

Михаил Райтман

**КАК** **н а й т и**  
**и** **СКАЧАТЬ**  
**в Интернете**  
**любые файлы**

2-е издание

Санкт-Петербург

«БХВ-Петербург»

2011

УДК 681.3.06  
ББК 32.973.26-018.2  
P18

**Райтман М. А.**

P18 Как найти и скачать в Интернете любые файлы. — 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2011. — 336 с.: ил.

ISBN 978-5-9775-0654-0

Описан ряд эффективных, в том числе и неочевидных, приемов поиска информации и нужных файлов.

Даны советы и рекомендации по бесплатному скачиванию и докачке файлов с файлообменных серверов, торрент-трекеров и узлов DC++. Книга знакомит с электронными библиотеками, FTP- и HTTP-архивами, "варезными" сайтами и форумами. Показано, как оформлять свои раздачи на трекерах и осуществлять управление рейтингом, скачивать объемные файлы, экономить трафик и деньги при медленном подключении к Интернету, бесплатно скачивать музыку и видео. Особое внимание уделено обеспечению анонимности и безопасности в Интернете. Приведены интересные факты о мнимом "одиночестве" в сети, даны приемы обхода некоторых ограничений и запретов системных администраторов. Словарь в конце книги содержит термины из компьютерного сленга. Во втором издании добавлена глава об андеграундном компьютерном искусстве, а также разделы о деятельности различных хакерских групп, бесплатных играх, телефонных звонках и SMS, анонимных прокси-серверах.

*Для широкого круга читателей*

УДК 681.3.06  
ББК 32.973.26-018.2

**Группа подготовки издания:**

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Григорий Добин</i>
Редактор	<i>Анна Кузьмина</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Корректор	<i>Зинаида Дмитриева</i>
Дизайн обложки	<i>Елены Беляевой</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 29.10.10.  
Формат 70×100<sup>1/16</sup>. Печать офсетная. Усл. печ. л. 27,09.  
Тираж 3000 экз. Заказ №  
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию  
№ 77.99.60.953.Д.005770.05.09 от 26.05.2009 г. выдано Федеральной службой  
по надзору в сфере защиты прав потребителей и благополучия человека.

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

ISBN 978-5-9775-0654-0

© Райтман М. А., 2010  
© Оформление, издательство "БХВ-Петербург", 2010

# Оглавление

<b>Глава 1. Подготовка к погружению во Всемирную паутину .....</b>	<b>7</b>
Что нужно, чтобы начинать "охоту" за файлами .....	7
Обеспечение анонимности в Интернете .....	10
Мания преследования: миф и реальность .....	16
<b>Глава 2. Как посетить запрещенный для доступа сайт .....</b>	<b>20</b>
Получение доступа посредством анонимайзера .....	20
Настройка браузера для доступа к веб-сайтам через прокси .....	24
<b>Глава 3. Способы обхода ограничений администратора сети .....</b>	<b>27</b>
Смена расширения: как обойти ограничения администратора в офисе .....	28
Как установить и запустить "Аську", если администратор заблокировал эту возможность..	33
Как получить доступ к социальным сетям, если это запрещено в вашем офисе .....	35
<b>Глава 4. Секреты поиска файлов в Интернете .....</b>	<b>38</b>
Секреты запросов Google: невозможные возможности поиска .....	40
Тайны других поисковых систем .....	48
Поиск файлов на FTP-серверах .....	50
<b>Глава 5. Как правильно скачивать файлы с веб-страниц и FTP-серверов .....</b>	<b>56</b>
Менеджеры закачек на службе у пользователя .....	57
Загрузка с помощью менеджера закачек Download Master .....	57
Загрузка файлов с FTP-серверов .....	73
Загрузка файлов средствами FTP Explorer .....	73
Загрузка файлов средствами FileZilla .....	75
<b>Глава 6. Загружаем веб-сайты целиком .....</b>	<b>79</b>
Создание нового проекта загрузки в программе Offline Explorer Pro .....	79
Настройка программы Offline Explorer Pro .....	83
Загрузка веб-сайта на компьютер .....	87
Особенности загрузки некоторых сайтов .....	91
<b>Глава 7. Обмен файлами или загружаем по частям .....</b>	<b>93</b>
Сервис Depositfiles.com .....	98
Сервис Dump.ru .....	102
Сервис Easy-share.com .....	103

Сервис Filefactory.com .....	104
Сервис Files.mail.ru .....	106
Сервис Ifolder.ru .....	107
Сервис Ipicture.ru .....	109
Сервис Letitbit.net.....	110
Сервис Megaupload.com .....	113
Сервис Openfile.ru .....	114
Сервис Rapidshare.com .....	115
Сервис Яндекс.Диск .....	118
Другие сервисы .....	119
"Зеркальные" сервисы .....	120
Работа с инструментом Flash Release .....	120

## **Глава 8. Обходим ограничения файлообменных хостингов ..... 125**

Поиск файла на другом хостинге .....	125
Параллельная загрузка "зеркал" с разных сервисов.....	126
Получение прямых ссылок на файлы хостингов.....	127
Смена IP-адреса компьютера .....	128
Использование сети Tor .....	129
Уничтожение cookies: забудь, кто я .....	130
Идеи обхода ограничений .....	133
Как не скачать все, что вы хотите .....	133

## **Глава 9. Скачиваем фотографии, видео- и аудиоролики с YouTube, "В Контакте" и других сервисов ..... 136**

Поиск среди временных файлов .....	136
Сохранение файлов средствами специальных сервисов и скриптов.....	138

## **Глава 10. Город грехов: доступно все, но не все дозволено ..... 144**

"Нелегальные" сайты.....	146
Форумы, где ссылки лежат .....	150
FTP- и HTTP-архивы, электронные библиотеки.....	151

## **Глава 11. Пиринговые сети, торренты, трекеры и раздачи на службе**

<b>у пользователя.....</b>	<b>155</b>
Как работает пиринговая сеть.....	155
Современные пиринговые сети .....	159
BitTorrent .....	159
EDonkey2000 .....	160
Сеть Kad Network или Kademila.....	160
Программа-клиент µTorrent .....	161
Окно программы µTorrent .....	163
Настройка программы µTorrent .....	166
Закачка файлов с помощью программы µTorrent .....	169
Создание собственной раздачи .....	172
Работа с трекером на примере RuTracker.org .....	177
Создание своей раздачи на трекере .....	182
Маленькие хитрости для повышения рейтинга .....	183
Хитрости результативного поиска по трекерам .....	185
Популярные трекеры и каталоги .....	187

<b>Глава 12. Популярный способ закачки файлов по "магнитным" ссылкам программой DC++ .....</b>	<b>189</b>
Принцип работы программы-клиента DC++ .....	190
Структура сети Direct Connect .....	191
Предварительная настройка программы DC++ .....	192
Знакомство с интерфейсом программы DC++ .....	199
Поиск и закачка файлов.....	200
Открытие и загрузка файлов по magnet-ссылкам .....	204
Как создать magnet-ссылку.....	206
Загрузка файла по magnet-ссылке .....	207
Каталоги и системы поиска magnet-ссылок в Интернете .....	209
<b>Глава 13. Как качать терабайты тем, у кого медленный или дорогой Интернет .....</b>	<b>210</b>
Заказы и получение файлов на электронный почтовый ящик .....	211
Заказ и получение файлов почтой .....	213
Сервисы сжатия трафика.....	215
Настройка программы Toonel.....	217
Настройка браузера.....	219
<b>Глава 14. Вarez, крэки, кейгены и прочее: что важно об этом знать .....</b>	<b>222</b>
Инструменты обхода защиты программ от нелегального копирования .....	222
Сцена: андеграунд Интернета .....	225
Что такое Promo, LP, OST, Score и другие термины релизов .....	230
<b>Глава 15. Демосцена .....</b>	<b>233</b>
Искусство ASCII-Art.....	233
Трекерная музыка .....	236
Интро и демо .....	238
<b>Глава 16. Обеспечение собственной безопасности .....</b>	<b>241</b>
Фишинг и другие методы мошенничества .....	241
Вредоносные программы и борьба с ними .....	246
Антивирусный пакет AVG Free .....	247
Знакомство с программой .....	248
Антивирусный монитор.....	250
Сканирование всего компьютера.....	250
Использование LinkScanner.....	252
Онлайн-проверка файлов на вирусы .....	254
<b>Глава 17. Скрываем свое поведение в Интернете с помощью TOR.....</b>	<b>256</b>
Установка Tor.....	258
Настройка программного обеспечения .....	261
Настройка браузера Internet Explorer .....	261
Настройка браузера Firefox .....	263
Настройка мессенджера на примере ICQ.....	264
Настройка почтовой программы на примере Thunderbird.....	265
Создание узла Tor .....	266

<b>Глава 18. Все бесплатно .....</b>	<b>268</b>
Бесплатные операционные системы.....	269
Современные версии операционной системы Linux.....	269
SUSE Linux .....	270
Mandriva Linux.....	270
Ubuntu Linux .....	271
Бесплатное программное обеспечение .....	273
Офисные приложения.....	273
Текстовый редактор и редактор веб-страниц OpenOffice.org Writer .....	273
Редактор электронных таблиц OpenOffice.org Calc .....	274
Приложение для создания презентаций OpenOffice.org Impress.....	274
Векторный редактор OpenOffice.org Draw.....	275
Веб-обозреватели .....	277
Mozilla Firefox .....	277
Opera.....	277
Google Chrome.....	277
Графические редакторы .....	277
Создание и запись CD- и DVD-дисков.....	279
Электронная почта.....	280
Воспроизведение мультимедийных файлов .....	281
Просмотр графических файлов.....	283
Антивирусная защита .....	284
Бесплатные онлайн-приложения .....	286
Бесплатно смотрим телевизор и слушаем радио онлайн.....	289
Бесплатно играем в игры.....	293
Как бесплатно или очень дешево звонить и отправлять SMS/MMS через Интернет .....	296
Как сэкономить на покупке платных программ .....	298
Платные программы — совершенно бесплатно!.....	300
 <b>Приложение 1. Таблица бесплатных и недорогих аналогов платных программ.....</b>	 <b>301</b>
 <b>Приложение 2. Краткий глоссарий интернет-терминов пользователя .....</b>	 <b>304</b>

# ГЛАВА 1



## Подготовка к погружению во Всемирную паутину

Нет, я понимаю, что такое виртуальная реальность; но может мне кто-нибудь объяснить, что такое реальность?

