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 Колисниченко

Самоучитель

Анонимность и безопасность в ИНТЕРНЕТЕ

от «чайника» к пользователю

Санкт-Петербург

«БХВ-Петербург»

2012

УДК 681.3.06
ББК 32.973.26-018.2
К60

Колисниченко Д. Н.

К60 Анонимность и безопасность в Интернете. От «чайника» к пользователю. — СПб.: БХВ-Петербург, 2012. — 240 с.: ил. — (Самоучитель)

ISBN 978-5-9775-0363-1

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

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Компьютерная верстка	*Натальи Караваевой*
Корректор	*Наталия Першакова*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Марины Дамбиевой*
Зав. производством	*Николай Тверских*

Подписано в печать 26.12.11.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 19,35.
Тираж 1500 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12.

ISBN 978-5-9775-0363-1

Оглавление

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.

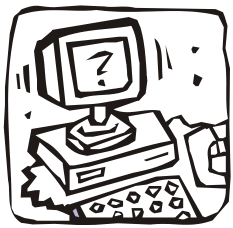
Не обойдите вниманием и *приложения*! В *первом* вы познакомитесь с программой AVZ и еще несколькими полезными утилитами, а во *втором* будет рассмотрена программа Traffic Inspector, которая весьма пригодится дома, поскольку позволяет блокировать доступ к Интернету по времени суток и по адресу, — ваши 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/

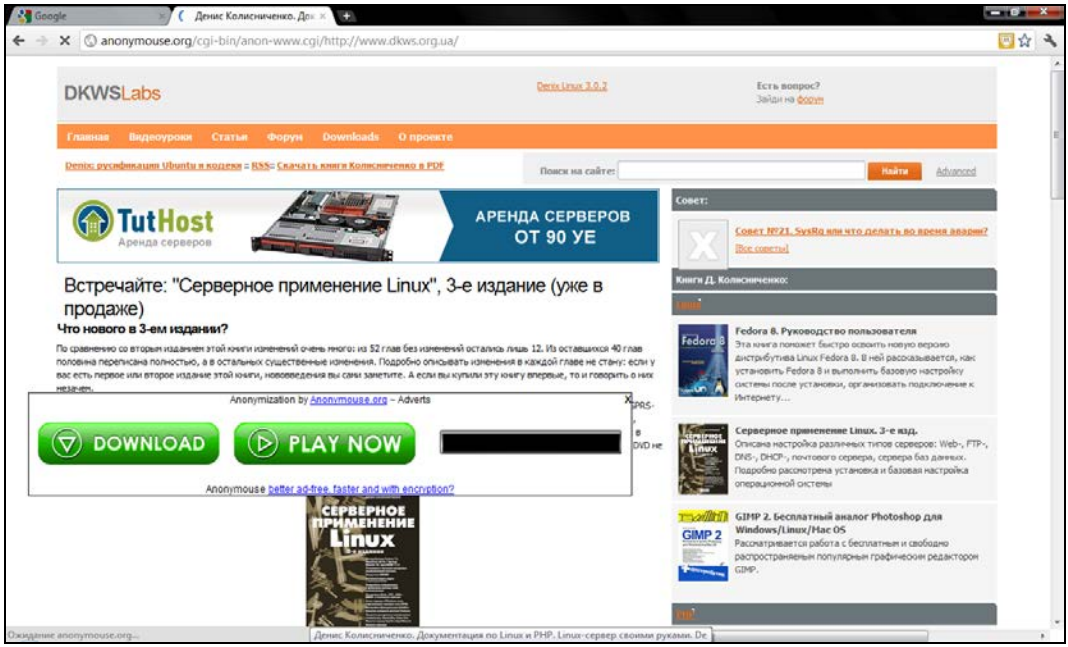


Рис. 1.1. Просмотр сайта через **anonymouse.org**: анонимайзер добавил большой рекламный баннер

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 администратор 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 об 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)

