Алексей Гладкий
Безопасность и анонимность работы в Интернете
Как защитить компьютер от любых посягательств извне

Введение

Вопрос обеспечения безопасности и анонимности своего пребывания в Интернете волнует многих пользователей: ведь это позволяет заходить на любые сайты, свободно общаться и работать, получать доступ к веб-ресурсам, которые закрыты для обычного доступа (например, заблокированы системным администратором), отправлять анонимные почтовые сообщения, и т. д. В любом случае, в Сети лучше не оставлять следов своего пребывания — этим могут воспользоваться те же злоумышленники.

Кстати, в последние годы мошенничество в Интернете цветет махровым цветом, а количество обманутых и пострадавших от него людей растет не по дням, а по часам. Хищение денег, кража конфиденциальной информации, вымогательство, откровенный обман и элементарное «кидалово» — несть числа приемам и способам, которыми

оперируют современные Остапы Бендеры для «сравнительно честного отъема денег у населения».

Причем далеко не всегда они действуют нагло и стремительно (хотя такого тоже хватает). Современный интернет-злоумышленник умеет расположить к себе потенциальную жертву, и вызвать полное доверие к себе. Когда же наступает «прозрение» и жертва осознает, что ее обманули — предпринимать что-либо очень сложно, а зачастую — почти нереально.

Лучший способ обезопасить себя от интернет-мошенников состоит в том, чтобы не попадаться на их уловки. И в этой книге, помимо прочего, мы расскажем о некоторых распространенных способах, которыми пользуются злоумышленники с целью обмана излишне доверчивых граждан.

Глава 1. Общие сведения о работе в Интернете

Интернет давно и прочно проник в нашу жизнь, и без него уже невозможно представить существование человечества. Им активно пользуются представители самых разных слоев нашего общества — независимо от возраста, рода занятий, профессиональной принадлежности, социального положения и иных факторов. Более

того — многие приобретают себе компьютер исключительно для того, чтобы иметь постоянный доступ к Интернету.

Однако вначале необходимо усвоить несколько рекомендаций и правил, которые неукоснительно должен соблюдать каждый пользователь Всемирной Паутины. Об этом и пойдет речь в первом разделе данной главы.

Рекомендации по Интернет-безопасности

Каждый пользователь Интернета должен четко осознавать, что Интернет может не только принести пользу, но и причинить немалый вред. Чтобы избежать неприятностей, строго соблюдайте перечисленные ниже рекомендации и правила.

♦ Для безопасной работы в Интернете обязательно наличие хорошей антивирусной программы. При этом необходимо, чтобы установленный антивирус мог работать в режиме мониторинга — это позволит выявлять опасность сразу при ее возникновении.

♦ Стоит соблюдать предельную осторожность при посещении неизвестных ресурсов в Интернете. В настоящее время получили распространение вирусы и вредоносные программы, для заражения которыми достаточно просто посетить

определенную веб-страницу.

♦ Если вы подключены к Интернету через телефонную линию, динамик модема должен быть включен. Это позволит своевременно выявить попытки сетевых злоумышленников подключить данный компьютер к тому или иному ресурсу путем набора заданного телефонного номера (часто это практикуют распространители порнографических сайтов и услуг аналогичного характера). Если в процессе работы слышно, что модем начал произвольно набирать какой-то номер без участия пользователя, необходимо немедленно отключиться от Сети путем отсоединения сетевого кабеля. После этого нужно проверить компьютер специальной программой категории Antispyware — скорее всего, в компьютер внедрен шпионский модуль автоматического дозвона.

♦ После скачивания из Интернета файлов, архивов и т. п. необходимо сразу же проверить их антивирусной программой, и лишь после этого запускать на выполнение, распаковывать и т. д. Многие вирусы и вредоносные программы могут представлять собой исполняемый файл либо архив.

♦ Почтовые письма, полученные от неизвестных и сомнительных отправителей, перед открытием нужно обязательно проверить хорошей антивирусной программой (с обновленными антивирусными базами). Если этого не делать, то

можно в короткие сроки превратить свой компьютер в рассадник вирусов.

♦ Никогда не отвечайте на письма, в которых содержится просьба прислать конфиденциальные данные (логин, пароль и т. п.) по указанному адресу. С помощью такого нехитрого приема злоумышленники завладевают чужими логинами и паролями.

♦ Также настоятельно не рекомендуется отвечать на письма, которые являются спамом — в противном случае спамер будет знать, что ваш почтовый ящик функционирует (а это важная информация для любого спамера). В результате количество получаемого спама будет многократно увеличиваться.

♦ Если при посещении различных ресурсов в Интернете (форумы, порталы, сайты и т. д.) требуется оставить о себе некоторые данные, то такая информация должна быть минимальна (например, совершенно необязательно сообщать свои паспортные данные, домашний адрес, различные пароли и т. п.). Несмотря на то, что на многих Интернет-ресурсах гарантируется полная конфиденциальность, не стоит быть наивным — если кому-то надо получить эту информацию, он ее получит. Причем варианты утечки информации могут быть самыми разными. Кто же может получить конфиденциальную информацию?

• Хакер. Он просто взломает систему защиты сайта либо портала (или сотворит нечто подобное).

• Шантажист. Если кто-то заводит в Интернете различные фривольные знакомства, указывая при этом в качестве средства связи номер телефона либо адрес основного почтового ящика, то по этим данным легко собрать на человека компромат. Это достигается за счет широких возможностей современных мощных поисковых систем.

• Лицо (или группа лиц), собирающее информацию индивидуального характера о людях (например, те же паспортные данные). В этом случае будет заинтересован (чаще всего — подкуплен) сотрудник портала, имеющий доступ к этим данным. В результате через некоторое время беспечный пользователь узнает (как правило, от правоохранительных органов), что, например, на его паспортные данные открыта оффшорная (ищи еще какая-нибудь) фирма, через которую каждый день «отмывается» десяток-другой миллионов долларов. Нетрудно догадаться, что ответственность за все это ляжет именно на пользователя, который легкомысленно доверил свои личные данные администрации Интернет-ресурса.

