не говоря уже о раздаче этого контента), вы нарушаете законодательство об авторских правах. А во время загрузки (раздачи) контента через торрент-трекер ваш IP-адрес виден всем. Теоретически при самом неблагоприятном для вас раскладе правоохранительные органы могут нанести вам очень неприятный визит.

Однако при работе в I2P такого не произойдет никогда, поскольку ваш IP-адрес будет зашифрован, а маршрутизация осуществляется по так называемым *туннелям*. Другими словами, доказать, что это именно вы скачали там-то и там-то фильм – практически невозможно. Конечно, нельзя утверждать, что невозможно вовсе. При особом желании доказать можно, но для этого придется потратить столько времени, средств и других ресурсов, что окажется проще снять другой фильм, чем доказывать, что вы скачали данный с трекера (а, сами понимаете, вы не один такой пользователь).

В сети I2P любой желающий может создать собственный сайт, причем абсолютно бесплатно, – не придется платить ни за регистрацию имени, ни за доменное имя вида **name.i2p**. А хостинг можно развернуть на своем компьютере, установив связку Apache + PHP + MySQL (если вы не понимаете, как это сделать, достаточно установить XAMPP[2] – благодаря этому продукту данная связка устанавливается очень легко). Сайты внутри I2P-сети скрытые – то есть, чтобы выяснить, на каком именно компьютере "лежит" тот или иной сайт, нужно опять-таки потратить массу ресурсов.

Скрытый сайт можно создать и в сети Tor, однако там вместо удобного имени вида **name.i2p** будет сгенерирован длиннющий хэш, который вам придется хранить в отдельном текстовом файле, – запомнить вы его не сможете.

Кроме скрытых сайтов и анонимных торрентов, в I2P работает анонимная почта, можно также организовать анонимное общение через популярные клиенты мгновенного обмена сообщениями и даже настроить Skype для работы через I2P. Мы уже отмечали ранее,

[2] XAMPP – кроссплатформенная сборка веб-сервера, содержащая Apache, MySQL, интерпретатор скриптов PHP, язык программирования Perl и большое количество дополнительных библиотек, позволяющих запустить полноценный веб-сервер.

что Skype использует проприетарные и очень сложные алгоритмы шифрования. Поддерживают они прослушку или нет – известно одним разработчикам Skype (в последнее время появляется все больше слухов, что прослушка разговоров в Skype возможна). Когда же вы отправляете Skype-трафик через I2P (или через Tor, как было показано в *главе 2*), прежде, чем добраться до разговора в Skype, желающим прослушать ваши разговоры придется вскрыть несколько слоев шифрования в I2P. Таким образом, использование I2P (или Tor) значительно усложняет задачу прослушки.

Еще два бонуса, предоставляемых сетью I2P обычным пользователям, заключаются в поддержке русского языка, а также кроссплатформенности – поскольку для создания программного обеспечения I2P использовался язык Java, то ПО для I2P можно запускать как в Windows, так и в Linux, Mac OS, Solaris и прочих операционных системах.

3.1.2. Недостатки

А теперь ложка дегтя – о недостатках I2P. Нет ничего идеального, и I2P – тоже не идеальна. Начнем с самой концепции I2P. Анонимизация и шифрование трафика происходит лишь внутри этой сети. Работая с I2P, вы можете обратиться только к I2P-ресурсам (к I2P-сайтам, почте, трекерам и т. д.). Если вы обращаетесь к ресурсу, не принадлежащему к I2P, защита не обеспечивается. С той же Tor все намного удобнее, поскольку вы можете обращаться к любым ресурсам Интернета, и при этом трафик будет анонимизирован и защищен.

Это и есть основной недостаток I2P. Но существуют еще два отрицательных момента, о которых вы также должны знать. Прежде всего, в I2P-сети очень мало русских ресурсов. Больше она популярна в Германии – немецких ресурсов и англоязычных сайтов в I2P очень много, а вот русскоязычных – единицы. Будет ли вам интересна I2P, зависит от владения английским и немецким языками и, разумеется, от информации, которую вы хотите найти в I2P.

Еще один недостаток – это существенные потоки трафика, проходящие через ваш компьютер. Если в Tor вы могли работать только в качестве клиента, то в сети I2P через ваш компьютер передается трафик других I2P-пользователей. Трафик зашифрован, тут особо беспокоиться не о чем, но если ваш интернет-тариф учитывает объем трафика, то I2P вам вряд ли подойдет, поскольку вы будете вынуждены платить и за свой трафик, и за трафик других пользователей, проходящий через ваш компьютер. Вы можете зайти в I2P, часик посидеть почитать какие-либо сайты, а за это время через ваш компьютер будет пропущено несколько гигабайтов трафика.

3.1.3. Шифрование информации в I2P

Весь трафик в сети I2P, в отличие от Tor, шифруется от отправителя к получателю. В общей сложности используются четыре уровня шифрования (сквозное, "чесночное", туннельное и шифрование транспортного уровня). Перед шифрованием I2P добавляет в отправляемый пакет случайное количество произвольных байтов, чтобы еще больше затруднить попытки анализа содержимого пакета и его блокировки.

В качестве адресов сети применяются криптографические идентификаторы (открытые криптографические ключи), не имеющие никакой логической связи с реальным компьютером. В сети I2P нигде не используются IP-адреса, поэтому определить настоящий IP-адрес узла, и, следовательно, установить его местонахождение, невозможно.