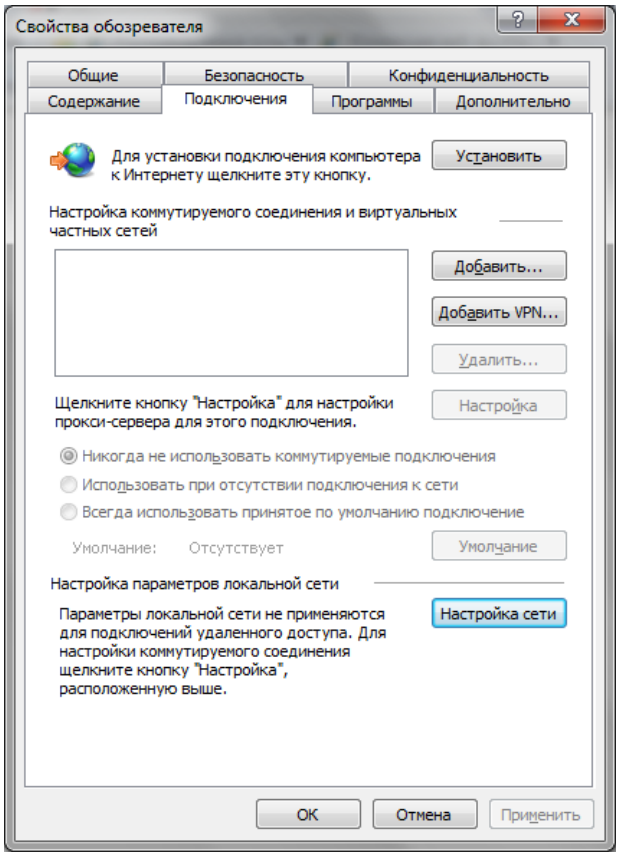


Рис. 1.3. Свойства обозревателя: вкладка **Подключения**

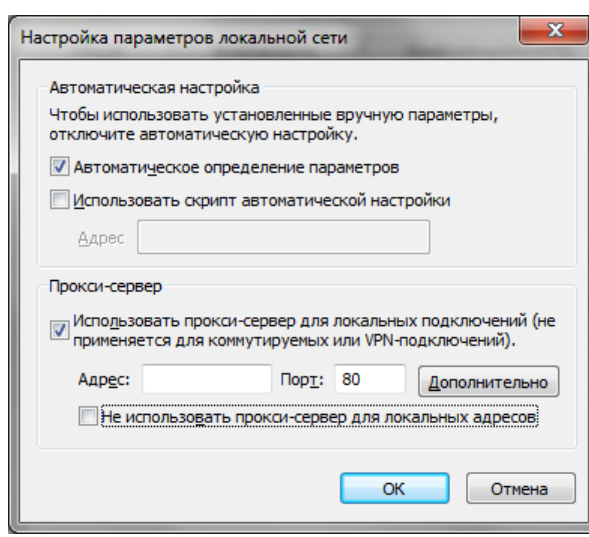


Рис. 1.4. Окно настройки параметров локальной сети

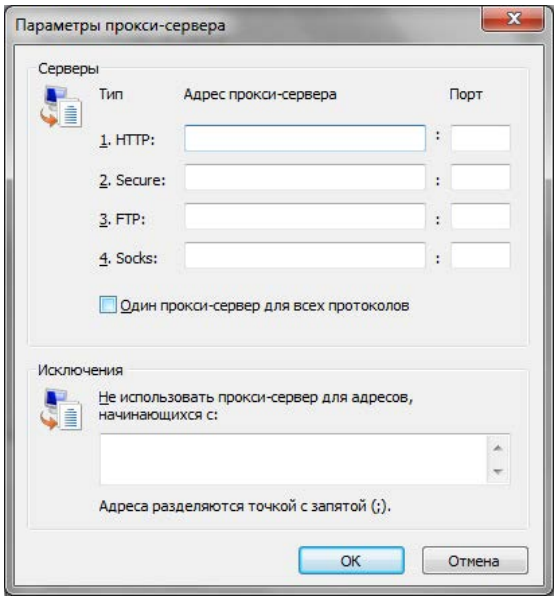