• Представитель известных силовых структур. Он просто свяжется с администрацией сайта

(портала) и вежливо попросит предоставить ему всю информацию о зарегистрировавшихся на сайте пользователях (и, разумеется, получит ее в кратчайшие сроки).

♦ По окончании работы в Интернете всегда отключайте сетевой кабель от телефонной линии или от локальной сети.

А вообще одним из главных правил работы в Интернете является постоянная бдительность. Помните: то, что вы видите на экране монитора — это лишь верхушка айсберга, и от ваших глаз скрыто огромное количество происходящих процессов, многие из которых имеют откровенно деструктивную направленность.

Как отредактировать параметры подключения к Интернету

Иногда в процессе работы возникает необходимость изменить те или иные параметры созданного ранее подключения к Интернету. Характерные примеры — изменение телефонного номера, через который осуществляется подключение, учетных данных, и т. п.

Чтобы перейти в режим просмотра и редактирования свойств подключения, необходимо в окне подключения нажать кнопку Свойства. Можно также в списке подключений щелкнуть на

значке подключения правой кнопкой мыши и в открывшемся контекстном меню выбрать команду Свойства. При выполнении любого из этих действий отобразится окно, которое показано на рис. 1.1.

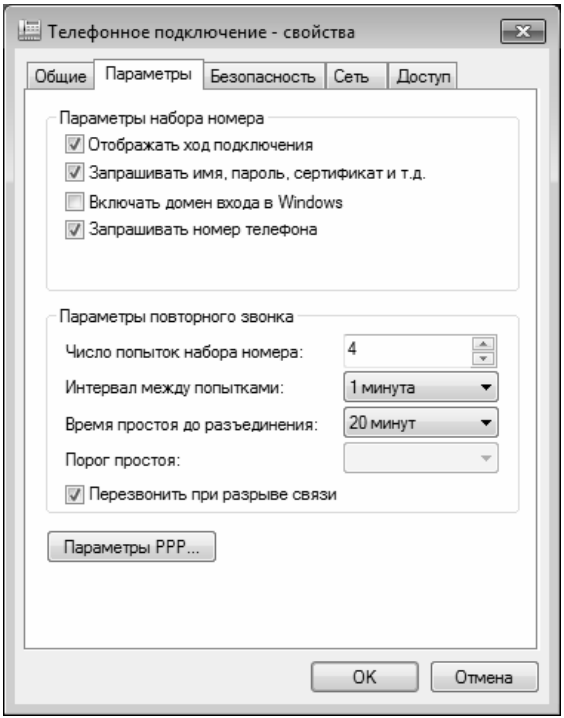

Рис. 1.1. Просмотр и редактирование свойств подключения к Интернету

Как видно на рисунке, это окно содержит

несколько вкладок. Каждая из этих вкладок содержит однотипные, сходные по назначению и функциональности параметры настройки. Рассмотрим некоторые наиболее востребованные у большинства пользователей параметры.

На вкладке Общие отображается название устройства, с помощью которого осуществляется подключение к Интернету (модема) и общие параметры подключения. Кнопка Настроить (она доступна для подключений через телефонную линию) позволяет открыть режим настройки параметров работы модема. При этом на экран выводится окно Конфигурация модема, в котором определяется максимальная скорость работы модема, а также с помощью соответствующих флажков включается/выключается аппаратное управление потоком, обработка ошибок и сжатие данных модемом. Слева внизу данного окна находится флажок Включить динамик модема, который обязательно нужно установить.

Параметры набора номера телефона (они также отображаются только для телефонных подключений) включают в себя поле Номер телефона (именно по этому номеру производится выход в Интернет), а также поля Код города и Код страны или региона, которые доступны только при установленном флажке Использовать правила набора номера. С помощью кнопки Другие можно

перейти в режим настройки дополнительных телефонных номеров, которые могут использоваться в данном подключении. При этом на экране отображается окно Дополнительные номера телефонов, изображенное на рис. 1.2.

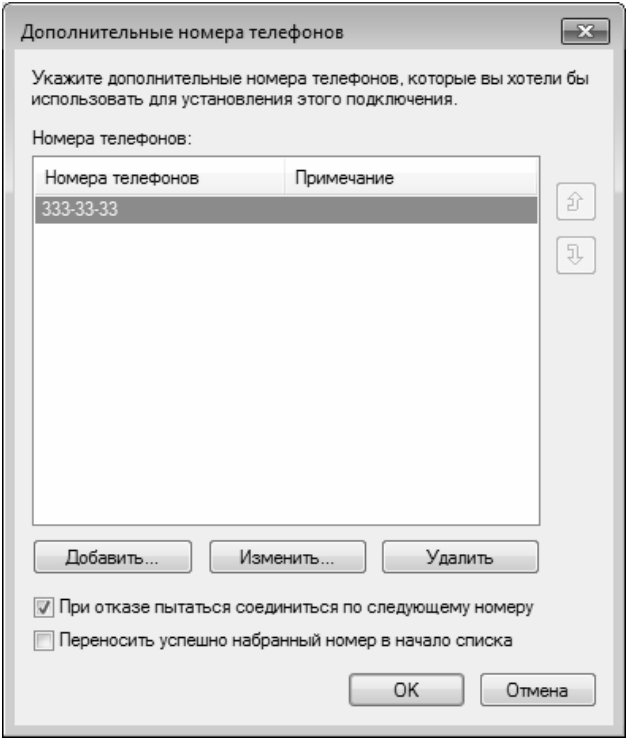

Рис. 1.2. Настройка дополнительных телефонных номеров

В данном окне с помощью кнопок Добавить, Изменить и Удалить осуществляется соответственно добавление новых номеров, редактирование и удаление из списка текущего номера. В режиме добавления либо изменения телефонных номеров можно ввести с клавиатуры произвольный комментарий.

