Михаил Райтман

КАК найти и СКАЧАТЬ в Интернете любые файлы

Санкт-Петербург
«БХВ-Петербург»
2010

УДК 681.3.06
ББК 32.973.26-018.2
Р18

Райтман М. А.

Р18 Как найти и скачать в Интернете любые файлы. — СПб.: БХВ-Петербург, 2010. — 336 с.: ил.

ISBN 978-5-9775-0510-9

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.

Для широкого круга читателей

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*
Редактор	*Анна Кузьмина*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.04.10.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 27,09.
Тираж 2000 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 978-5-9775-0510-9

Оглавление

Введение, или почему эта книга может вам пригодиться?

На книжной полке в магазине, в котором вы сейчас находитесь (хотя может уже сидите за компьютером дома :)), по соседству вы найдете еще десяток добрых книг про то, как все скачать, причем бесплатно, из Интернета. Проблема большинства таких изданий в том, что чаще всего они представляют собой обзор *как* можно качать: и так и этак, причем предполагается, что искомый файл уже найден. Самое полезное от подобных руководств есть и в этой книге. Но много и отличий. Например, я вам расскажу, как загружать файлы и просматривать содержимое веб-страниц, если по каким-то причинам это запрещено (например, администратором сети или в вашем городе/стране). В книге также вы найдете интересные факты и сведения об обеспечении безопасности, причем в начале книги упор сделан на вашу личную (в основном, анонимность), а в конце — вашего компьютера. Вы узнаете, как бесплатно загружать файлы с файлообменных сервисов и что делать, если искомый файл найден на платном хостинге. Познакомитесь с темными дебрями Интернета и разновидностями инструментов (лекарств, таблеток и пилюль от жадности), которыми нас заботливо снабжают как отдельные программисты и программистки, так и целые хакерские группы. Усвоите, чем все это грозит и как же можно расстаться с желанием бесплатно пользоваться тем, что платно. С этой целью я привел обзор бесплатного, аналогичного коммерческому, программного обеспечения и онлайн-инструментов для выполнения различных задач. Полезным, надеюсь, окажется материал о сохранении видеороликов с хостинговых сайтов и социальных сетей (разумеется, обычными методами это не всегда возможно), а также главы об основах работы с пиринговыми сетями. Причем вы научитесь не только скачивать файлы по magnet- и torrent-ссылкам, но и создавать собственные раздачи. Если же подключение к Интернету у вас дома или в офисе слишком медленное (дорогое), а требуется загрузить файл внушительных размеров или просмотреть "тяжелый" веб-

сайт — вы прочитаете советы, как справиться с данной ситуацией, по максимуму сэкономив деньги, в том числе заказав файлы с доставкой на дом и просматривая страницы в оффлайн-режиме. А познакомившись с понятием "фишинг", вы уясните, чем может навредить невнимательное участие в социальных сетях.

Дополнительно

В качестве дополнения вы узнаете о существовании субкультур компьютерного искусства — трекерной музыке, ASCII-графике и демосцене.

Но, самое главное: я вам в примерах покажу, как *искать* и, что важно, *находить* файлы — вы научитесь формировать поисковые запросы. Именно навыки корректного поиска вы почерпнете из этой книги. Как средствами поисковых систем типа Google, так и по FTP-серверам. Что еще важно — вы научитесь осуществлять поиск по трекерам с помощью внешних поисковых средств, т. к. встроенные нередко не выдают должных результатов. Наверняка вы удивитесь, узнав, насколько мощные инструменты скрывает лаконичная страничка Google.

А разобраться в терминах и аббревиатурах как надводной, так и подводной части Интернета позволит небольшой словарь в конце книги.

ГЛАВА 1

Особенности "рыбалки" в Интернете, или как найти все, что хочешь

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 видеофайл — 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 приступать 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 11*, 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 очень важно знать и иметь, прежде чем 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 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"[1]. 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 возможные 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

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

проверяющую на наличие вредоносных объектов сайты по ссылкам, найденным в поисковой системе. Кроме того, вам потребуется специализированное программное обеспечение.