Рис. 1.5. Окно параметров прокси-сервера

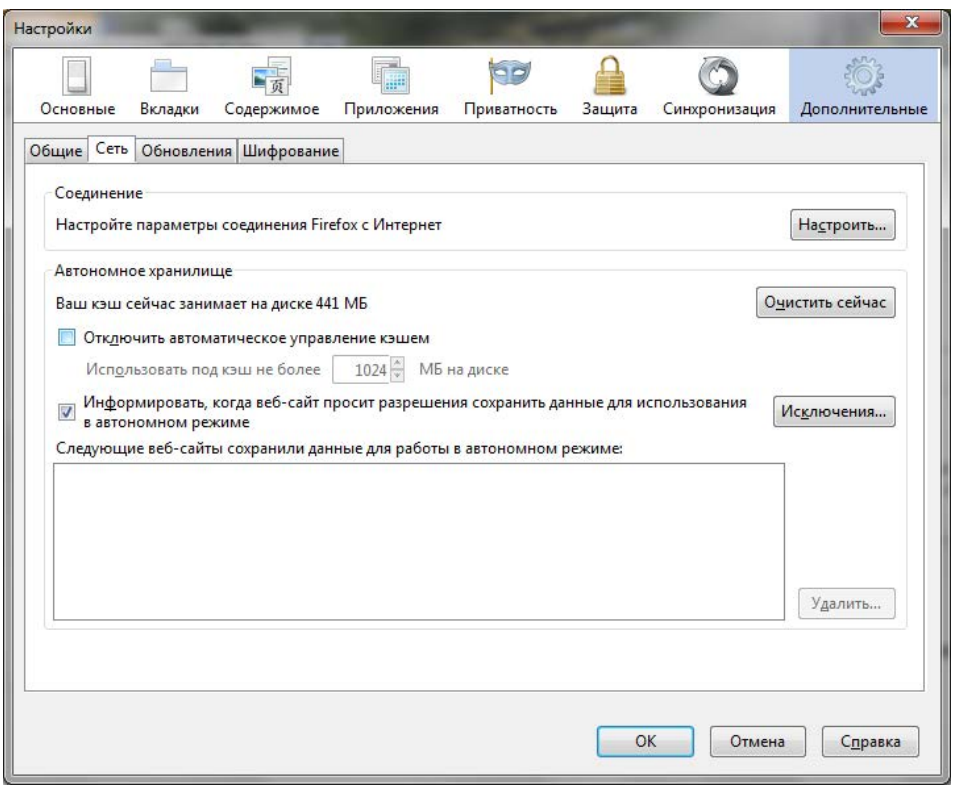


Рис. 1.6. Окно настроек Firefox

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 прокси-сервера 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).