С помощью установки соответствующих флажков можно включить режим соединения по следующему номеру в случае сбоя при первоначальном соединении, а также режим переноса успешно набранного номера в начало списка (использование данных режимов имеет смысл только в том случае, когда список содержит более чем один телефонный номер).

На вкладке Параметры (см. рис. 1.1) производится настройка параметров набора номера и повторного звонка. В выделенной области Параметры набора номера содержатся следующие флажки:

♦ Отображать ход подключения — при установленном данном флажке процесс подключения сопровождается появлением на экране информационных окон, в которых последовательно отображаются этапы подключения (набор номера, регистрация компьютера в сети и др.);

♦ Запрашивать имя, пароль, сертификат и

т. д. — если данный флажок установлен, то перед соединением система запросит подтверждение имени пользователя, пароля и иных параметров защиты (при их наличии);

♦ Включать домен входа в Windows — если данный флажок установлен, то перед соединением система запросит имя домена. Установка данного флажка срабатывает только при установленном флажке Запрашивать имя, пароль, сертификат и т. д.;

♦ Запрашивать номер телефона — если данный флажок установлен, то перед соединением система запросит подтверждение номера телефона. Данный параметр отображается только для телефонных подключений.

В выделенной области Параметры повторного звонка (см. рис. 1.1) настраиваются следующие параметры:

♦ Число попыток набора номера — в данном поле указывается количество попыток автоматического подключения, когда с первого раза соединиться не удается;

♦ Интервал между попытками — в данном поле указывается промежуток времени, через который производится очередная попытка подключения. Использование данного параметра имеет смысл в том случае, когда в поле Число повторений набора номера указано любое значение,

кроме 0;

♦ Время простоя до разъединения — через промежуток времени, указанный в данном поле, соединение будет разорвано при условии простоя компьютера.

Если установлен флажок Перезвонить при разрыве связи, то при непреднамеренном разрыве соединения будет производиться автоматическое подключение для восстановления соединения.

Что делать, если отсутствует связь с Интернетом

Каждый пользователь Интернета хотя бы раз сталкивался с ситуацией, когда по каким-то причинам Интернет был недоступен или скорость передачи данных неоправданно снижалась. Далее мы рассмотрим наиболее характерные причины подобных явлений, а также проанализируем сообщения об ошибках, выдаваемых операционной системой при возникновении проблем с Интернетом.

Причины отсутствия доступа к Сети

Одно из распространенных явлений — когда попытка соединиться с Интернетом по телефонной сети заканчивается неудачей уже на стадии набора

телефонного номера модемом. Обычно это происходит в случаях, когда модем либо не подключен к телефонной линии (возможно, для решения проблемы будет достаточно просто вставить штекер телефонного провода в соответствующий разъем), либо не настроен, либо используется другим приложением. Отметим, что в первом случае модем обычно начинает набор номера, и только после этого сообщает об отсутствии связи. Если телефонный номер для выхода в Интернет начинается с «восьмерки» (по аналогии с тем, как это делается для выполнения междугородних звонков) — то сообщение об отсутствии гудка может появиться как до, так и после набора «восьмерки» модемом.

Чтобы диагностировать неполадку, откройте Диспетчер устройств, дважды щелкните в дереве устройств на позиции модема, затем в открывшемся окне откройте вкладку Диагностика и нажмите кнопку Опросить модем. Если модем настроен правильно, через некоторое время (обычно — в пределах нескольких секунд) на экране отобразится результат опроса. Если ничего не получилось — перезагрузите компьютер и выполните данную операцию повторно.

Иногда обрыв связи случается в процессе набора телефонного номера. Как показывает практика, в большинстве случаев это происходит по

вине провайдера. Попробуйте позвонить по номеру, используемому для доступа в Интернет, с обычного аппарата. Если вы не смогли дозвониться (короткие гудки или вообще нет ответа), либо дозвониться получилось, но характерный звук работающего модема не слышен — значит, сбой возникает либо по причине проблем с телефонной линией, либо модем провайдера не работает либо перегружен.

Если же вы смогли дозвониться провайдеру — значит, проблема на вашей стороне. В этом случае следует проверить настройки подключения к Интернету, в частности — правильно ли указан телефонный номер для соединения в Интернетом. Есть и еще один важный нюанс: если АТС, через которую вы выходите в Интернет, не поддерживает тональный набор телефонных номеров — нужно в настройках подключения добавить перед номером телефона латинскую букву P и попробовать соединиться вновь.

Почти все модемы имеют динамик, с помощью которого пользователь прослушивает процесс набора номера и подключения к Интернету. Некоторые пользователи умеют на слух определить набор номера и ответ модема провайдера, благодаря чему они могут с высокой степенью достоверности диагностировать неполадку.

Также на стадии набора номера связь может

обрываться по причине неполадок и помех на телефонной линии, либо из-за неправильных настроек модема.

Еще одна распространенная ситуация заключается в том, что само соединение появляется, но при проверке учетных данных (логина и пароля) связь самопроизвольно обрывается.

Если ранее вы подключались к Интернету под своими учетными данными, которые сохранены в системе, и при этом их проверка занимала много времени — перезагрузите компьютер и попробуйте соединиться еще раз. Если же учетные данные вводятся при каждом подключении — проверьте, правильно ли вы их вводите. При этом проверьте регистр символов (при вводе учетных данных прописные и строчные буквы различаются), а также убедитесь в том, что режим Caps Lock отключен. Также проверьте раскладку клавиатуры (возможно, вы вводите учетные данные русскими буквами).

И еще одна распространенная причина, по которой соединение разрывается на этапе проверки учетных данных — это отсутствие денежных средств на счету пользователя.