Неизвестный автор

Итак, вы решили штурмовать Интернет с целью найти определенный файл. Это может быть что угодно: свежая композиция звезды в MP3- или LOSSLESS-формате FLAC, а может быть ремикс на эту песню неизвестного домашнего диджея. Или может быть дистрибутив программы определенной версии (что часто делают, не имея ключей на самую последнюю версию), образ диска с игрой. Или же видео-файл — фрагмент телевизионного шоу либо прикольный рекламный ролик. Ну и, разумеется, фотографии и графические абстракции в различных форматах, а также документы. Найти можно если и не абсолютно все, то очень и очень многое. Важно уметь искать. Искать эффективно. Так, чтобы результаты оправдывали запросы. Но прежде чем вплотную приступить к погружению в глобальную сеть, весьма важно обезопасить свой компьютер от возможного заражения. Тут Интернет сравним с голливудскими фантастическими фильмами, когда вверху небоскребов — офисы и царьки в желтых очках, а во мраке и грязи улиц внизу — основная масса: тут можно купить и превратить в реальность любое желание. Поэтому я рекомендую вам в первую очередь обратиться к *главе 16*, чтобы узнать, как защитить свой компьютер, а уже потом вернуться сюда. Но так как, я знаю, вы махнете на безопасность рукой и не последуете моему совету, кратенько и доходчиво объясню все в следующем разделе.

### Что нужно, чтобы начинать "охоту" за файлами

Первое, что вам нужно иметь, помимо компьютера с установленной операционной системой Windows 7 и доступа в Интернет (необязательно быстрого — далее в книге узнаете, почему), — это установленный браузер (Internet Explorer 8, Mozilla Firefox, Google Chrome или любой другой по душе) и всевозможные обновления

безопасности для системы. Операционную систему Windows 7 я рекомендую потому, что она намного надежнее Windows XP и не в пример быстрее Windows Vista. Подробнее про достижение максимальной производительности на компьютере с установленной операционной системой Windows 7 вы сможете прочитать в моей книге "Установка и настройка Windows 7 для максимальной производительности"<sup>1</sup>. Переходить на новую версию операционной системы рекомендовано еще потому, что поддержка предыдущих версий Windows в определенный момент прекращается (например, бесплатная поддержка Windows XP прекратилась в апреле 2009 года), после которого новые обнаруженные уязвимости остаются уже без внимания, и ваш компьютер с течением времени становится все менее защищенным.

### **ПРЕКРАЩЕНИЕ ПОДДЕРЖКИ WINDOWS XP**

Согласно опубликованному пресс-релизу Microsoft, корпорацией принято решение о прекращении поддержки операционной системы Windows XP всех модификаций из-за того, что еще в начале 2001 года была выявлена серьезнейшая проблема безопасности в исходном коде ядра операционной системы Windows XP, которая, как выяснилось в ходе внутреннего расследования, присутствовала еще со времен Windows 3.1. Корпорацией настоятельно рекомендуется всем пользователям Windows XP и более ранних версий Windows использовать операционные системы Windows Vista или Windows 7, основанные на исходном коде Windows Server 2003, в котором отсутствует вышеописанная "дыра".

Чтобы по максимуму залатать вероятные уязвимости, установите по возможности все доступные через Центр обновления пакеты обновлений безопасности. Пакеты Service Pack и отдельные файлы обновлений позволяют решать проблемы безопасности, обнаруженные после выхода финальной версии операционной системы. Если же скорость или цена подключения к Интернету не позволяют этого сделать, можно попробовать отправить сообщение в корпорацию Microsoft с просьбой выслать свежий пакет обновлений.

Браузер Internet Explorer желателен версии 8, впрочем, если вы работаете в среде Windows 7 — он уже у вас предустановлен. Также вы можете использовать любой другой браузер — Opera, Safari, Chrome, Firefox. Выбирайте любой! От сторонних производителей в первую очередь вам понадобится антивирусное программное обеспечение. Скорее всего, вы уже пользуетесь каким-либо антивирусным сканером (Defender не в счет). Лучше, если это Антивирус Касперского или AVG Anti-Virus с антивирусными базами в актуальном состоянии. Программа AVG Anti-Virus Free бесплатна, имеет русский интерфейс и удобную встроенную функцию Link Scanner, автоматически проверяющую на наличие вредоносных объектов сайты по ссылкам, найденным в поисковой системе. Если обе перечисленные программы заставляют вас "воротить нос", воспользуйтесь решением Microsoft Security Essentials, которое обеспечивает защиту домашнего компьютера в реальном времени от вирусов, программ-шпионов и других вредоносных программ.

А также вам потребуется специализированное программное обеспечение.

---

<sup>1</sup> Райтман М. Установка и настройка Windows 7 для максимальной производительности (+ DVD-ROM). — СПб.: БХВ-Петербург, 2010.



### ПРИМЕЧАНИЕ

При медленном подключении к Интернету, доступ к антивирусным базам программы Антивирус Касперского можно получить тут: <ftp://ftp.kaspersky.com/>. Можете попросить друга с быстрым доступом к Интернету загрузить их для вас, а вы, в свою очередь, обновите базы уже в автономном режиме (если программа предполагает такую возможность).

Итак, вот список всего того, что вам понадобится.

- ◆ **Операционная система Windows 7.** Этот продукт действительно достоин того, чтобы за него заплатили деньги. Поэтому рекомендую его купить. К сожалению, загрузить дистрибутив уже нельзя, как было с RC-версиями<sup>1</sup>. На веб-сайте по адресу [windows.microsoft.com/ru-RU/windows7/products/features](http://windows.microsoft.com/ru-RU/windows7/products/features) вы можете узнать, что нового в версии 7 операционной системы ждет вас.
- ◆ **Браузер.** Вполне можно, не заморачиваясь, пользоваться встроенным в операционную систему Windows 7 браузером Internet Explorer 8. Загрузить дистрибутив можно с веб-сайта [www.microsoft.com/rus/windows/internet-explorer/](http://www.microsoft.com/rus/windows/internet-explorer/). Отличная бесплатная альтернатива — браузер Mozilla Firefox, доступный по адресу [www.mozilla-europe.org/ru/firefox/](http://www.mozilla-europe.org/ru/firefox/).
- ◆ **Tor.** Тор — это клиент сети виртуальных туннелей, который позволит вам повысить уровень анонимности и безопасности в Интернете. Подробнее о программе вы узнаете в *главе 17*. Загрузить приложение можно по адресу [www.torproject.org/easy-download.html.ru](http://www.torproject.org/easy-download.html.ru) (вам нужен установочный файл пакета для Windows).
- ◆ **Антивирусное приложение.** Тут сложно что-то рекомендовать, т. к. каждый пользователь испытывает симпатии к определенному антивирусу. Из платных могу посоветовать Антивирус Касперского 2011, Kaspersky Internet Security 2011 или Kaspersky CRYSTAL (ранние версии могут вызывать сбои в работе Windows 7), а из бесплатных вполне ничего AVG Anti-Virus Free. Программа Norton Antivirus имеет особенность сильно снижать производительность компьютера в момент автоматической проверки (которую весьма сложно настроить под себя), а ESET NOD32 слишком тихо сидит в области уведомлений, ничем не выдавая своего присутствия. Фанаты также могут использовать Dr.Web и другие антивирусные приложения. Самое главное, чтобы они обеспечивали необходимый уровень защиты и их базы всегда были в актуальном состоянии. Продукты Касперского можно загрузить по адресу [www.kaspersky.ru](http://www.kaspersky.ru), а программу AVG Anti-Virus Free — на веб-сайте [www.avg.com/ru-ru/avg-products](http://www.avg.com/ru-ru/avg-products).
- ◆ **Менеджер закачек.** Однозначно — программа Download Master. Это менеджер закачек, который позволяет по очереди закачивать файлы по добавленным пользователем ссылкам. Загрузить дистрибутив совершенно бесплатной программы Download Master можно на веб-сайте [westbyte.com/dm/](http://westbyte.com/dm/). Это практически идеальный продукт, поэтому искать аналогичные утилиты нет смысла.
- ◆ **Офлайн-браузер.** Тут есть из чего выбрать. Можно попробовать в деле две программы с русским интерфейсом: первую и платную, WebCopier, можно загрузить

---

<sup>1</sup> RC — Release candidate.

зять на веб-сайте [www.maximumsoft.com/](http://www.maximumsoft.com/); вторую и бесплатную, HTTrack, — на веб-сайте [www.httrack.com/](http://www.httrack.com/). В книге будет описан процесс работы с офлайн-браузером Offline Explorer, имеющим огромный недостаток — он платный.

- ◆ **FTP-клиент.** С FTP-серверов загружать файлы позволяет программа Download Master. Когда он бессилён, в качестве более удобного и продвинутого инструмента можно порекомендовать бесплатный Filezilla, который можно загрузить с веб-сайта [filezilla.ru/](http://filezilla.ru/).
- ◆ **Торрент-клиент.** Необходим для загрузки по протоколу BitTorrent. Дистрибутив этой программы имеет малый размер и доступен для бесплатной загрузки на веб-сайте [www.utorrent.com/](http://www.utorrent.com/).
- ◆ **Direct Connect-клиент.** Необходим для обработки ссылок вида magnet:, и в виде дистрибутива программы DC++ может быть загружен на веб-странице [dcplusplus.sourceforge.net/](http://dcplusplus.sourceforge.net/).
- ◆ **Дополнительные программные средства.** Сюда входят различные утилиты, без которых можно обойтись, но которые расширяют функциональность, например, веб-сайта. Ссылки и обзоры таких программ я буду размещать по мере необходимости.

На первый взгляд — все. Теперь я расскажу вам об элементарных правилах безопасности в Интернете.

## Обеспечение анонимности в Интернете

Теперь главное, что вам нужно сделать, — создать несколько электронных почтовых ящиков, необходимых для регистрации на различных веб-сайтах. Реальный рабочий или домашний электронный адрес указывать нельзя! Если только это не тщательно проверенный сервис и реальные данные необходимы для продолжительной работы с помощью регистрационных данных.