> ***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 оффлайн (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. Загрузить дистрибутив уже нельзя, как было с RC-версиями[1], а вот почитать поподробнее можно на веб-сайте по адресу: **http://www.microsoft.com/rus/windows/windows-7/default.aspx**.
- **Браузер.** Вполне можно, не заморачиваясь, пользоваться встроенным в операционную систему Windows 7 браузером Internet Explorer 8. Загрузить дистрибутив можно с веб-сайта: **http://www.microsoft.com/rus/windows/internet-explorer/**.
- **Антивирусное приложение.** Тут сложно что-то рекомендовать, т. к. каждый пользователь испытывает симпатии к определенному антивирусу. Из платных могу посоветовать Антивирус Касперского 2010 или Kaspersky Internet Security 2010 (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. Антивирус Касперского можно загрузить по адресу: **http://www.kaspersky.ru/**, а программу AVG Anti-Virus Free — на веб-сайте **http://www.avgrussia.ru/lite-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 **http://**

[1] RC — Release candidate.

westbyte.com/dm/. Это практически идеальный продукт, поэтому искать аналогичные утилиты нет смысла.

- **Оффлайн-браузер.** Тут есть из чего выбрать. Можно попробовать в деле две программы с русским интерфейсом: первую и платную, WebCopier, можно загрузить на веб-сайте **http://www.maximumsoft.com/**; вторую и бесплатную, HTTrack, — на веб-сайте **http://www.httrack.com/**.
- **FTP-клиент.** С FTP-серверов загружать файлы позволяет программа Download Master. Когда он бессилен, а также в качестве более удобного инструмента можно порекомендовать платный CuteFTP, который можно загрузить с веб-сайта **http://www.globalscape.com/downloads/**.
- **Торрент-клиент**, необходимый для загрузки по протоколу BitTorrent. Дистрибутив этой программы имеет малый размер и доступен для бесплатной загрузки на веб-сайте **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 **http://dcplusplus.sourceforge.net/download/**.
- **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 безопасности 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. 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 не-

скольких минут до нескольких месяцев. В принципе, больше и не нужно. Если вы, например, регистрируетесь на форуме, вы 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 (**http://itrashmail.com/**), позволяющих создать временный электронный почтовый ящик. В поле ввода **Ящик** нужно указать произвольное название почтового ящика, а в открывающемся списке выбрать один из доступных серверов (на момент написания книги был доступен только один сервер), а затем нажать кнопку **Вход**.