Бывают случаи, когда подключение к Интернету происходит без проблем, но вот сервисами воспользоваться невозможно (система выдает информационное сообщение об ошибке). Такое может происходить по причине отсутствия

TCP/IP-соединения. В первую очередь проверьте правильность настроек данного подключения к Интернету. Для проверки наличия соединения нужно в окне Запуск программы, которое вызывается с помощью команды Пуск ▸ Выполнить, ввести значение ping google.com. Если соединение функционирует исправно, то вы должны получить примерно следующий ответ (может отличаться IP-адрес и время):

Обмен пакетами с google.com [74.125.232.18] с 32 байтами данных;

Ответ от 74.125.232.18: число байт=32 время=214мс TTL=250;

Ответ от 74.125.232.18: число байт=32 время=2214мс TTL=250;

Ответ от 74.125.232.18: число байт=32 время=2514мс TTL=250;

Ответ от 74.125.232.18: число байт=32 время=236мс TTL=250.

При отсутствии соединения вы получите следующий ответ: Неизвестный IP-адрес google.com.

Иногда соединение бывает нестабильным или не устанавливается вообще, оно часто разъединяется, а скорость работы необъяснимо мала. Обычно причина кроется в плохом качестве телефонной сети или в некорректных настройках самого модема. Часто такое можно заметить при

попытке подключения через старую аналоговую телефонную станцию. Для устранения неполадки установите оптимальные настройки модема, которые лучше всего подходят для данной телефонной линии. В частности, при плохом качестве подключения на скорости 33,6 Кбит/с можно уменьшить ее, соответствующим образом откорректировав параметры настройки модема. Для этого в настройках подключения на вкладке Общие нажмите кнопку настройки модема, и в появившемся окне измените значение параметра Наибольшая скорость. При уменьшении скорости передачи данных можно добиться более стабильной работы соединения.

Если при попытке соединения на экране отображается следующее информационное сообщение: «Ошибка при соединении с сервером» или «Модем не был обнаружен», еще до того, как модем успевает набрать телефонный номер — вероятно, появились неполадки с настройкой удаленного доступа к операционной системе. В такой ситуации проблему можно решить путем переустановки данного компонента системы.

Расшифровка кодов ошибок удаленного доступа

Если при попытках подключения к Интернету возникают проблемы, то на экране отображается не только сообщение об ошибке, но и ее код. Этот код позволяет с высокой степенью достоверности установить истинную причину неисправности, и определить методы ее устранения. Далее мы приведем расшифровку кодов наиболее часто встречающихся при подключении к Интернету ошибок.

♦ 600 Начатая операция не закончена — сообщение свидетельствует о том, что произошла внутренняя ошибка. Для устранения проблемы обычно бывает достаточно перезагрузить систему.

♦ 602 Указанный порт уже открыт — в данном случае COM-порт, через который обычно происходит подключение, уже занят другим процессом, подключением или приложением (например, это может быть программа, которая используется для отправки факсов). В данном случае проблема решается закрытием программы, которая заняла COM-порт.

♦ 606 Указанный порт не подключен — здесь также причина кроется во внутренней ошибке, для устранения которой достаточно перезагрузить систему. В некоторых случаях перезагрузка может

и не потребоваться — при попытке повторного подключения все проходит нормально.

♦ 628 Подключение было закрыто — если данное сообщение появилось при попытке подключения через телефонную сеть, то попробуйте соединиться еще пару раз. Если все повторяется — отключите дополнительные настройки модема и уменьшите его скорость.

♦ 629 Подключение было закрыто удаленным компьютером — в данном случае причины ошибки могут быть разными: это и помехи на линии, и непоправимая ошибка в телефонной сети, и неудавшаяся попытка соединения с удаленным модемом на текущей скорости. Попробуйте дозвониться еще раз, нажав кнопку Перенабрать. Если все повторилось вновь — уменьшите скорость подключения модема до 9,6 Кбит/с, и попытайтесь соединиться вновь. Иногда прояснить ситуацию можно, попробовав подключиться к удаленному модему через другую телефонную линию.

♦ 634 Не удалось зарегистрировать компьютер в удаленной сети — этот сообщение говорит о том, что ваш компьютер не получается зарегистрировать в Сети. Как правило, это происходит при наличии проблем с протоколом NetBIOS, но иногда такую ошибку вызывают также сбои с протоколами TCP/IP или IPX. Причиной обычно является то, что данный IP-адрес уже кем-то занят в Интернете. Для

устранения проблемы обращайтесь к своему Интернет-провайдеру.

♦ 636 Устройство, подключенное к порту, не соответствует ожидаемому — такое сообщение выдается в случаях, когда аппаратная часть вашего компьютера несовместима с настройками конфигурации для подключения. Обычно это происходит после экспериментов с «железом», в частности — когда было заменено какое-то сетевое оборудование (модем или последовательный порт). В данном случае рекомендуется проверить настройки и конфигурацию удаленного доступа к сети.

♦ 646 Вход в это время дня для пользователя с данной учетной записью не разрешен — это сообщение говорит о том, что пользователь имеет доступ в Интернет только в определенное время суток, и в данный момент ему доступ закрыт.

♦ 647 Учетная запись отключена — данное сообщение свидетельствует о блокировке данной учетной записи. Проблему можно решить только через провайдера — возможно, администратор закрыл пользователю доступ за неуплату или по причине совершения пользователем каких-либо нарушений (например, рассылка спама, и др.).

♦ 676 Телефонная линия занята — это сообщение дополнительных пояснений не требует. В данном случае либо повторно вручную запустите

процесс набора номера, либо в настройках подключения установите режим автоматического дозвона.

♦ 678 Ответ не получен — в данном случае проблема может быть как на вашей стороне, так и на стороне провайдера. Причина в том, что модем или другое устройство не отвечает на телефонный звонок, следовательно — соединение установить не удается. Если номер телефона в настройках подключения указан верно, а телефонный кабель вставлен в то гнездо, в которое нужно — скорее всего, проблема на стороне провайдера.