### **О Личных данных**

В Интернете никогда нельзя указывать реальные данные, такие как фамилия, имя, отчество, адрес, телефон, адрес электронной почты и т. п. Ничего, что могло бы ассоциировать вас как кибер-персонажа с реальным человеком. Ни в коем случае не размещайте подлинные фотографии, возьмите за правило использовать аватары. Причем на различных сайтах — разные. Исключение имеют известные веб-сайты, для регистрации на которых необходимо указывать реальные данные. В любых других случаях сведения, введенные вами, могут использоваться злоумышленниками!

В идеале — это временная почта, т. е. вы создаете временный почтовый ящик, как правило, без регистрации, письма в котором сохраняются от нескольких минут до нескольких месяцев. В принципе, больше и не нужно. Если вы, например, регистрируетесь на форуме, то можете указать адрес электронной почты на одном из таких сервисов. После того как придет письмо со ссылкой подтверждения регистрации, вы активируете учетную запись, перейдя по ссылке в письме, и теперь временный почтовый ящик можно закрыть и забыть про него — он автоматически будет удален через определенный промежуток времени. Чаще всего, вам достаточно указать логин, т. е. первую часть электронного адреса, до символа @, и уже можно

загрузить содержимое ящика. Существует также сервис, позволяющий создать любой временный почтовый ящик, попадающая в который почта будет автоматически пересылаться на ваш реальный электронный адрес.

На рис. 1.1 приведен пример одного из таких веб-сервисов (**pochta.bestinv.org**), позволяющих создать временный электронный почтовый ящик. В поле ввода нужно указать произвольное название почтового ящика, а затем щелкнуть мышью по ссылке **Задать свой e-mail**.

The screenshot shows the website interface for creating a temporary email. At the top, there is a language selection menu with options: Russian, English, Dutch, German, Polish, Spanish. The main heading is "Временная почта. Временный почтовый ящик". Below it, a text block explains that users can get a temporary email that expires in 15 minutes and can be used for reading and replying. There are two options: "Получить временный e-mail" (with a note that the address is randomly generated) and "Задать свой e-mail" (with a text input field and "@ trash.bestinv.org" next to it). At the bottom, there is a statistics line: "Создано адресов: 1335 · Получено писем: 1823 · Действующих писем: 1016 · Уничтоженных писем: 807 · Отправлено писем: 11".

Рис. 1.1. Вид сервиса временной электронной почты

Как правило, сервис рассчитан на то, что почтовый ящик используется здесь и сейчас, окно браузера не будет закрываться, поэтому восстановление содержимого ящика после закрытия программы Internet Explorer не предусмотрено. Содержимое почтового ящика обновляется каждую минуту, а спустя 15 минут после создания он будет уничтожен. Впрочем, вы можете продлевать жизнь своему почтовому ящику, используя ссылку **Дайте мне снова 15 минут**. Для вашего удобства далее я привел небольшую табл. 1.1 со списком доступных на момент написания книги сервисов временной почты.

Таблица 1.1. 25 бесплатных сервисов временной почты

Название	Адрес в Интернете	Комментарии
10MinuteMail	<b>www.10minutemail.com</b>	Почтовый ящик удаляется через 10 минут с возможностью пролонгации
Disposable Inbox	<b>www.disposableinbox.com</b>	Срок хранения сообщений — 24 часа. Есть возможность ответа на входящие сообщения
FilzMail	<b>filzmail.com</b>	Срок хранения сообщений — 24 часа
GuerrillaMail	<b>www.guerrillamail.com</b>	Почтовый ящик удаляется через 60 минут
Jetable.org	<b>www.jetable.org</b>	Указывается реальный адрес и продолжительность жизни ящика — от 1 часа до месяца. Затем генерируется адрес временного почтового ящика, который вы указываете на любых сайтах. Почта, попадающая на адрес сгенерированного почтового ящика, автоматически пересылается на реальный

Таблица 1.1 (продолжение)

Название	Адрес в Интернете	Комментарии
Mailexpire	<a href="http://mailexpire.com/create.php">mailexpire.com/create.php</a>	Продолжительность жизни ящика — от 12 часов до 3 месяцев
Mailinator	<a href="http://www.mailinator.com">www.mailinator.com</a>	Ограничения до 10 одновременно сохраняемых сообщений. Также ограничен размер каждого сообщения — 120 Кбайт
MakeMeTheKing	<a href="http://www.makemetheking.com">www.makemetheking.com</a>	
Melt Mail	<a href="http://meltmail.com">meltmail.com</a>	Указывается реальный адрес и продолжительность жизни ящика — от 3 до 24 часов. Затем генерируется адрес временного почтового ящика, который вы указываете на любых сайтах. Почта, попадающая на адрес сгенерированного почтового ящика, автоматически пересылается на реальный
Mint Email	<a href="http://www.mintemail.com/perfwd">www.mintemail.com/perfwd</a>	Указывается временный и реальный адреса. Продолжительность жизни ящика — от 12 часов до 3 месяцев. Почта, попадающая на адрес временного почтового ящика, автоматически пересылается на реальный
myTrashMail.com	<a href="http://www.mytrashmail.com">www.mytrashmail.com</a>	Продолжительность жизни — до месяца. Лимит — 4 Мбайт, до 2 Мбайт на одно письмо
Spam.la	<a href="http://www.spam.la">www.spam.la</a>	Отображаются все письма, пришедшие на любые почтовые ящики с доменом @spam.la. Можно использовать любое название ящика, а потом фильтровать письма на главной странице сайта
SpamBox	<a href="http://spambox.us">spambox.us</a>	Продолжительность жизни — от 30 минут до года с возможностью пролонгации
SpamFree24	<a href="http://spamfree24.org">spamfree24.org</a>	Создание временного почтового ящика на любом из пяти доменов на выбор. Сообщения хранятся несколько часов
Spamobox	<a href="http://www.spamobox.com">www.spamobox.com</a>	Почтовый ящик удаляется через 60 минут с возможностью пролонгации
TempEMail	<a href="http://www.tempemail.net">www.tempemail.net</a>	Почтовый ящик удаляется через 14 дней
Tempinbox	<a href="http://www.tempinbox.com/english">www.tempinbox.com/english</a>	Обязательно следует установить флажок, что вы подтверждаете условия соглашения
Tempomail.fr	<a href="http://tempomail.fr/creation_en.php">tempomail.fr/creation_en.php</a>	Указывается реальный адрес и продолжительность жизни ящика — от 4 часов до месяца. Почта, попадающая на адрес сгенерированного почтового ящика, автоматически пересылается на реальный
ThisMail	<a href="http://www.thismail.ru">www.thismail.ru</a>	Почтовый ящик удаляется через 120 минут
UnMail.ru	<a href="http://unmail.ru">unmail.ru</a>	Указывается реальный адрес и продолжительность жизни ящика — от 1 часа до месяца. Затем генерируется адрес временного почтового ящика, который вы указываете на любых сайтах. Почта, попадающая на адрес сгенерированного почтового ящика, автоматически пересылается на реальный

Таблица 1.1 (окончание)

Название	Адрес в Интернете	Комментарии
Will Hack For Food	<a href="http://wh4f.org">wh4f.org</a>	Необходимо указать любые имя пользователя и пароль, а затем выбрать продолжительность жизни ящика до недели. Данные сохраняются, вы можете входить в свою учетную запись со своим именем и паролем. До 10 сообщений размером не более 1 Мбайт. Продолжительность жизни аккаунта от 8 часов до 7 дней
YOPmail	<a href="http://www.yopmail.com">www.yopmail.com</a>	Срок хранения сообщений — 8 дней
Временная почта	<a href="http://pochta.bestinv.org">pochta.bestinv.org</a>	Почтовый ящик удаляется через 15 минут с возможностью пролонгации
Одноразовое.ru	<a href="http://odnorazovoe.ru">http://odnorazovoe.ru</a>	Срок хранения сообщений — 24 дня
Почта для спама	<a href="http://www.mailforspam.com">www.mailforspam.com</a>	Используется любой логин. Ящик доступен по адресу <a href="http://www.mailforspam.com/mail/логин">www.mailforspam.com/mail/логин</a>

Помимо временных почтовых ящиков, которые необходимо создавать перед регистрацией, вы можете выбрать определенные и уникальные имена/пароли, а затем зарегистрировать несколько постоянных почтовых ящиков. Временные адреса электронной почты удобны в тех случаях, когда необходимо выполнить несколько или выполнять периодически регистрацию на сервере, чтобы получить несколько учетных записей. Так делается, к примеру, на торрент-трекерах, ведущих статистику пользователя: благодаря нескольким учетным записям вы можете загружать файлы в пределах бесплатного лимита, перманентно продлевая его за счет новых регистраций, и, следовательно, следить за рейтингом вам ни к чему. Если же вы часто пользуетесь различными новостными веб-сайтами, предполагающими регистрацию для просмотра пользователем ссылок на файлы, — тут несколько учетных записей не нужны. Достаточно завести ящик электронной почты вида [vasyapupkin@mail.ru](mailto:vasyapupkin@mail.ru) и указывать его при регистрации на всех веб-сайтах. Это очень удобно по нескольким причинам. Во-первых, вы всегда точно помните адрес электронной почты, когда его требуется указывать в виде логина (если же в качестве логина используется уникальное имя, то можно указывать, например, первую часть адреса электронной почты — vasyapupkin). Во-вторых, иногда адрес электронной почты используется при восстановлении пароля (вот тут можно тоже завести один пароль на все сайты) — если была проведена регистрация на временный ящик, то письмо с данными восстановления пароля вы, скорее всего, уже не получите. Постоянный адрес электронной почты же будет существовать длительное время, пока вы им пользуетесь. Сервисы Mail.ru и Rambler вполне удобны и быстры, лишены недостатков. Самый удобный и безопасный — это ИМХО<sup>1</sup>, Gmail, соединение с ним идет через зашифрованный протокол HTTPS (об этом позже). Также вы можете попробовать следующие адреса: [www.nextmail.ru/](http://www.nextmail.ru/), [www.pochta.ru/](http://www.pochta.ru/), [www.freemail.ru/](http://www.freemail.ru/), [mail.yandex.ru/](http://mail.yandex.ru/), [www.hotmail.ru/](http://www.hotmail.ru/) и др.