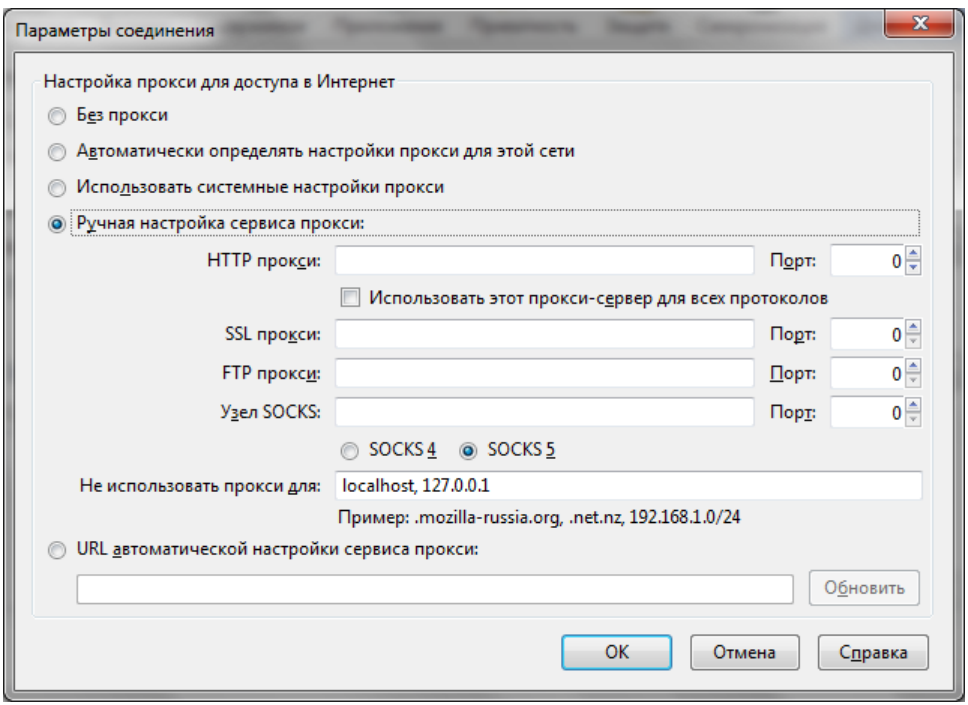


Рис. 1.7. Параметры соединения

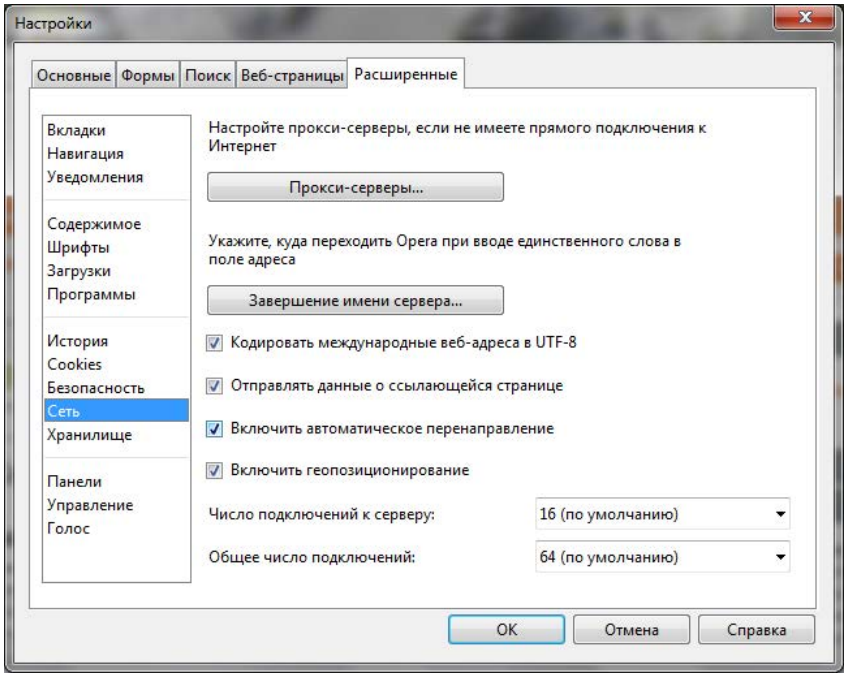


Рис. 1.8. Настройки браузера Opera

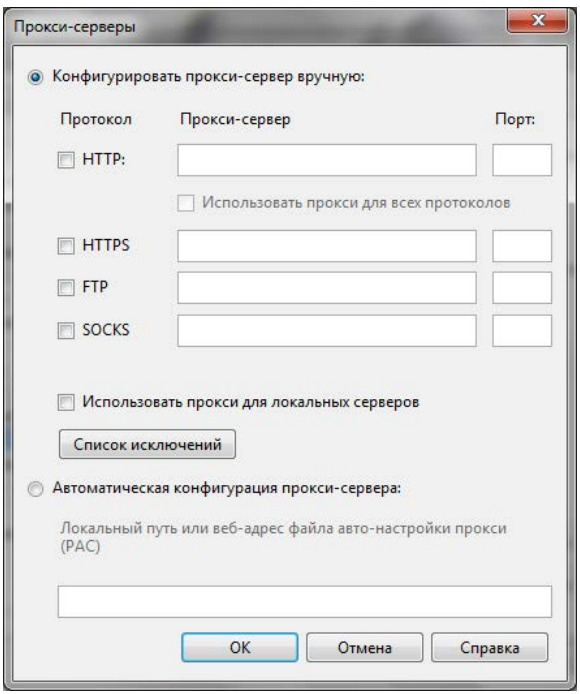


Рис. 1.9. Параметры прокси-сервера

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.