♦ 680 Отсутствует гудок — это сообщение также особых пояснений не требует. Видимо, модем просто не подключен к телефонной сети.

♦ 691 Доступ запрещен, поскольку такие имя пользователя и пароль недопустимы в этом домене — такое сообщение появляется при наличии проблем с учетными данными. В первую очередь проверьте правильность их ввода, а также раскладку клавиатуры и режим Caps Lock. Не исключено, что истек срок действия ваших учетных данных (например, закончился период оплаченного доступа к Интернету, и др.).

♦ 720 Попытка подключения не удалась, поскольку подключенному и локальному компьютерам не удалось согласовать управляющие протоколы PPP — это сообщение информирует об

отсутствии сетевых протоколов управления PPP, настроенных для данного подключения. Такое же сообщение появится и в том случае, когда соответствующий сетевой протокол вообще не был установлен. Подобный сбой может появляться после корректировки сетевого протокола при обновлении ПО.

♦ 721 Удаленный компьютер не отвечает — такое сообщение появляется в случае, когда при попытке начать PPP-диалог ответ с удаленного сервера получен не был. В данном случае проблемы могут быть как на вашей стороне, так и на стороне провайдера.

♦ 736 Удаленный компьютер завершил работу протокола управления — такое сообщение выдается в случае, когда диалог протокола управления каналом PPP начался, но был прекращен удаленным сервером. Как правила, этот сбой возникает по причине неполадок на удаленном компьютере.

♦ 770 Удаленный компьютер отверг попытку подключения — уже из формулировки сообщения об ошибке можно понять, что при попытке подключения что-то не понравилось удаленному компьютеру. Возможно, это настройки вызывающего приложения, либо прочие аппаратные настройки локального компьютера.

♦ 771 Попытка подключиться не удалась,

поскольку сеть перегружена — эта ошибка обусловлена перегрузкой телефонной сети (подобное может возникать и при попытке обычного телефонного звонка). Подождите пару минут и попробуйте подключиться к Интернету повторно.

Как правильно настроить интернет-обозреватель

Безопасность и анонимность работы в Интернете во многом зависят от текущих настроек интернет-обозревателя. Пользователь самостоятельно может выставить требуемые параметры и, тем самым, обеспечить как требуемый уровень безопасности, так и максимально адаптировать программу к своим потребностям. Далее мы расскажем, как выполняется настройка популярных обозревателей Internet Explorer и Mozilla Firefox.

Настройка Internet Explorer

Для перехода в режим настройки параметров Internet Explorer необходимо выполнить команду главного меню Сервис ▸ Параметры. При

активизации данной команды на экране отображается окно, изображенное на рис. 1.3.

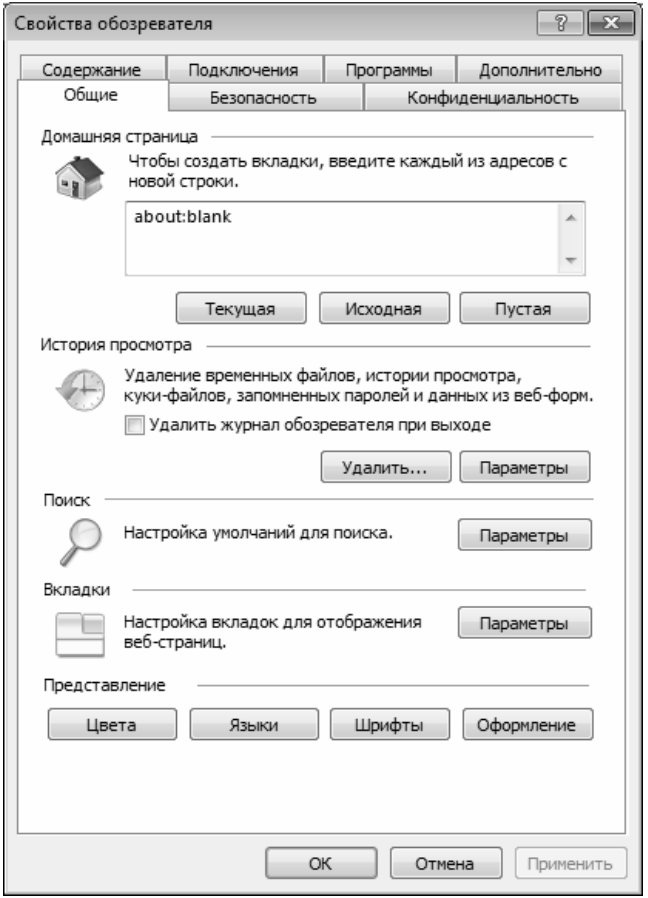

Рис. 1.3. Настройка Internet Explorer

Как видно на рисунке, данное окно состоит из нескольких вкладок. Каждая вкладка содержит параметры настройки соответствующего назначения. Далее мы рассмотрим те параметры, которые являются наиболее востребованными у большинства пользователей.

На вкладке Общие (она открыта на рис. 1.3) выполняется настройка параметров общего назначения.

В верхней части вкладки указывается адрес веб-страницы, которая выбрана пользователем в качестве домашней. Домашняя веб-страница — это страница в Интернете, которая по умолчанию открывается при каждом запуске обозревателя. К данной странице можно вернуться в любой момент, выполнив команду главного меню Вид ▸ Переход ▸ Домашняя страница. Нажатие кнопки Текущая позволяет выбрать в качестве домашней ту страницу, которая открыта в данный момент. Кнопка Исходная восстанавливает в качестве домашней ту страницу, которая была задана при установке интернет-обозревателя. Если домашняя страница не нужна, то следует нажать кнопку Пустая. В этом случае при запуске интернет-обозревателя будет открываться пустая страница.