<sup>1</sup> ИМХО от англ. *IMHO* — In my humble opinion (по моему скромному мнению).

Разумеется, со всеми этими "постоянными" электронными почтовыми ящиками лучше всего работать в почтовом клиенте, а не через веб-интерфейс. Особенно, если у вас несколько, а то и десяток зарегистрированных почтовых ящиков. Можете для этих целей использовать The Bat!, а еще лучше — Почта Windows Live, бесплатное приложение из пакета Windows Live (рис. 1.2). Программа Почта Windows Live доступна всем пользователям операционной системы Windows, а дистрибутив ее, как и другие программы пакета, можно загрузить на веб-сайте [home.live.com/](http://home.live.com/). Единственно, для использования всех возможностей понадобится потратить несколько минут на веб-сайте [www.microsoft.com/rus/liveid/default.aspx](http://www.microsoft.com/rus/liveid/default.aspx), чтобы создать свой идентификатор Windows LiveID.

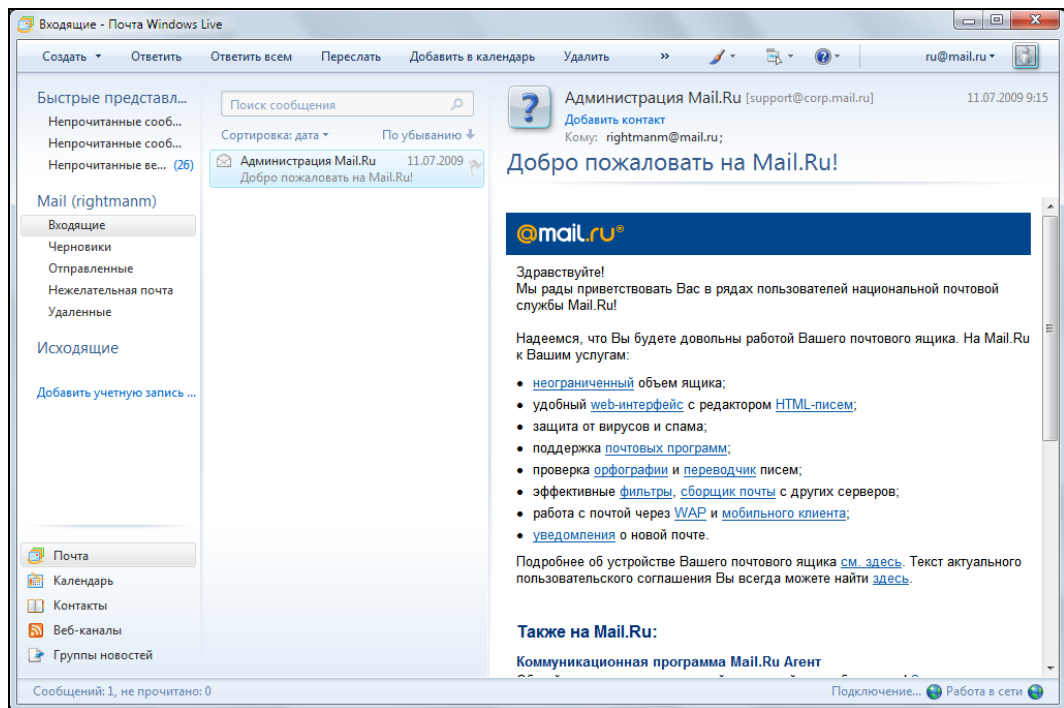


Рис. 1.2. Главное окно программы Почта Windows Live

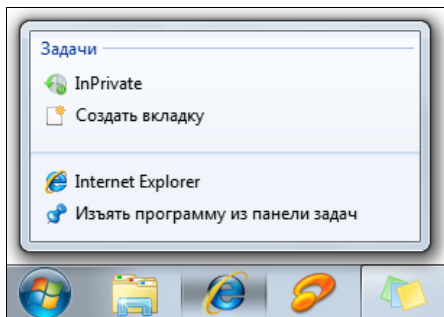
С электронной почтой, надеюсь, вы разобрались. Антивирусное приложение установили. Еще могу посоветовать не отключать штатный брандмауэр Windows, если только вы не используете аналогичное приложение других производителей.

Теперь извольте познакомиться с приватным режимом работы браузера Internet Explorer 8. Его можно запустить несколькими способами:

- ◆ в операционной системе Windows 7 щелкнуть правой кнопкой мыши на ярлыке программы, расположенном на панели задач, и выбрать во всплывающем списке команду **InPrivate** (рис. 1.3);
- ◆ в главном окне программы Internet Explorer 8 в меню **Безопасность** (Safety) выбрать команду **Просмотр InPrivate** (InPrivate Browsing);

- ♦ в главном окне программы Internet Explorer 8 нажать сочетание клавиш <Ctrl>+<Shift>+<P>.

Рис. 1.3. Всплывающий список программы Internet Explorer



В любом случае, браузер будет запущен в приватном режиме, о чем сообщит кнопка **InPrivate** перед строкой ввода адреса, нажатие которой выводит всплывающее сообщение о предназначении функции. В окне браузера, запущенном в режиме InPrivate, можно открывать неограниченное количество вкладок, однако защита распространяется только в пределах этого окна. Режим InPrivate позволяет посещать любые веб-страницы без сохранения временных файлов Интернета, файлов cookies, журнала посещенных узлов и других сведений. Если быть точным, то журнал посещения веб-страниц, данные форм и паролей, содержимое адресной

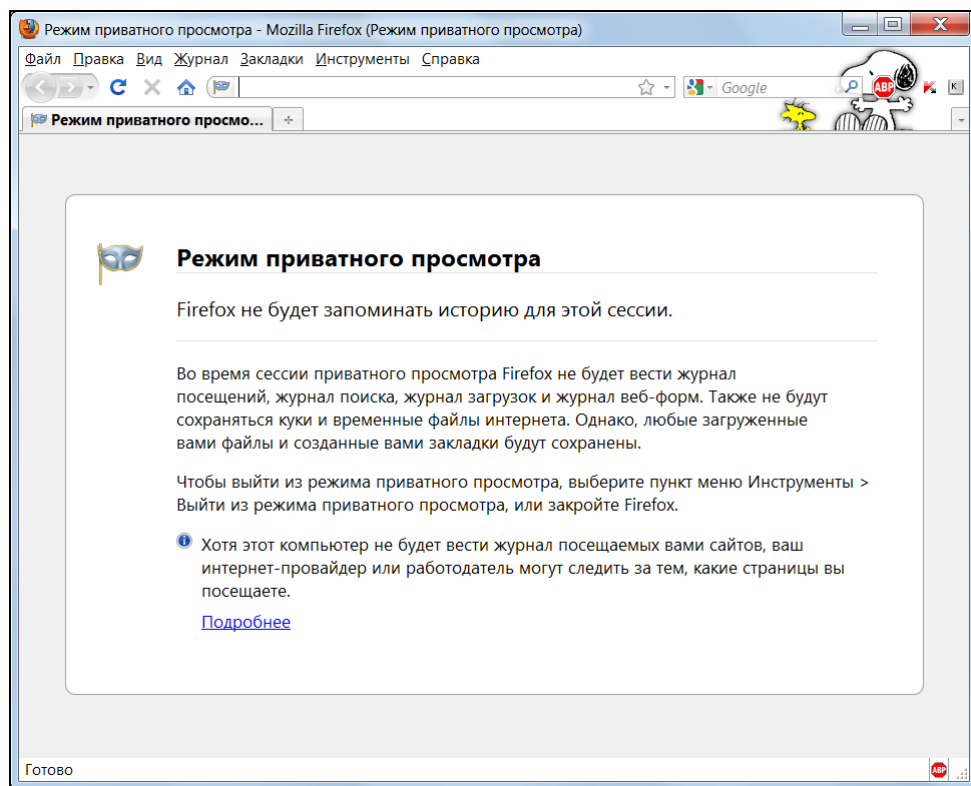


Рис. 1.4. Приватный режим в Firefox

строки и функции автозаполнения не сохраняются. Временные файлы Интернета, файлы cookies, данные функции автоматического восстановления после сбоя (ACR) и хранилище моделей объектов документов (DOM) сохраняются во время сеанса работы и удаляются после закрытия окна браузера. Данные антифишинга сохраняются в зашифрованном виде. Все элементы, которые вы добавите в **Избранное** в этом режиме, будут сохранены и после закрытия окна программы. Также, следует учитывать, что сетевой администратор может получить доступ к сведениям о посещенных веб-узлах даже в режиме InPrivate. И с помощью этого режима анонимность в Интернете не обеспечивается. Режим InPrivate предназначен для ограничения доступа к приведенным выше данным других (локальных) пользователей вашего компьютера.

Аналогичным приватным режимом обладает и ближайший конкурент ослика IE — браузер Firefox (рис. 1.4). Для входа в него достаточно выбрать команду меню **Инструменты | Войти в режим приватного просмотра** (Tools | Private Browsing) или же нажать сочетание клавиш <Ctrl>+<Shift>+<P>. Выход в "общественный" свет осуществляется повторным выбором команды меню или нажатием сочетания клавиш. В приватной сессии Firefox не ведет журналы посещений, загрузок, поиска и данных веб-форм, та также не сохраняет временные файлы и cookie.

## Мания преследования: миф и реальность

Часто бывает, особенно при подключении к Интернету через локальную сеть, что доступ к некоторым веб-сайтам заблокирован. Выводится предупреждение, что доступ запрещен, страница попросту не отображается или происходит перенаправление на какой-либо другой сайт, например, на главную страницу портала компании — все это говорит о том, что доступ вам к этому и подобным сайтам перекрыли. Так, например, во многих офисах запрещен доступ к социальным сетям типа **odnoklassniki.ru/** или **vkontakte.ru/**, в других, где ограничивается загрузка мультимедийных материалов, — к сайтам с соответствующим контентом. Или же на уровне национального шлюза существует запрет на посещение веб-страниц с определенным содержанием. В большинстве случаев подобные ограничения можно обойти.