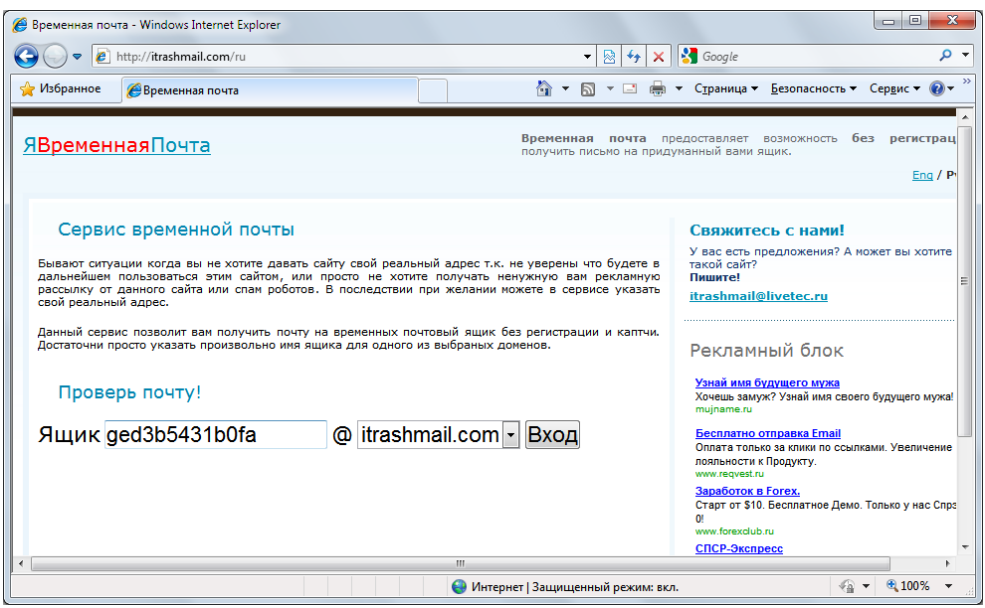

Рис. 1.1. Вид сервиса временной электронной почты

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. Впрочем, если, например, вы использовали в качестве логина (названия

ящика) сочетание ***sitewalker***, то ваш почтовый ящик будет доступен по ссылке **http://itrashmail.com/ru/elist?email=*sitewalker*&domain=*itrashmail.com***. Исходя из содержимого ссылки, вполне можно понять, куда нужно подставить логин, а куда — домен, чтобы получить доступ к почтовому ящику. Режимом слежки на этом сайте называется не что иное, как процесс автоматического обновления содержимого почтового ящика в течение 15 секунд. Для вашего удобства далее я привел небольшую табл. 1.1 со списком доступных на момент написания книги сервисов временной почты.

Таблица 1.1. *20 бесплатных сервисов временной почты*

Название	Адрес в Интернете	Комментарии
10MinuteMail	**http://www.10minutemail.com/**	Почтовый ящик удаляется через 10 минут с возможностью пролонгации
FilzMail	**http://filzmail.com/**	Срок хранения сообщений — 24 часа
GuerrillaMail	**http://www.guerrillamail.com/**	Почтовый ящик удаляется через 15 минут
Jetable.org	**http://www.jetable.org/**	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
MailEater.com	**http://www.maileater.com/**	
Mailinator	**http://www.mailinator.com/**	
MakeMeTheKing	**http://www.makemetheking.com/**	
Melt Mail	**http://meltmail.com/**	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	**http://www.mintemail.com/perfwd/**	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

Таблица 1.1 *(окончание)*

Название	Адрес в Интернете	Комментарии
myTrashMail.com	**http://www.mytrashmail.com/**	Продолжительность жизни — до месяца. Лимит — 4 Мбайт, до 2 Мбайт на одно письмо
Spam.la	**http://www.spam.la/**	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
SpamFree24	**http://spamfree24.org/**	Создание временного почтового ящика на любом из шести доменов на выбор. Сообщения хранятся несколько часов
Spamobox	**http://www.spamobox.com/**	Почтовый ящик удаляется через 60 минут с возможностью пролонгации
TempEMail	**http://www.tempemail.net/**	
Tempinbox	**http://www.tempinbox.com/english/**	Обязательно следует установить флажок, что вы подтверждаете условия соглашения
UnMail.ru	**http://unmail.ru/**	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
Will Hack For Food	**http://wh4f.org/**	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
YOPmail	**http://www.yopmail.com/**	Срок хранения сообщений — 5 дней
Почта для спама	**http://www.mailforspam.com/**	
Явременная почта	**http://itrashmail.com/ru**	

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** 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. Сервис Rambler советовать не буду, т. к. письма приходят с задержкой, а часто и пропадают по пути. Сервис Mail.ru вполне удобен и быстр, лишен недостатков. Самый удобный и безопасный — это, Gmail, соединение с ним идет через зашифрованный протокол https (об этом позже). Также вы можете попробовать следующие адреса: **http://www.nextmail.ru/**, **http://www.pochta.ru/**, **http://www.freemail.ru/**, **http://mail.yandex.ru/**, **http://www.hotmail.ru/** и др.

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 **http://home.live.com/**. Единственно, для использования всех возможностей понадобится потратить несколько минут на веб-сайте **http://www.microsoft.com/rus/liveid/default.aspx**, чтобы создать свой идентификатор Windows LiveID.