СОВЕТ

Вы можете выбрать сразу несколько домашних страниц — в этом случае каждая из них будет открываться в отдельной вкладке. Для этого на вкладке Общие сформируйте список страниц, разделяя их нажатием Enter (чтобы каждый новый адрес был введен с новой строки).

Для удаления временных файлов Интернета, истории посещенных веб-страниц и прочей информации предназначена кнопка Удалить. При ее нажатии отображается окно, в котором путем установки соответствующих флажков нужно отметить данные, которые должны быть удалены, и нажать кнопку Удалить.

С помощью кнопки Параметры, которая находится справа от кнопки Удалить, осуществляется переход в режим настройки и редактирования параметров папки временных файлов Интернета. При этом на экране открывается окно Параметры, которое показано на рис. 1.4.

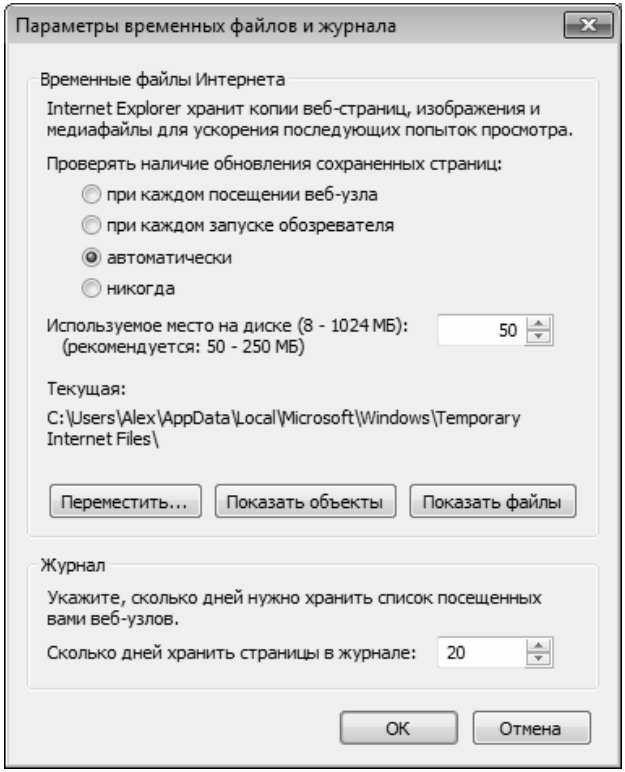

Рис. 1.4. Настройка параметров папки временных файлов Интернета

В данном окне устанавливается требуемый режим проверки обновления сохраненных страниц, отображается расположение папки, содержащей временные файлы Интернета, и указывается

максимальный объем места на жестком диске, предназначенного для этой папки. С помощью кнопки Переместить можно переместить папку временных файлов Интернета в указанное место; при этом на экране открывается окно Обзор папок, в котором следует указать требуемый путь. Для немедленного открытия папки с временными файлами Интернета используйте кнопку Показать файлы.

В поле Сколько дней хранить страницы в журнале указывается количество дней, в течение которых должны храниться ссылки на недавно посещаемые страницы (по умолчанию предлагается хранить их в течение 20 дней).

С помощью кнопки Цвета (см. рис. 1.3) осуществляется переход в режим выбора цветов, предназначенных для отображения веб-страниц. При нажатии на данную кнопку на экране открывается окно, в котором выполняются необходимые действия.

Для настройки параметров шрифтов, используемых при отображении веб-страниц, на вкладке Общие следует воспользоваться кнопкой Шрифты, а для выбора языка — кнопкой Языки. С помощью кнопки Оформление осуществляется переход в режим настройки стиля отображения веб-страницы.

Если говорить непосредственно о параметрах

безопасности работы в Интернете, то ряд из них вынесены на вкладку Безопасность, содержимое которой показано на рис. 1.5.

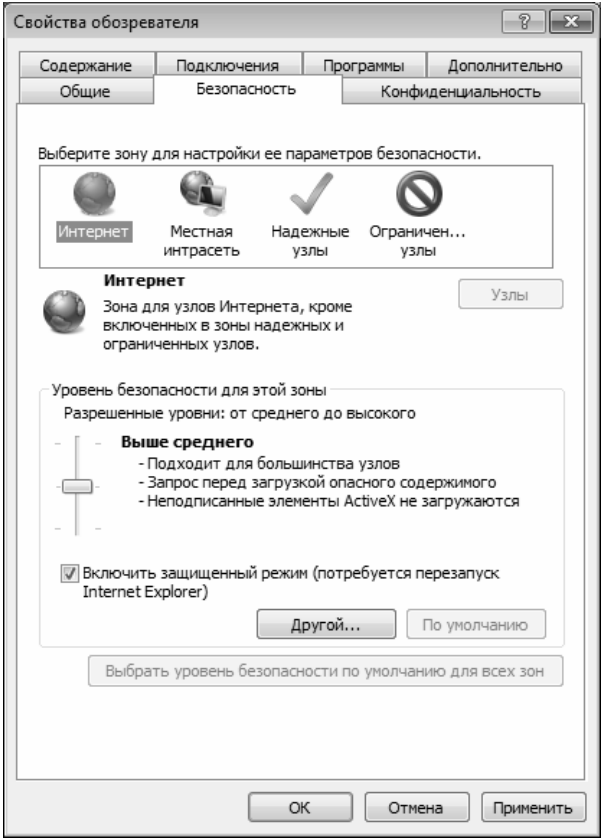

Рис. 1.5. Настройка параметров безопасности

В верхней части данной вкладки приводится перечень зон Интернета, доступных с данного локального компьютера, в нижней — для каждой зоны настраивается уровень безопасности. Для этого следует выделить значок зоны Интернета и с помощью кнопки Другой перейти в режим редактирования уровня безопасности для этой зоны.