Но прежде, чем в последующих главах я расскажу о приемах обхода подобных ограничений, вам надо узнать следующее. Во-первых, если введены какие-то ограничения, значит, это прописано в каком-либо приказе компании и, соответственно, нарушение пункта (пунктов) этого документа может повлечь ответственность сотрудника вплоть до увольнения. Поэтому вы на свой страх и риск будете пытаться нарушить запрет — подумайте, может, стоит подождать до вечера или выходных и получить доступ к развлекательным ресурсам из дома или интернет-кафе. Во-вторых, за редким исключением, вашу бесправную деятельность вполне можно распознать и пресечь — лучше, если это сделает администратор (с ним можно договориться — он же тоже человек). Распространенные способы обхода ограничений известны подготовленным администраторам, и когда их пытаются обмануть, им это может очень сильно не понравиться.



## **ПРЕДУПРЕЖДЕНИЕ**

Ваш провайдер тоже "знает" о ваших пристрастиях все и при необходимости может предоставить все сведения об активности IP-адреса вашего компьютера заинтересованным и уполномоченным лицам. При желании можно получить доступ к любой информации: сведениям о посещенных вами веб-сайтах, содержимом писем электронной почты и сообщений ICQ, с помощью провайдера узнать ваш IP-адрес и ваши личные данные.

Администратор может выборочно просматривать различные сведения о сетевой активности пользователей, такие как объем загруженного трафика, посещенные веб-узлы и т. п. Разумеется, появление в списке посещенных веб-сайтов IP-адресов социальных сетей, порноресурсов и т. д. или же загрузка внушительных объемов данных привлекут внимание ответственного человека. Так что делайте выводы. Ну а если желание получить доступ к чему-либо запретному просто-таки огромное, поехали дальше.

Если обход ограничений на доступ к социальным сетям или загрузка одной-двух песенок в MP3 в наихудшем случае может грозить увольнением (скорее, даже выговором), то нарушение авторских прав (а также и другие формы нарушений) может закончиться куда более плачевно. Особенно это касается случаев наподобие размещения пиратского контента на веб-сайтах или хакинга. В любом случае, посягательство на чью-то собственность может быть терпеливо воспринято собственником до определенного момента, достижения обозначенных границ. Если вы думаете, что выложив дистрибутив операционной системы с активатором на файлообменном ресурсе, вы останетесь незамеченным — вы заблуждаетесь. В 2006 году одной из директив Евросоюз обязал провайдеров хранить данные о трафике своих клиентов до двух лет и дольше. При желании определенных структур эта информация может быть предоставлена по первому же запросу. В некоторых странах (в том числе и в России) нормативные акты требуют от провайдеров установки оборудования, отслеживающего информационные потоки и контролируемого такими организациями, как Федеральная служба безопасности. Национальные шлюзы также могут контролироваться властями и в том числе запрещать доступ из страны к определенным ресурсам. В США под контролем Агентства национальной безопасности функционирует и проект ECHELON, анализирующий и сохраняющий содержимое сетевых и телефонных сеансов связи.

## **ПАРА СЛОВ ОБ ЭЛЕКТРОННОЙ ПОЧТЕ**

Сообщения электронной почты, прежде чем попасть от отправителя к адресату, мнут узлы провайдеров, которыми пользуются оба человека. В том случае, если сообщение отправляется в другую страну, то помимо провайдеров оно мнует еще и шлюзы обеих стран. На всех этапах своего пути оно может быть перехвачено, начиная хакерами и заканчивая службами безопасности — письмо пересылается по открытым каналам связи без какой-либо защиты. Это, как если вы разговариваете по телефону, а некто третий поднял трубку и подслушивает ваш разговор. При необходимости, во время передачи, в текст сообщения могут быть внесены изменения, и в результате вас могут скопрометировать, испортить репутацию и даже подвести к суду. Причем для поиска вашего сообщения не нужно просматривать миллионы посланий — быстро и эффективно все сделает программное обеспечение, фильтрующее поток данных. К примеру, поток электронных писем может фильтроваться на предмет наличия таких слов, как "warez" или "хакер" — в случае обнаружения ключевых слов текст письма будет изучен тщательнее.

Как описано в примечании, электронная почта может тщательно фильтроваться. Точно так же фильтруется и интернет-трафик. Например, в 2004 году при запросе в Google слова "falundafa"<sup>1</sup> появлялось диалоговое окно с сообщением, что по запросу ничего не обнаружено. Запрос производился с территории Китая и блокировался программой-фильтром национального шлюза до вывода результатов поиска. Фильтр способен сканировать содержимое запрашиваемых веб-страниц, а затем блокировать попытки просмотра при обнаружении "неправильных" слов. Кроме того, блокировка веб-сайтов на правительственном уровне может происходить по IP-адресу и доменному имени. Еще используется сравнительно новый метод — при запросе "запрещенной" веб-страницы ваш браузер автоматически перенаправляется на другой веб-сайт.

Помимо шлюзов и серверов провайдеров, составить ваш портрет может и сам компьютер, которым вы пользуетесь дома, на работе или в интернет-кафе. Все ваши шаги сохраняются в небольших файлах cookies, размещаемых как на локальном компьютере, так и на посещаемом сервере. Файлы cookies содержат различные данные, например, сведения о местоположении пользователя, чтобы при запросе пользователя из России открывать страницу **microsoft.ru**, а не **microsoft.com** или **microsoft.us**. Просмотрев файлы cookies на вашем компьютере, можно сделать вывод о ваших привычках и пристрастиях.

Поэтому периодически нужно выполнять удаление файлов cookies в браузере. Для этого в Internet Explorer нужно выбрать команду меню **Безопасность | Удалить журнал обозревателя** (Safety | Delete Browsing History) и в открывшемся диалоговом окне установить флажок **Файлы "cookie"** (Cookies). После нажатия кнопки **Удалить** (Delete) временные файлы Интернета, включая файлы cookies, будут удалены. В Firefox те же цели преследует команда меню **Инструменты | Стереть недавнюю историю** (Tools | Clear recent history). В открывшемся диалоговом окне следует установить флажки напротив удаляемых категорий данных (рис. 1.5), вы-

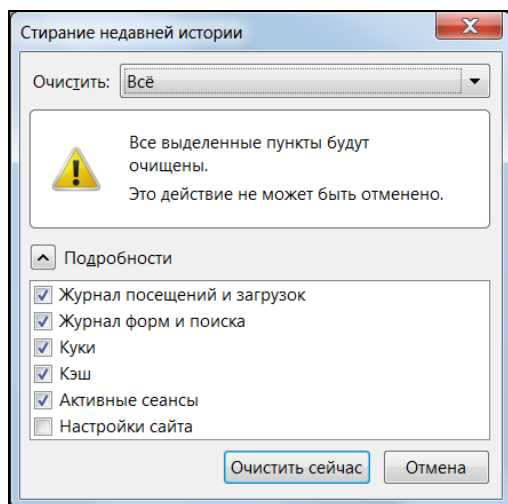


Рис. 1.5. Диалоговое окно Стирание недавней истории

<sup>1</sup> Духовное движение, запрещенное в Китае.

брать диапазон времени в раскрывающемся списке **Очистить** (Time range to clear) и нажать кнопку **Очистить сейчас** (Clear now).

И настойчиво рекомендую установить и настроить приложение Tor — это не сложно, а уровень анонимности и безопасности существенно повысится.

Этот небольшой отступ от темы книги я сделал для того, чтобы вы поняли серьезность ситуации, что нужно с осторожностью вести себя в Интернете, не привлекать внимание (под взглядом Большого Брата (☺)), соблюдать правила наподобие "не разжигать национальную рознь", "не нарушать авторские права" и т. п.

## ГЛАВА 2



# Как посетить запрещенный для доступа сайт

Туда, где вам нужно быть обязательно,  
сегодня попасть нельзя.

*Закон Мерфи*

В этой главе я расскажу, как обойти ограничения в Интернете и посетить те узлы, доступ к которым ограничен. Это может быть блокировка на уровне государства (национальным шлюзом) или в более мелких масштабах — на уровне организации или провайдера.

## Получение доступа посредством анонимайзера

Самый простой вариант обойти ограничение на посещение конкретного узла — воспользоваться CGI-прокси или "анонимайзером". В отличие от HTTP-прокси, ничего в настройках браузера изменять не нужно, требуется лишь перейти на веб-сайт "анонимайзера", содержащий поле ввода адреса и кнопку перехода на введенный адрес. В качестве примера в первом издании книги использовался реальный сайт — [www.bikermatch.co.uk/](http://www.bikermatch.co.uk/), зарегистрироваться на котором могли только обладатели IP-адресов Великобритании, т. е. предположительно жители туманного Альбиона. На данный момент доступ к регистрации открыт для всех, а найти другой, похожий ограничениями, сайт не удалось. Поэтому воспользуемся сервисом определения IP-адреса пользователя, причем с отображением его местонахождения на карте Google.Maps, IpGeoBase (рис. 2.1).

Как видно из содержимого страницы, по IP-адресу определено местонахождение пользователя — Тула, Российская Федерация, а также и указано на карте.

### **ОПРЕДЕЛЕНИЕ СОБСТВЕННОГО IP-АДРЕСА**

Определить собственный IP-адрес вы можете также, например, на веб-сайтах [2ip.ru](http://2ip.ru), [www.myip.ru](http://www.myip.ru) или [www.whoer.net/ext](http://www.whoer.net/ext).

Теперь я попробую использовать прокси-сервер, через который проложит путь запрос от моего компьютера к серверу [ipgeobase.ru/](http://ipgeobase.ru/). Прокси-серверов в Интернете тысячи, и располагаться они могут в самых различных государствах. Также вам следует знать, что информация о том, что вы обращаетесь к прокси-серверу, тайной не является.

IpGeoBase Release 0.2

При поддержке RUcenter

Главная страница | Расширенный поиск | Архив | Программное обеспечение | Обратная связь | Помощь

Поиск географического местонахождения IP-адреса, выделенного RIRе локальным интернет-регистром (LIR-ам) для Российской Федерации. Поиск IP адреса осуществляется с точностью до города. База обновляется ежедневно!

Ваш IP-адрес: 94.28.142.33  
 Ваш город: Тула  
 Ваш регион: Тульская область  
 Ваш округ: Центральный

Неправильно? Сообщите нам!