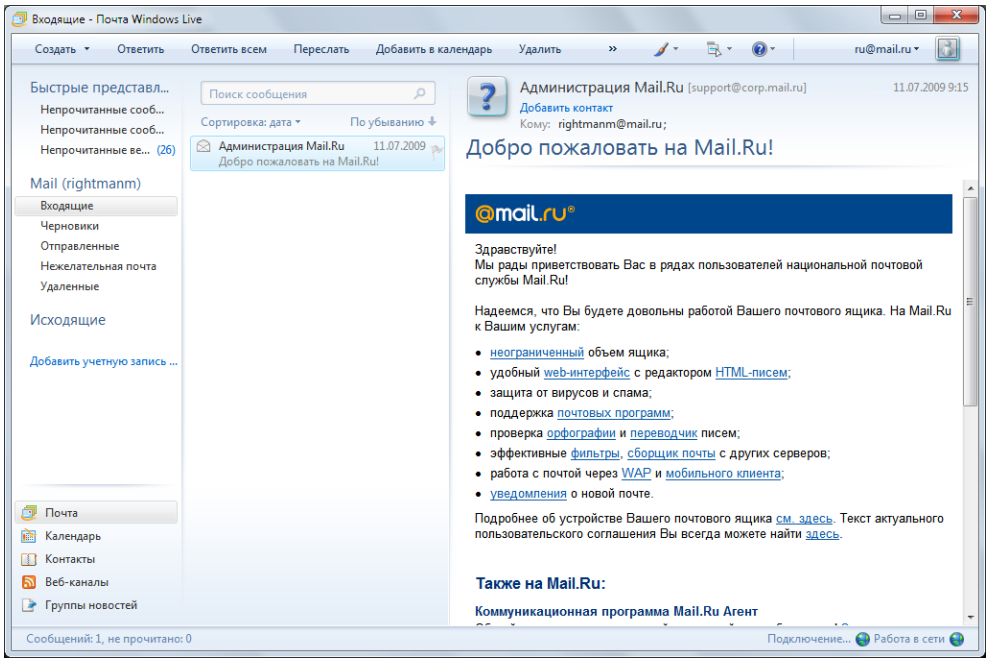

Рис. 1.2. Главное окно программы Почта Windows Live

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);

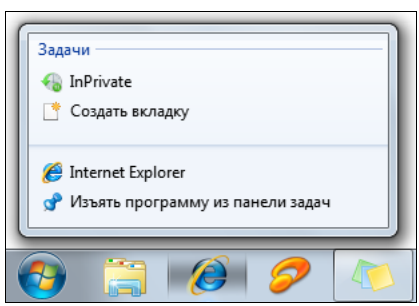

Рис. 1.3. Всплывающий список программы Internet Explorer

- 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>.

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 посещений веб-страниц, данные форм и паролей, содержимое адресной 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.

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 **http://odnoklassniki.ru/** или **http://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 содержимым. В большинстве случаев подобные ограничения можно обойти.

Но прежде, чем 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 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 вебсайтов 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, минуют узлы провайдеров, которыми пользуются оба человека. В том случае, если сообщение отправляется в другую страну, то помимо провайдеров оно минует 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 скомпрометировать, 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"[1] 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 со-

[1] Духовное движение, запрещенное в Китае.

держат различные данные, например, сведения о местоположении пользователя, чтобы при запросе пользователя из России открывать страницу **microsoft.ru**, а не **micorosft.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, выбрав команду меню **Безопасность | Удалить журнал обозревателя** (Safety | Delete Browsing History) и в открывшемся диалоговом окне установив флажок **Файлы "cookie"** (Cookies) (рис. 1.4). После нажатия кнопки **Удалить** (Delete) временные файлы Интернета, включая файлы cookies, будут удалены.