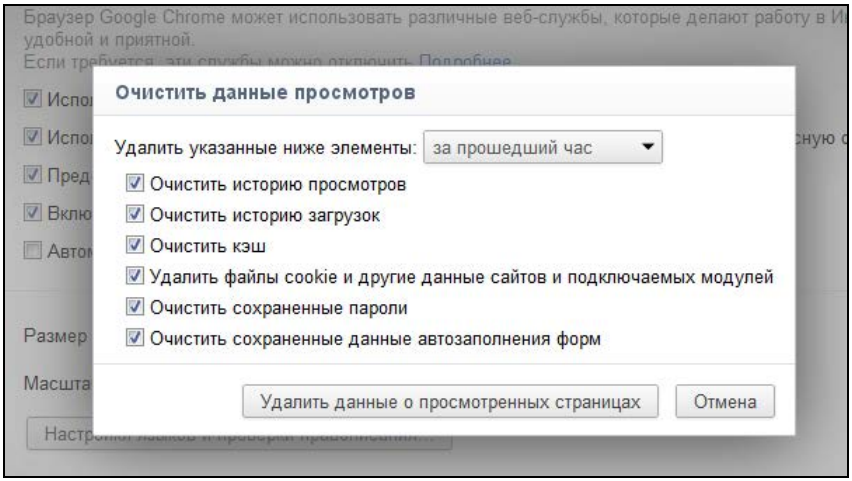


Рис. 1.10. Заметаем следы в Google Chrome

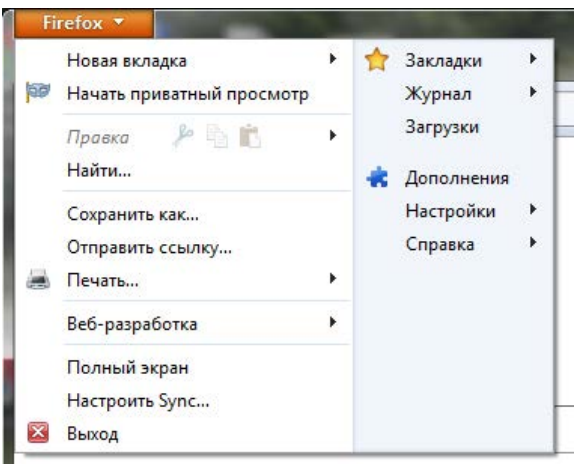


Рис. 1.11. Режим приватного просмотра в Firefox

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**.