Последние новости:

5 Августа, 2010  
 XML сервис поставлен на мониторинг. [Подробнее>>>](#)

2 Апреля, 2010  
 Технические проблемы [Подробнее>>>](#)

IP адрес:  Искать

[Расширенный поиск>>>](#)

Ваш IP: 94.28.142.33  
 Город: Тула  
 Регион: Тульская область  
 Фед. округ: Центральный  
 Неправильно? Сообщите нам!

ПО предоставлено Куташовым И.Е (www.astron-gt.ru)

Рис. 2.1. Сервис IpGeoBase определил местонахождение пользователя

Самый простой вариант прокси-сервера — это CGI-прокси или "анонимайзер", веб-сайт которого сразу содержит строку, куда вводится адрес заблокированного узла, а затем осуществляется переход на соответствующую страницу. Множество ссылок на подобные сервисы можно получить, указав в качестве запроса "CGI проху" или "анонимайзер" в поисковой строке веб-сайта Google или Яндекс. На момент написания книги вполне нормально функционировали **hideme.ru**, **anonymouse.org**, **www.hidemyass.com**, **g-tunnel.com** и **www.shadowsurf.com**. Также в русском сегменте Интернета есть отличный постоянно обновляющийся веб-сайт и форум, содержащий информацию о свежих прокси-серверах, различных полезных программах и т. п. Адрес: **www.freeproxy.ru/ru/index.htm**.

Существуют как бесплатные, так и платные CGI-прокси. Недосток бесплатных в том, что скорость работы их часто оставляет желать лучшего. Минус платных — приходится платить деньги, причем от сбоев связи вы все равно не застрахованы. Иной раз вам придется перебрать не один десяток CGI-прокси, чтобы получить приемлемое качество соединения.

### БЛОКИРОВКА ПРОКСИ-СЕРВЕРОВ

Разумеется, доступ к прокси-серверам тоже может блокироваться системными администраторами, поэтому периодически возникает потребность в смене CGI-прокси. Думаю, это не проблема, т. к. их количество исчисляется десятками тысяч, а заблокировать все просто невозможно.

Я воспользуюсь русским веб-сайтом PROXer, расположенным по адресу **www.proxer.ru** (рис. 2.2).

Удобство этого веб-сайта в том, что, по сути, не являясь прокси-сервером, он позволяет выбрать подходящий CGI-прокси из списка проиндексированных. Все,

что нужно сделать, — ввести адрес веб-сайта и нажать кнопку **PRoX!**. Будет автоматически предложен один из доступных прокси-серверов, а затем произойдет автоматическое перенаправление на него (не забудьте включить всплывающие окна). После ввода адреса (в моем случае, **http://ipgeobase.ru** (без этого список не выводится, а происходит редирект на главную страницу)) и нажатия кнопки **List** вы увидите список прокси-серверов (рис. 2.3).

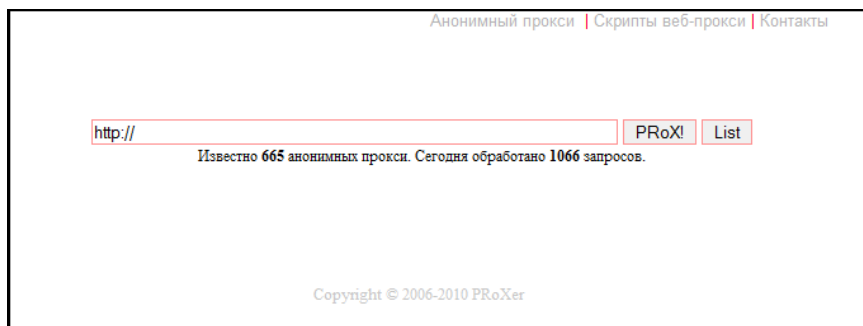


Рис. 2.2. Веб-сайт PRoXer

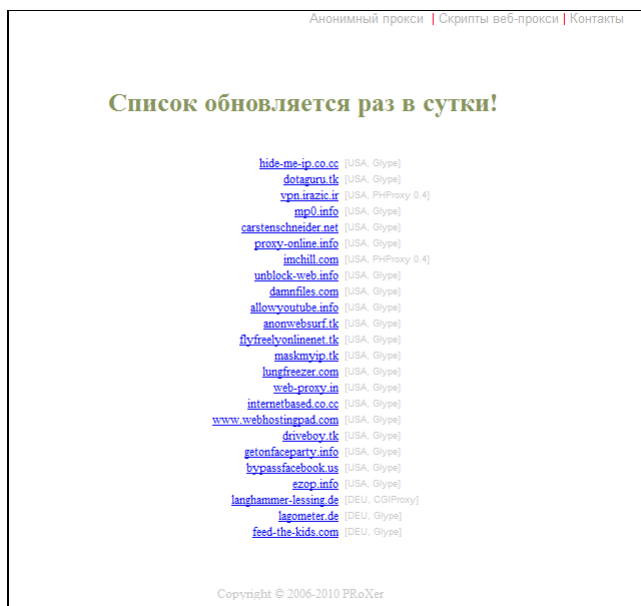


Рис. 2.3. Список предлагаемых прокси-серверов

Ради интереса, попробую выбрать прокси-сервер, расположенный, допустим, в Турции. Попался **gizlinet.org**: в строку ввожу адрес **http://ipgeobase.ru** и нажимаю кнопку **Siteye Git** (рис. 2.4).

После минутного ожидания (ну, не все прокси стремительны, тем более бесплатные) видим результат (рис. 2.5).

К сожалению, сервис не отобразил не только положения на карте, но и страну, в которой находится обладатель данного IP. Другие же сервисы уверенно заявляли, что я совершенно точно вышел в Интернет из Стамбула.

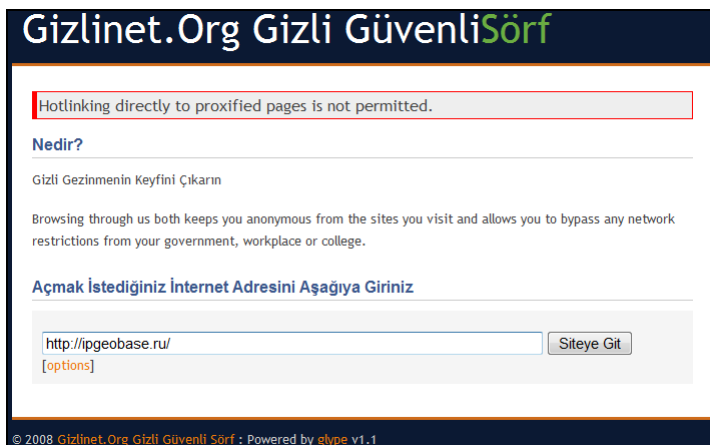
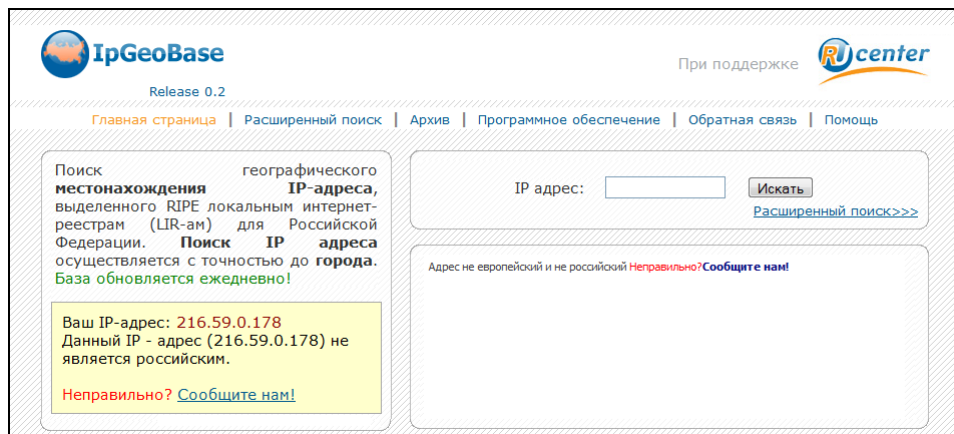
Рис. 2.4. Вид страницы ресурса [gizli.net](http://gizli.net)

Рис. 2.5. IP-адрес изменен

Таким образом, можно получить доступ к содержимому многих веб-сайтов, просмотр которых на вашем компьютере по каким-то причинам запрещен.

### **АДРЕСА ПРОКСИ-СЕРВЕРОВ**

Вы можете просмотреть списки адресов свежих прокси-серверов на веб-сайте [tools.rosinstrument.com/proxy/](http://tools.rosinstrument.com/proxy/).

Важно иметь в виду, что сам факт вашего обращения к прокси-серверу тайной для администратора не является, так же, как и все остальные данные (в том числе какой заблокированный ресурс вы хотите просмотреть, его содержимое), потому что обмен информацией происходит по незашифрованному каналу связи. То же касается НТТР-прокси, отличие которых от "анонимайзеров" заключается в необходимости указывать IP-адрес и порт в свойствах браузера (или любой другой программы, имеющей возможность работать через прокси-сервер) и работать с заблокированными веб-сайтами напрямую, без CGI-прокси.

Для повышения уровня безопасности можно воспользоваться защищенным протоколом связи — HTTPS. Буква *S* обозначает *secure* — безопасный. В этом случае, при подключении HTTPS прокси-серверу передается только команда подключения к определенному узлу, а прокси-сервер, в свою очередь, организует в обе стороны пассивную передачу зашифрованного трафика. Можно определить, что вы подключились к прокси-серверу, но узнать, какой веб-сайт вы решили "нелегально" посетить, — затруднительно. Такие узлы можно определить по наличию протокола HTTPS в адресе, например, <https://www.torproject.org>.

Важно выяснить, действительно ли предлагаемый прокси-сервер является анонимным и способен зашифровать ваше реальное месторасположение. В этом случае вы можете обратиться к веб-сайтам определения вашего IP-адреса, некоторые из них указаны ранее, или же просмотреть сведения о "себе" с помощью специализированных сайтов типа [www.stilllistener.addr.com/checkpoint1/index.shtml](http://www.stilllistener.addr.com/checkpoint1/index.shtml) или [servicevpn.net/who](http://servicevpn.net/who). После того как вы настроите подключение к прокси-серверу, посетите один из подобных веб-сайтов и просмотрите, насколько тщательно скрывается информация о вашем местоположении, IP-адресе, браузере и другие сведения.