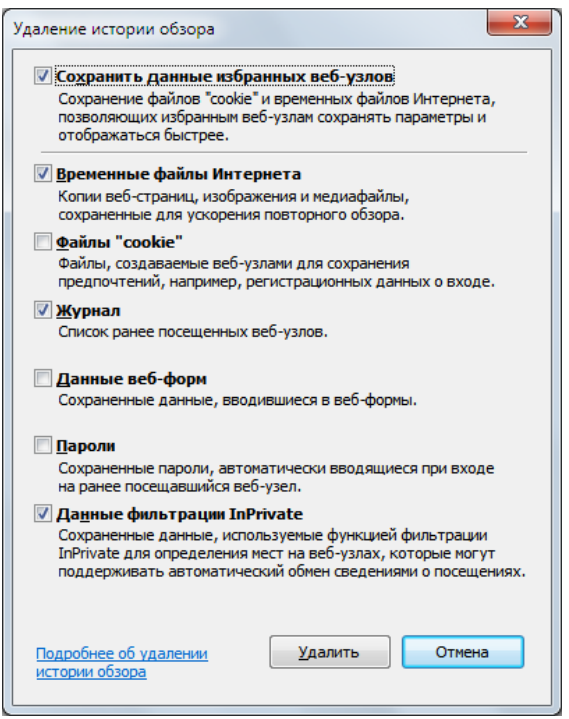

Рис. 1.4. Диалоговое окно **Удаление истории обзора**

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 взором Большого Брата (смайл)) и соблюдать правила наподобие "не разжигать национальную рознь", "не нарушать авторские права" и т. п.

Интернет-цензура и фильтры: как попасть туда, куда доступ ограничен или заблокирован

В этом разделе 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.

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. Для примера я расскажу, как открыть доступ к форме регистрации на веб-сайте **http://www.bikermatch.co.uk/**, регистрироваться на котором могут только обладатели IP-адресов Великобритании, т. е. предположительно жители туманного Альбиона. Запускаю браузер Internet Explorer и пытаюсь получить доступ к веб-сайту **http://www.bikermatch.co.uk/**. Загрузка происходит нормально. Перехожу в раздел **Full search** (Полный поиск) — открывается страница с сообщением, что требуется регистрация, совершенно бесплатная. Щелкаю мышью на ссылке **Join Free** (Присоединиться бесплатно)... Упс, я и не догадывался, что живу в России (смайл) (рис. 1.5).

Рис. 1.5. Доступ с моим IP-адресом запрещен

Как видно из содержимого страниц, посещать ресурс могут только пользователи из Великобритании. Полужирным начертанием выделено ваше (на рисунке — мое) местонахождение.

Определение собственного IP-адреса

Определить собственный IP-адрес вы можете, например, на веб-сайтах **http://2ip.ru/**, **http://www.myip.ru/** или **http://www.whoer.net/ext**. Также вы можете заходить на подобные веб-сайты через прокси-сервер, чтобы убедиться, что ваш IP-адрес действительно заменен.

Попробую использовать прокси-сервер, через который проложит путь запрос от моего компьютера к серверу **http://www.bikermatch.co.uk/**. 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.

Самый простой вариант прокси-сервера — это CGI-прокси или "анонимайзеры", веб-сайты которых сразу содержат 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 proxy" или "анонимайзер" в поисковой строке веб-сайта Google или Яндекс. На момент написания книги вполне нормально функционировали **http://anonymouse.org/**, **http://www.hidemyass.com/** и **http://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 я вам не скажу — учитесь пользоваться поиском.

Существуют как бесплатные, так и платные CGI-прокси. Недостаток 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 **http://www.proxer.ru/** (рис. 1.6).

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!**.