При необходимости можно восстановить стандартные параметры безопасности для каждой зоны. Это осуществляется нажатием кнопки По умолчанию (предварительно следует выделить значок той зоны Интернета, для которой выполняется данная операция). Чтобы применить используемые по умолчанию параметры сразу для всех зон, нажмите кнопку Выбрать уровень безопасности по умолчанию для всех зон.

Также некоторые параметры безопасности находятся на вкладке Дополнительно, содержимое которой представлено на рис. 1.6.

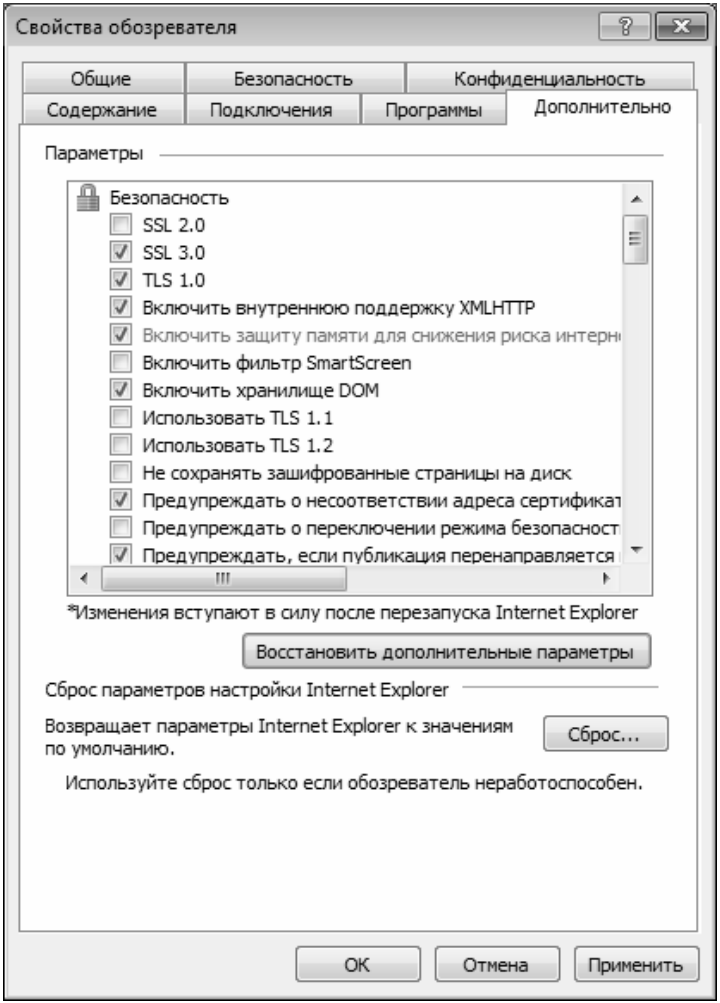

Рис. 1.6. Вкладка Дополнительно

Помимо прочего, здесь с помощью соответствующих флажков можно включать/выключать отображение рисунков и их рамок, воспроизведение анимации, звуков и видео на веб-страницах, использовать автоматическую проверку обновления Internet Explorer и т. д. В отдельный раздел вынесены параметры безопасности. При необходимости можно восстановить значения параметров, предлагаемые системой по умолчанию — для этого следует нажать кнопку Восстановить дополнительные параметры.

Все параметры данной вкладки в зависимости от функционального назначения разделены в группы: Безопасность, Международный, Мультимедиа, Настройка HTTP 1.1, Обзор, Печать и Специальные возможности. Далее мы рассмотрим наиболее значимые параметры, с которыми приходится работать многим пользователям.

Параметры группы Безопасность предназначены для настройки дополнительных параметров безопасности.

♦ SSL 2.0, SSL 3.0 и TLS 1.0 — установка данных флажков включает режим, при котором отправка и получение конфиденциальной информации будет осуществляться с использованием протоколов соответственно SSL 2.0, SSL 3.0 и TLS 1.0. При этом необходимо

учитывать следующее:

• Протокол SSL 2.0 поддерживается всеми безопасными веб-узлами.

• Протокол SSL 3.0 имеет более высокую степень защиты, чем протокол SSL 2.0, но некоторые веб-узлы его не поддерживают.

• Протокол TLS 1.0 имеет степень защиты, сравнимую с протоколом SSL 3.0, и также может поддерживаться не всеми веб-узлами.

♦ Не сохранять зашифрованные страницы на диск — при установке данного флажка включается запрет на сохранение секретных сведений в папке с временными файлами Интернета. Этот режим полезно устанавливать в том случае, когда к компьютеру и к выходу в Интернет имеют доступ несколько пользователей.

♦ Предупреждать о переключении режима безопасности — если установлен этот флажок, то при переключении между безопасными и небезопасными узлами Интернета на экране будет отображаться соответствующее предупреждение.

♦ Проверка подписи для загруженных программ — при установленном данном флажке в Internet Explorer включается режим проверки подлинности загружаемых программ.

♦ Проверят, не отозван ли сертификат сервера — при установке данного флажка Internet Explorer будет выполнять проверку действительности

сертификатов узлов в Интернете. Изменение данного параметра начинает действовать только после перезапуска Internet Explorer.

♦ Удалять все файлы из папки временных файлов Интернета при закрытии обозревателя — если установлен данный флажок, то при закрытии окна Internet Explorer будет выполняться автоматическая очистка папки временных файлов Интернета (эта папка называется Temporary Internet Files).

Группа Мультимедиа включает в себя параметры, определяющие порядок отображения мультимедийного содержимого на веб-страницах. Эти параметры перечислены ниже.

♦ Включить автоматическую подгонку размеров изображения — с помощью данного флажка включается такой режим отображения веб-страниц, при котором слишком большие изображения автоматически подгоняются под размер окна интернет-обозревателя.