Каждое сетевое приложение, работающее через I2P, строит для себя анонимные зашифрованные туннели – обычно одностороннего типа, когда исходящий трафик идет через одни туннели, а входящий – через другие. Выяснить, какое приложение создало тот или иной

туннель, – тоже невозможно (точнее, очень сложно, поэтому будем считать, что таки практически невозможно).

Все пакеты, передаваемые по сети, могут расходиться по разным туннелям, что делает бессмысленной попытку перехвата (прослушки) данных. И в самом деле – поскольку данные передаются по разным туннелям, проанализировать поток данных даже с помощью снифера[3] не получится. Каждые 10 минут происходит смена уже созданных туннелей на новые с новыми цифровыми подписями и ключами шифрования (у каждого туннеля свой ключ шифрования и своя цифровая подпись).

Вам не нужно беспокоиться, чтобы прикладные программы обеспечивали шифрование трафика. Если существует недоверие к программам, имеющим закрытый исходный код (взять тот же Skype), можно или попытаться заставить эти программы работать через I2P, или поискать альтернативные программы с открытым кодом. Так, вместо Skype можно использовать Ekiga – простую программу для IP-телефонии. Правда, она не умеет шифровать данные (они передаются в открытом виде), но о шифровании позаботится I2P. Конечно, ваш собеседник тоже должен использовать I2P, иначе толку от всех этих мероприятий (настройки Skype для работы через I2P или установки и использования Ekiga) не будет.

Шифрование и дешифрование пакетов осуществляются соответственно на стороне отправителя (шифрование) и на стороне получателя (расшифровка). В отличие от Tor, никто из промежуточных участников обмена не может перехватить зашифрованные данные, и никто из участников не знает, кто на самом деле является отправителем, а кто получателем, поскольку передающий пакеты узел может быть как отправителем, так и промежуточным узлом.

Промежуточный узел не может узнать конечные точки (кто отправил пакеты, и куда они следуют), так же он не может определить, что случилось с только что переданным следующему узлу пакетом: принял его себе (то есть следующий узел является получателем) или передал следующему узлу.

В I2P используются следующие методы (алгоритмы) шифрования:

AES (256 битов);
схема Эль-Гамаля (2048 битов);
алгоритм Диффи – Хеллмана (2048 битов);
DSA (1024 бита);
HMAC (256 битов);
SHA256 (256 битов).

3.1.4. Как работать с I2P?

Все очень и очень просто. Принцип работы I2P с точки зрения неискушенного пользователя такой же, как и в случае с Tor. Вы устанавливаете I2P на свой компьютер, изменяете, если сочтете нужным, настройки по умолчанию (хотя в 99 % случаев этого делать не придется, поскольку I2P – это программа, работающая "из коробки", то есть не требующая настройки) и настраиваете свои сетевые программы – в их настройках следует указать использование прокси-сервера с IP-адресом 127.0.0.1 (порт 4444). Аналогичные действия мы проделывали при настройке сетевых программ на использование прокси-сервера Tor (только номер порта был другим).

После этого вы можете заходить на I2P-сайты сети, например, на **http://i2p2.i2p** – это официальный сайт проекта I2P.

---

[3] Сниффер – анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа либо только анализа сетевого трафика.

По трафику, отправляемому вашим компьютером в Интернет, очень сложно понять, что от вас исходит – то ли это ваш трафик, то ли это транзитный трафик других клиентов I2P-сети. Другими словами, доказать причастность кого-либо к конкретной сетевой активности весьма тяжело.

3.1.5. Tor или I2P?

В *главе 2* мы познакомились с распределенной сетью Tor. Здесь рассматривается подобный проект – I2P. Так что же лучше: Tor или I2P? Такой вопрос рано или поздно задаст любой пользователь, поработавший хотя бы раз с Tor или I2P. Спешу вас разочаровать, сравнивать I2P и Tor нельзя – это все равно, что сравнивать апельсины с яблоками. Кому-то нравятся апельсины, а кому-то – яблоки. Из яблок не получится апельсиновый сок, и наоборот. Каждая из сетей призвана решать свои задачи, поэтому выбирать между I2P и Tor нужно, исходя из поставленных задач.

Сеть I2P – это изолированная, закрытая сеть без выхода во "внешний" Интернет. И пусть в I2P имеется "прокси", позволяющий выйти в Интернет, но это особо не влияет на функционирование сети I2P в целом. I2P не предназначена для обычного серфинга в открытом Интернете. I2P идеальна для анонимного и безопасного обмена файлами, анонимного общения, анонимного хостинга сайтов внутри I2P-сети.

Концепция Tor несколько иная. Изначально Tor разрабатывалась для работы с открытым Интернетом. С ее помощью, как было показано в *главе 2*, можно легко посещать заблокированные сайты, анонимно посещать обычные сайты и т. п.

Давайте подытожим:

вам нужно *анонимное общение* (например, по Skype или ICQ)? Тогда лучше воспользоваться I2P. При этом человек, с которым вы собираетесь общаться, тоже должен использовать I2P;

если же вам нужно *анонимно посетить* тот или иной сайт или же посетить сайт, заблокированный "злым" администратором, тогда следует воспользоваться Tor. Использование Tor можно сравнить с маскировкой, а вот I2P является своеобразным подпольем мировой Сети.

Что же касается преимуществ и недостатков, то они есть у каждой сети, но перечислять мы их не будем, поскольку эти недостатки незначительны, и при использовании той или иной сети по назначению вы о них даже и не вспомните.

3.2. Установка ПО I2P

3.2.1. Установка Java-машины

Программное обеспечение для работы с I2P написано на Java, а поэтому, если на вашем компьютере не установлена виртуальная машина Java, самое время ее установить.

Конец ознакомительного фрагмента.