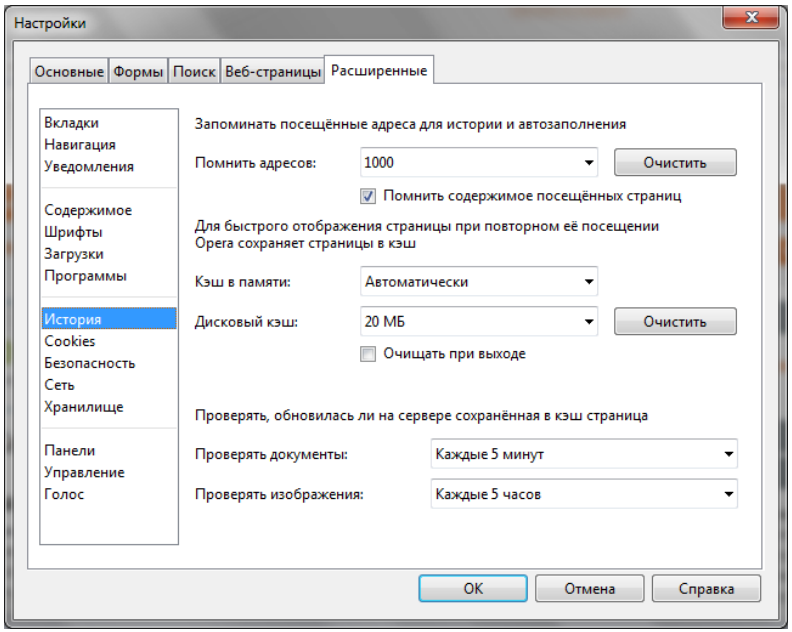


Рис. 1.12. Заметаем следы в Opera

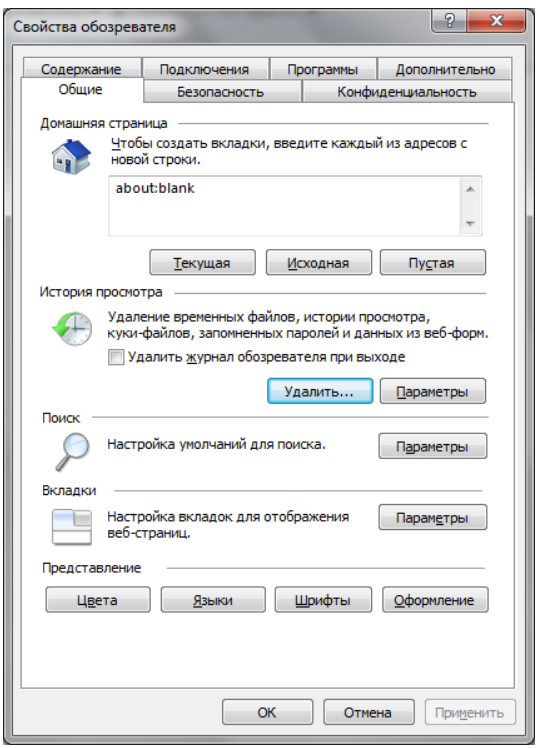


Рис. 1.13. Свойства обозревателя Internet Explorer

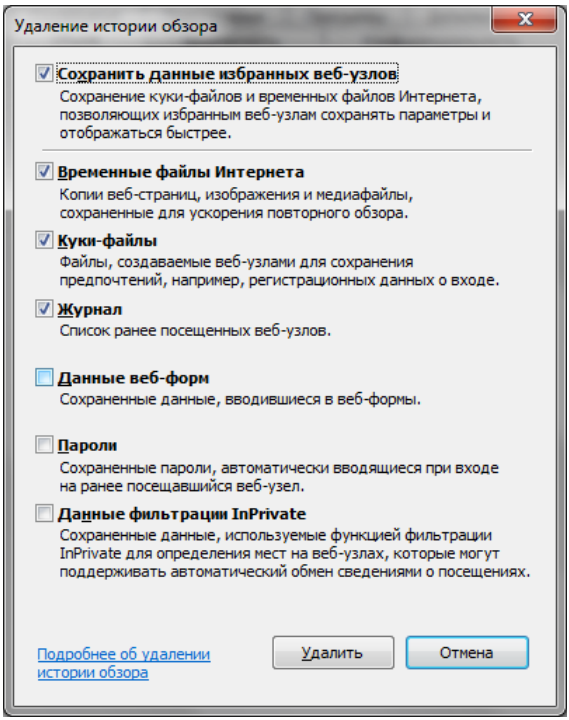


Рис. 1.14. Удаляем историю обзора

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 кон-

тролирующих 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):

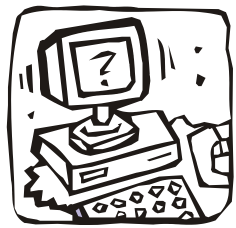
> 3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:
>
> 1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
>
> 2) использовать информацию, в том числе распространять ее, по своему усмотрению;
>
> 3) передавать информацию другим 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.