## Настройка браузера для доступа к веб-сайтам через прокси

Далее я расскажу, как указать подключение через прокси-сервер в настройках браузера Internet Explorer.

1. В главном окне программы Internet Explorer выберите команду меню **Сервис | Свойства обозревателя** (Tools | Internet Options). Откроется одноименное диалоговое окно.
2. Перейдите на вкладку **Подключения** (Connections). Содержимое диалогового окна **Свойства обозревателя** (Internet Options) изменится (рис. 2.6).
3. Нажмите кнопку **Настройка сети** (LAN Settings). Откроется диалоговое окно **Настройка параметров локальной сети** (Local Area Network (LAN) Settings) — рис. 2.7.

### **НАСТРОЙКА ПРОКСИ В FIREFOX**

В браузере Firefox настройка прокси происходит аналогично. Выбрав команду меню **Инструменты | Настройки** (Tools | Options), вы откроете одноименное диалоговое окно, в котором нужно перейти на вкладку **Дополнительно** (Advanced). Далее следует выбрать дополнительную вкладку **Сеть** (Network) и нажать кнопку **Настроить** (Setup). Открывшееся после этого диалоговое окно предназначено для указания данных прокси-сервера.

4. Чтобы назначить подключение через прокси-сервер, нужно установить флажок **Использовать прокси-сервер для локальных подключений** (Use a proxy server for your LAN), а затем указать в поле ввода **Адрес** (Address) IP-адрес прокси-сервера (HTTP или HTTPS) вида 61.19.213.42, а в поле ввода **Порт** (Port) — порт подключения, например, 8080.



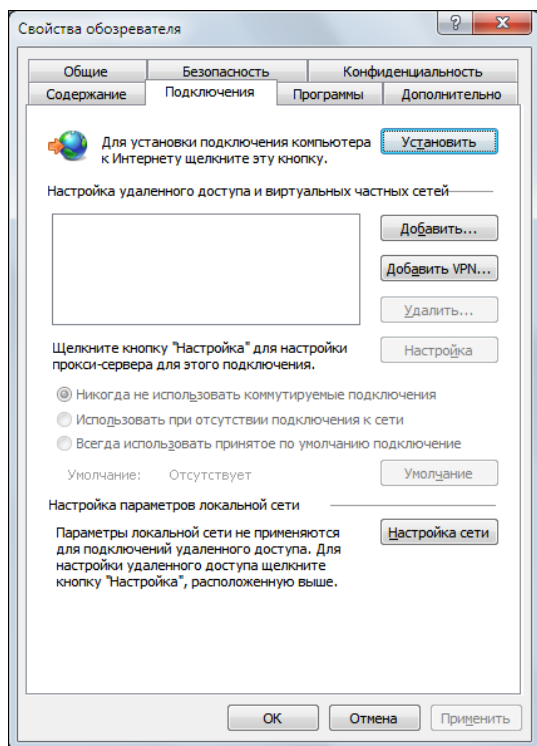


Рис. 2.6. Диалоговое окно Свойства обозревателя

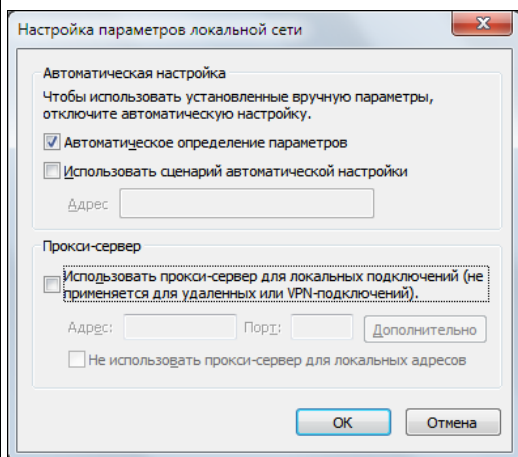


Рис. 2.7. Диалоговое окно Настройка параметров локальной сети

5. Вы также можете нажать кнопку **Дополнительно** (Advanced) и в открывшемся диалоговом окне указать адреса различных прокси-серверов для разных протоколов.

#### **ПРИМЕЧАНИЕ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ С УДАЛЕННЫМ ИЛИ VPN-ПОДКЛЮЧЕНИЕМ**

Указанные шаги недоступны, если вы получаете доступ в Интернет с помощью удаленного или VPN-подключения. В этом случае нужно выделить активное подключение в списке, расположенном на вкладке **Подключения** (Connections) диалогового окна **Свойства обозревателя** (Internet Options) и нажать кнопку **Настройка** (Settings).

После того как вы настроите подключение через прокси в свойствах браузера, вы сможете несколько безопаснее чувствовать в Интернете и посещать заблокированные администратором узлы. Для лучшего шифрования можно использовать цепочки прокси, например, указав в свойствах браузера подключение через HTTP-прокси, загрузите искомую страницу не напрямую, а через "анонимайзер". Или даже два "анонимайзера". Получится цепочка вида "HTTP-прокси — CGI-прокси — CGI-прокси". Так обнаружить вас будет еще сложнее. Только подбирать следует достаточно скоростные прокси-серверы, иначе, если хотя бы одно звено будет работать слишком медленно, загрузки требуемой веб-страницы будете ждать очень долго или же произойдет обрыв соединения.

Тем не менее, в описанных случаях вы сможете более-менее анонимно просматривать только содержимое веб-страниц, а электронная почта, ICQ и другие средств

ва связи остались в совершенно незашифрованном виде. Для обеспечения более высокого уровня анонимности можно воспользоваться услугами целой анонимной сети, такой как Tor.

Далее я привел небольшой список прокси-серверов (что, в принципе, бессмысленно, т. к. они постоянно перестают работать, а на их месте возникают новые):

- ◆ Anonymizer — [www.anonymizer.ru](http://www.anonymizer.ru);
- ◆ Anonymouse — [anonymouse.ws](http://anonymouse.ws);
- ◆ Guardster — [www.guardster.com](http://www.guardster.com);
- ◆ HideMyAss — [www.hidemyass.com](http://www.hidemyass.com);
- ◆ MegaProxy — <https://www.megaproxy.com/freesurf/>;
- ◆ ProxyWeb — [www.proxyweb.net](http://www.proxyweb.net);
- ◆ ShadowSurf — [www.shadowsurf.com](http://www.shadowsurf.com);
- ◆ The Cloak — [www.the-cloak.com/login.html](http://www.the-cloak.com/login.html);
- ◆ W3Privacy — [www.w3privacy.com](http://www.w3privacy.com);
- ◆ WebWarper — [webwarper.net](http://webwarper.net).

Чаще всего посредством "анонимайзеров" пользователи пытаются получить доступ к веб-сайтам типа **odnoklassniki.ru** и **vkontakte.ru**. Разумеется, с этой задачей прокси-серверы справляются. Вспомнил о социальных сетях я потому, что обнаружил в Интернете сервисы, специально предназначенные для получения доступа к этим сайтам, такие как **zapretanet.ru**. Сомнительно, что сайты с платным хостингом (т. е. за данный сайт владелец вносит плату) будут бесплатно предлагать услуги пользователям по предоставлению доступа к социальным сетям. Вполне вероятно, что генерируемые на этих веб-сайтах ссылки — не что иное, как прямой путь на фишинговые сайты, создаваемые с целью завладения вашими данными: логином, паролем и прочими сведениями. Зачем это кому-то может быть нужно? Хотя бы для продажи рекламодателям: по содержимому ваших диалогов и учетных записей (например, раздела **Предпочтения**) вполне можно составить о вас портрет — кто вы и что готовы приобрести. Впоследствии приходящий спам на ваш электронный, да и почтовый ящик будет рекламировать именно то, в чем вы зарегистрированы.

### **ПОЛУЧЕНИЕ ДОСТУПА К САЙТАМ СОЦИАЛЬНЫХ СЕТЕЙ**

Подавляющее большинство офисных прокси запрещают доступ к сайтам социальных сетей, типа "В Контакте", "Одноклассники" и т. п. Первый способ обхода ограничений знаете. Еще вариант заключается в указании в адресной строке браузера IP-адресов этих сайтов. Об этом подробнее в следующей главе.

К тому же, представьте интерес, например, магазина электроники: "просканировав" предпочтения десятков и сотен тысяч пользователей социальных сетей, можно сформировать мнение, какие товары в первую очередь пользуются популярностью, на покупку каких товаров стоит привлечь скидкой и т. п. Будьте осторожны при посещении различных веб-сайтов, предполагающих ввод логина и пароля для активации аккаунта. Обязательно убедитесь, что содержимое в адресной строке браузера соответствует реальному адресу веб-сайта: **odnoklassniki.ru**, а не **odn~~a~~klassniki.ru**, **odn0klassniki.ru** или вообще **rtl-odnoshkolniki.ru**. Подробнее про фишинг я написал в последней главе, там же привел скриншот поддельного веб-сайта, существовавшего на момент написания книги. Будьте осторожны!

## ГЛАВА 3



# Способы обхода ограничений администратора сети

Именно в тот момент, когда вам нужно собрать доказательства несанкционированной деятельности, окажется, что регистрация событий не включена.

*Закон Мерфи для администраторов сети*

Надеюсь, некоторые советы в предыдущей главе помогли вам получить доступ к тем веб-страницам, посещение которых ограничено или запрещено. Конечно, описанные методы работают не в 100% случаев, и в других ситуациях вам сможет помочь специализированный софт, например WideCap ([widecap.ru](http://widecap.ru)), или попытка договориться с системным администратором. А может быть, вообще лучше бросить эту затею и наслаждаться свободой веб-серфинга и download дома. Но понятно, запретный плод сладок, в чужом огороде и дичка вкусна и т. д. Ну что ж, доступ к одноклассникам получили, теперь вы хотите скачать новую песню, исполненную вашим другом или сразу целый видеоальбом. Вполне резонное желание — чем же еще заниматься на работе? С этим несколько сложнее. Хотя бы потому, что при посещении веб-сайтов трафик в вашу сторону будет незначителен. А в случае с мультимедийными (и другими) файлами объем входящего трафика пропорционально увеличивается с каждым днем согласно вашим аппетитам и укреплению мнения, что вас никто не заметит.