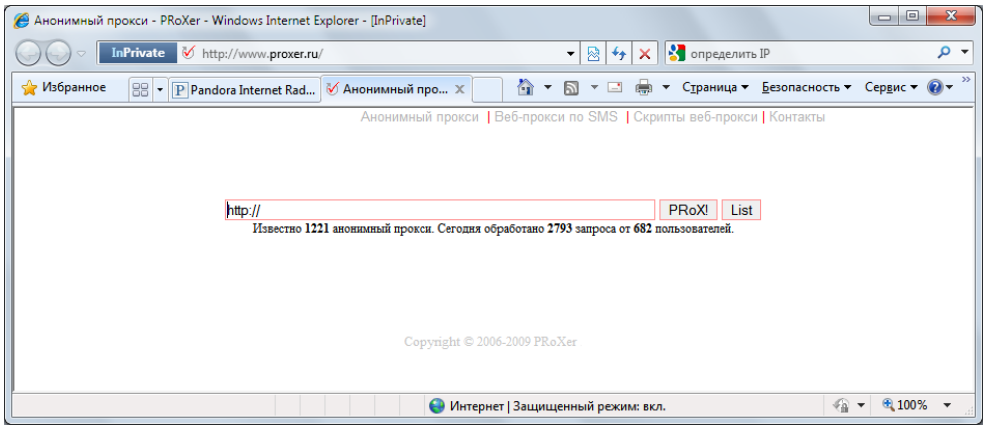

Рис. 1.6. Веб-сайт PRoXer

Будет автоматически предложен один из доступных прокси-серверов, а затем произойдет автоматическое перенаправление на него (не забудьте включить всплывающие окна). Я же воспользуюсь списком, чтобы выбрать прокси-сервер, расположенный в Великобритании, т. к. другие локации сервисом **http://www.bikermatch.co.uk/** игнорируются. После ввода адреса (без этого список не выводится, а происходит редирект на главную страницу) и нажатия кнопки **List** вы увидите список прокси-серверов (рис. 1.7).

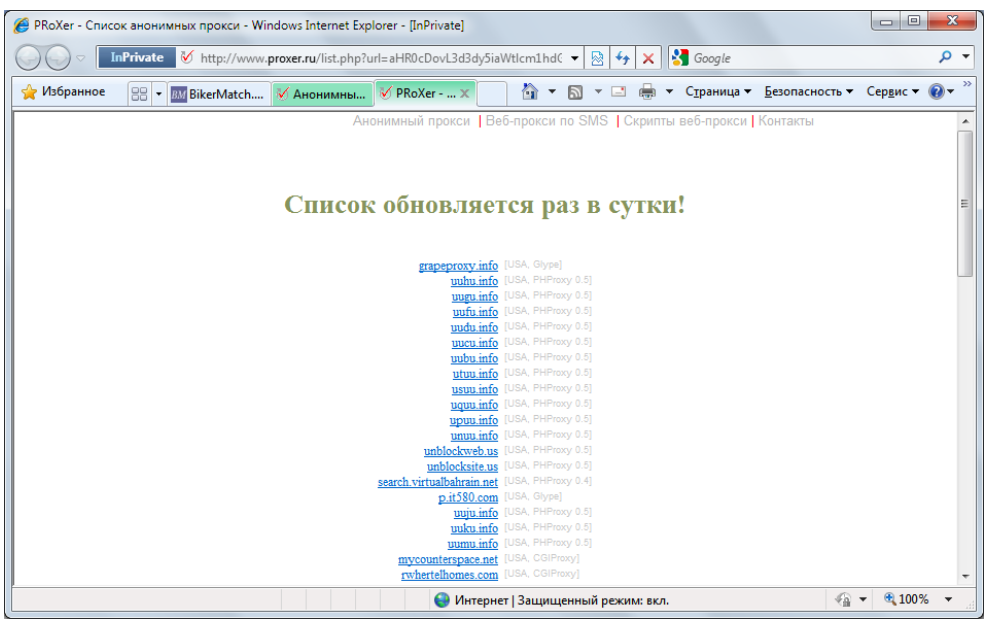

Рис. 1.7. Список предлагаемых прокси-серверов

Ради интереса, попробую выбрать прокси-сервер, расположенный, допустим, в Нидерландах. Попался **http://jailbreaked.net/**: в строку ввожу адрес **http://www.bikermatch.co.uk/** и нажимаю кнопку **Surf** (рис. 1.8).