### **ВОЗМОЖНЫЕ ПРОБЛЕМЫ**

Нарушение правил "поведения" в сети офиса может грозить вам штрафом, выговором и даже увольнением. Советами, описанными в этой книге, вы пользуетесь на свой страх и риск! Кроме вас никто ответственности не несет!

Ложное представление, потому что сисадмин уже давно следит за вами, что, даже после заграждения "анонимайзерами", мегабайты и гигабайты трафика выдадут вас с головой, что вы занимаетесь отнюдь не загрузкой бизнес-отчетов и материалов для развития фирмы. Проверка же вашего компьютера в ваше отсутствие (не беспокойтесь, пароль вашей учетной записи Windows давно известен, а если нет — существуют программы "кейлоггеры" и различные способы сброса/восстановления пароля) и обнаруженные, к примеру, cookies станут доказательством. Поэтому еще раз вас предупреждаю, что все последствия, к которым могут привести ваши действия, полностью на вашей совести. И если вас это не побуждает отказаться от своей

затеи, далее попробую дать пару советов, если на вашем компьютере запрещено загружать файлы каких-либо типов.

## Смена расширения: как обойти ограничения администратора в офисе

В корпоративных сетях другим способом (первый заключается в ограничении доступа к сайту целиком<sup>1</sup> — об обходе этого лимита вы узнали в предыдущей главе) ограничения доступа к материалам в Интернете является запрет на открытие/просмотр/загрузку файлов определенных расширений. Скажем, чаще всего блокируется загрузка видео и звуковых файлов, например, по расширению MP3, а вы страсть как хотите загрузить какую-либо песню определенного исполнителя. Вариантов обойти ограничение может быть несколько:

- ◆ воспользоваться средствами веб-сайта с инструментами по смене расширения. Подобная возможность есть на различных веб-сайтах, находимых по запросу "музыка бесплатно и без регистрации";
- ◆ попробовать найти нужный файл размещенным с другим (доступным для загрузки) расширением, к примеру, в виде архива RAR. В отношении музыкальных композиций это могут быть не отдельные дорожки, а альбомы целиком, запакованные в единый архив, с расширениями RAR, ZIP, 7Z и др.;
- ◆ воспользоваться услугами одного из сервисов, предлагающих переслать искомый файл на адрес электронной почты;
- ◆ воспользоваться услугами так называемой "файловой почты", позволяющей средствами сервиса загружать любые файлы, записывать на диски и отправлять на указанный почтовый адрес. Некоторые подобные сервисы включают возможность скачивания пользователем файла (ранее выбранного для загрузки) со сменной расширением;
- ◆ воспользоваться средствами пиринговых сетей (но если в сети вашего предприятия действуют какие-либо ограничения, почти наверняка вам запрещен доступ к "магнитным" ссылкам и торрент-файлам);
- ◆ использовать метод подстановки расширения. В этом случае следует перейти по ссылке запрашиваемого файла: если загрузка данного типа файлов запрещена (стоит убедиться, что действительно определенный тип файлов заблокирован для загрузки, а не искомый файл удален с сервера владельцами ресурса), то вы увидите страницу с сообщением, что веб-страница не может быть отображена. В данном случае можно попробовать вручную сменить расширение на другое.

Рассмотрю описанные методы более подробно.

Самое первое, что следует попробовать, — загрузить файл с другим расширением на одном из ресурсов, предоставляющих такую возможность (рис. 3.1).

---

<sup>1</sup> Или наоборот, доступ запрещен ко всем сайтам, за исключением, к примеру, корпоративных. В этом случае обойти запреты практически невозможно, но, к счастью, такие "зверские" ограничения редки.

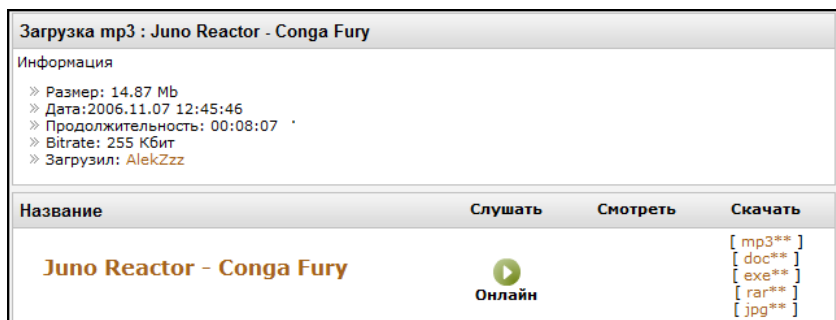


Рис. 3.1. Смена расширения загружаемого файла средствами веб-сайта

Как видно из рисунка, выбранный файл можно загрузить с одним из расширений на выбор (MP3, DOC, EXE, RAR или JPG), которое затем нужно сменить на истинное.

### ОТОБРАЖЕНИЕ РАСШИРЕНИЙ ФАЙЛОВ В WINDOWS

По умолчанию расширения файлов в операционной системе Windows скрыты. Для их отображения следует открыть окно любой папки (или запустить программу Проводник (Explorer)). Нажав клавишу <Alt>, чтобы отобразить строку меню, выберите команду **Сервис | Параметры папок (Tools | Folder Options)**. Перейдите в открывшемся диалоговом окне на вкладку **Вид (View)** и сбросьте флажок **Скрывать расширения для зарегистрированных типов файлов (Hide extensions for known file types)**. Стоит также помнить, что установка ошибочного расширения файла приведет к невозможности его чтения, поэтому изменяйте расширения только в тех случаях, когда четко представляете себе результат операции.

Если доступные на веб-сайте расширения файлов у вас заблокированы или же искомый файл отсутствует, попробуйте поискать файл с другим расширением, например, создав запрос вида "Вася Пупкин — Песня.rar". Как вариант, в Интернете можно обнаружить сразу весь альбом данного исполнителя, упакованный в архив RAR, ZIP или др. В этом случае, нужно оформлять запрос в виде "Вася Пупкин — Альбом (2011)"<sup>1</sup> (можно и без указания года, но тогда результаты поиска будут не совсем теми, которые требуются). Навести справки о названии альбома или сборника, в который входит та или иная композиция, можно на веб-сайте **www.discogs.com** (в основном зарубежные исполнители). Стоит учесть, поиски релиза (альбома, пластинки, сборника и т. п.), а не отдельной песни в большинстве случаев выведут вас на файлообменный сервис или торрент-трекер.

Как вариант, вы можете заказать какой-либо файл прислать на указанный адрес электронной почты. Эта возможность понравится также тем, у кого лимитированный Интернет, а доступ к электронной почте неограничен и (или) бесплатен. Существует несколько сервисов, позволяющих высылать запрашиваемые файлы по электронной почте. Обнаружить их вы можете по следующим адресам: **postfile.ru**, **filemail.ru**, **www.tcompressor.ru/Files-by-Email**. Как правило, небольшие файлы

<sup>1</sup> Причем кавычки, в которые заключен сам запрос, — весьма важная деталь. Об этом вы узнаете в одной из следующих глав.

(до 10 Мбайт) вы сможете заказать совершенно бесплатно. Подробнее об услуге отправки файлов на ваш адрес электронной почты мы поговорим в одной из следующих глав.

Существует и возможность отправки загруженных сервером файлов в виде записанных CD- или DVD-дисков на указанный вами почтовый адрес. В этом случае вы оплачиваете загрузку и запись диска (примерно 300—400 руб. за полностью заполненный DVD-диск), а также услуги почтовой связи. Подробнее *см. главу 9*.

Еще один способ — воспользоваться средствами одноранговых или пиринговых сетей. В качестве примера в одной из глав данной книги я описал приемы работы с пиринговой сетью BitTorrent, наиболее популярной в настоящее время. В этом случае ограничения по типу файла не учитываются, но в большинстве случаев, если существуют какие-либо ограничения, доступ к пиринговым сетям также заблокирован.

Метод подстановки расширения я опишу прямо сейчас. Оговорюсь, что работает он далеко не на всех веб-сайтах, но попытаться вы можете. Суть метода в том, что, к примеру, заблокированный к загрузке файл `song_of_vasya.mp3` вы запрашиваете как `song_of_vasya.klz` (любой набор символов после точки или же строго определенный правилами сервера). Вы загружаете файл `song_of_vasya.klz`, изменяете расширение на MP3 и спокойно прослушиваете его в проигрывателе. Теперь о сайтах. На каждом веб-сайте, поддерживающем технику подмены расширения, существуют свои правила. Так, например, известный (правда, и платный) ресурс **irecs.ru** позволяет сменить стандартное расширение файла MP3 на один из девяти вариантов других форматов.

### **БЕСПЛАТНО НА IRECS.RU**

Везде можно найти что-то бесплатное. Ресурс **irecs.ru** — не исключение. В разделе **Бесплатно** ([irecs.ru/free/](http://irecs.ru/free/)) вы можете бесплатно скачивать композиции дня, а при балансе более 150 руб. — вам еще доступны 15 релизов радиопередач и живых выступлений.

Это удобно, т. к. вы можете сразу определить, что все файлы будете загружать с расширением, к примеру, MAN. А что же делать тем, у кого все эти форматы запрещены, а разрешен только внутренний формат документов компании, к примеру, SHIT. Смешно? Проверим.

1. Щелкните правой кнопкой мыши на прямой ссылке к файлу. Откроется контекстное меню браузера.

### **ПРЯМЫЕ ССЫЛКИ**

*Прямой ссылкой к файлу* можно считать ссылку вида **www.site.com/123.exe** или же с любым другим окончанием, при щелчке мышью на которой начинается непосредственная загрузка файла (а не переход на другую веб-страницу).

2. Выберите команду **Копировать ярлык** (Copy Shortcut), чтобы скопировать прямую ссылку в буфер обмена.
3. Удалите содержимое адресной строки браузера, а затем щелкните на ней правой кнопкой мыши и выберите команду **Вставить** (Paste) из контекстного меню. В адресной строке появится ссылка к запрашиваемому файлу.