Рис. 1.8. Вид страницы ресурса **http://www.bikermatch.co.uk/**

Произвожу тот же порядок действий: перехожу в раздел **Full Search** (Полный поиск), а затем щелкаю мышью на ссылке **Join Free** (Присоединиться бесплатно). Что и требовалось доказать — теперь я житель цветочной и свободной Голландии. Но результат, тем не менее, не достигнут, доступа к веб-сайту все равно нет. Теперь я выберу из списка английский прокси-сервер, допустим, **http://awemazing.co.uk/**.

Указав в строке ввода адрес — **http://www.bikermatch.co.uk/** — и нажав кнопку **Go** (Перейти), получаю доступ к искомому веб-сайту. Перехожу в раздел **Full Search** (Полный поиск), а затем щелкаю мышью на ссылке **Join Free** (Присоединиться бесплатно) (рис. 1.9).

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

Получение рассылки с адресами прокси-серверов

Вы можете подписаться на рассылку списка адресов прокси-серверов на веб-сайте **http://www.peacefire.org/circumventor/**. Периодичность поступления обновленных списков — 3—4 дня.

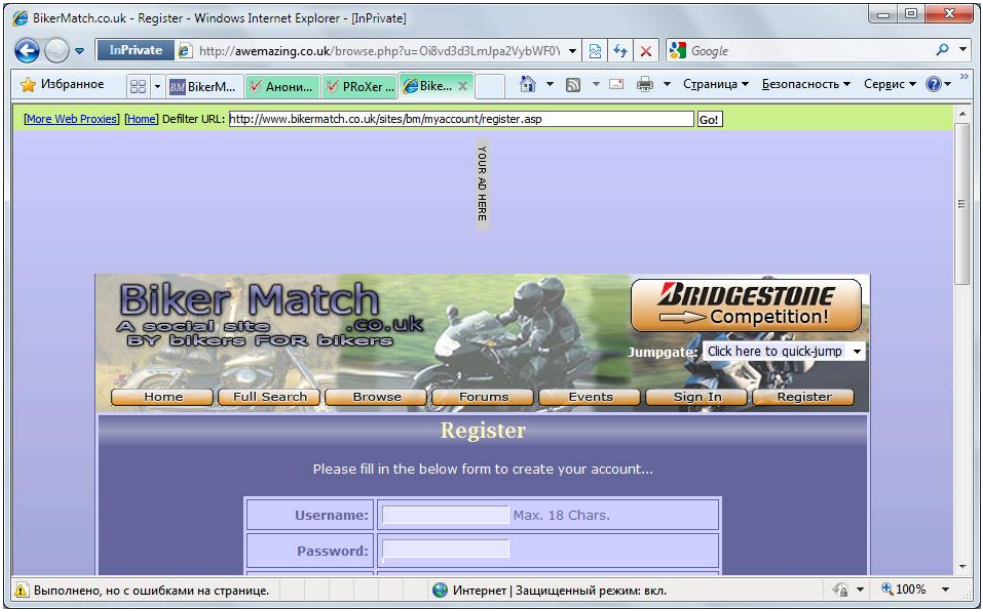

Рис. 1.9. Доступ к регистрационной форме получен

Важно иметь в виду, что сам факт вашего обращения к прокси-серверу тайной для администратора не является, ровно 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 HTTP-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 выше, или же просмотреть сведения о "себе" с помощью специализированных сайтов типа **http://www.stilllistener.addr.com/checkpoint1/index.shtml** или **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. 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. 1.10).

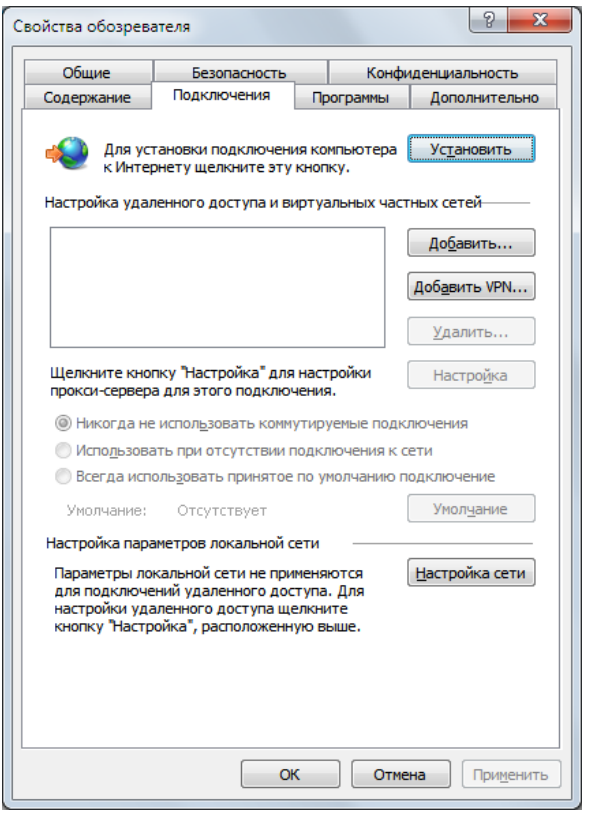

Рис. 1.10. Диалоговое окно **Свойства обозревателя**

3. Нажмите кнопку **Настройка сети** (LAN Settings). Откроется диалоговое окно **Настройка параметров локальной сети** (Local Area Network (LAN) Settings) — рис. 1.11.

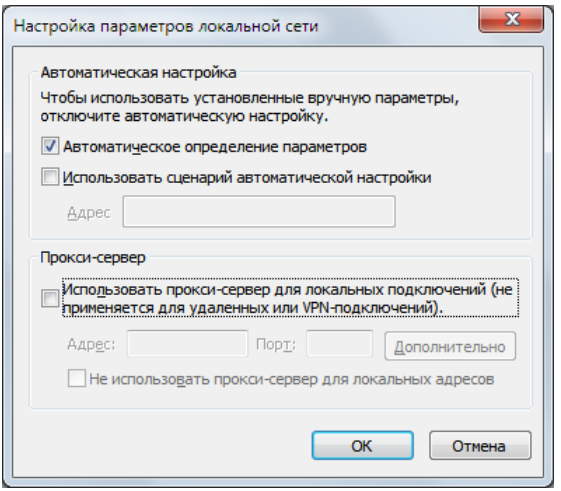

Рис. 1.11. Диалоговое окно **Настройка параметров локальной сети**

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.
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 пущего шифрования можно использовать цепочки прокси, например, указав в свойствах браузера подключение через http-прокси, загрузите искомую страницу не напрямую, а че-

рез "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 средства связи остались в совершенно незашифрованном виде. Для обеспечения более высокого уровня анонимности можно воспользоваться услугами целой анонимной сети, такой как Tor. Об анонимной сети Tor я расскажу в последней главе этой книги.

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

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

Чаще всего посредством "анонимайзеров" пользователи пытаются получить доступ к веб-сайтам типа **http://odnoklassniki.ru/** и **http://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 **http://xy4me.ru/** и **http://.zapretanet.ru/**. Сомнительно, что сайты с платным хостингом будут бесплатно предлагать услуги пользователям по предоставлению доступа к социальным сетям, если таковой заблокирован. Вполне вероятно, что генерируемые на этих веб-сайтах ссылки — не что иное, как прямой путь на фишинг-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. 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: **http://odnoklassniki.ru/**, а не **http://odnaklassniki.ru/**, **http://odn0klassniki.ru/** или вообще **http://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!

Смена расширения: как обойти ограничения администратора и прокси-сервера

Надеюсь, некоторые советы в предыдущем разделе 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 (**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 ди́чка 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. 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