♦ Воспроизводить анимацию на веб-страницах — этот флажок используется для включения/выключения режима воспроизведения анимации на веб-страницах. Необходимость данного параметра (кстати, его изменение вступает в силу после перезапуска Internet Explorer) обусловлена тем, что некоторые веб-страницы, содержащие анимацию, загружаются очень

медленно, поэтому ее воспроизведение иногда имеет смысл отключить.

♦ Воспроизводить звуки на веб-страницах — с помощью этого флажка вы можете включать/выключать воспроизведение звуковых файлов на веб-страницах.

♦ Показывать изображения — с целью ускорения загрузки веб-страниц можно отключить режим отображения графических изображений путем снятия данного флажка.

♦ Показывать рамки рисунков — если данный флажок установлен, то во время загрузки рисунков будут отображаться их рамки. Это позволит получить представление о расположении элементов веб-страницы до ее полной загрузки. Включение данного режима имеет смысл только при установленном флажке Отображать рисунки.

♦ Улучшенная передача цветовых оттенков — при установленном данном флажке включается режим сглаживания изображений.

Группа Настройка HTTP 1.1 содержит два параметра. С помощью флажка Использовать HTTP 1.1 включается режим использования протокола HTTP 1.1 при подключении к веб-узлам, а если установлен флажок Использовать HTTP 1.1 через прокси-соединения, то при подключении к веб-узлам через прокси-сервер будет использоваться протокол HTTP 1.1.

Что касается группы Обзор, то здесь стоит обратить внимание на перечисленные ниже параметры.

♦ Включение стилей отображения для кнопок и иных элементов управления на веб-страницах — если установлен данный флажок, то при отображении веб-страниц для оформления будут применяться параметры настройки экрана Windows.

♦ Выводить подробные сообщения об ошибках http — если установлен данный флажок, то в случае возникновения ошибок при подключении к какому-либо серверу будет отображаться подробная информация об ошибке и советы по ее устранению. В противном случае показывается только код и название ошибки.

♦ Использовать пассивный FTP-протокол (для совместимости с брандмауэрами и DSL-модемами) — при установленном данном флажке используется пассивный FTP-протокол, при котором не требуется определение IP-адреса компьютера. Данный режим считается более безопасным.

♦ Использовать одно и то же окно для загрузки ссылок (если вкладки отключены) — если этот флажок снят, то при открытии веб-страниц с помощью ссылок они будут открываться не в уже открытом окне интернет-обозревателя, а в новом (если отключен режим работы с вкладками).

♦ Подчеркивать ссылки — с помощью данного переключателя выбирается подходящий режим подчеркивания ссылок. Возможные варианты:

• Всегда — ссылки подчеркиваются все время (этот режим установлен по умолчанию).

• Никогда — ссылки не подчеркиваются никогда.

• При наведении — ссылки подчеркиваются только при подведении к ним указателя мыши.

♦ Разрешение сторонних расширений обозревателя — если этот флажок снят, то использование средств сторонних разработчиков (не корпорации Microsoft), предназначенных для Internet Explorer, будет невозможно. Изменение значения данного параметра начинает действовать только после перезапуска Internet Explorer.

♦ Уведомлять по окончании загрузки — если установить этот флажок, то по окончании загрузки файлов на экране будет отображаться соответствующее сообщение.

Группа Печать включает в себя один параметр — флажок Печатать цвета и рисунки фона. Если этот параметр включен, то при печати веб-страницы будет также распечатываться фоновое изображение либо фоновые рисунки. При включении данного режима следует учитывать, что в зависимости от используемого принтера возможно ухудшение

скорости и качества печати.

Последняя группа параметров на вкладке Дополнительно называется Специальные возможности. Если в ней установлен флажок Всегда расширять текст для изображений, то при снятом флажке Показывать изображения (его описание приведено чуть выше) размер рисунка будет увеличиваться для отображения всего связанного с ним текста. Если установлен флажок Перемещать системную каретку вслед за фокусом и выделением, то системная каретка будет перемещаться в зависимости от изменения фокуса или выделения. Данный параметр важен при использовании программ, использующих системную каретку для определения нужной области экрана.

Настройка Mozilla Firefox

Чтобы перейти к настройкам программы, используйте команду главного меню Инструменты ▸ Настройки — при ее активизации на экране откроется окно настройки параметров Mozilla Firefox, изображенное на рис. 1.7.

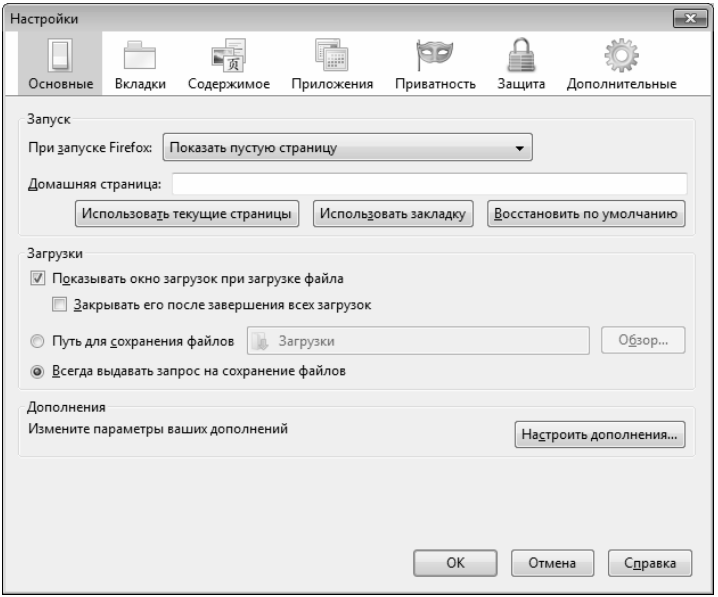

Рис. 1.7. Настройка параметров Mozilla Firefox

Окно настройки состоит из нескольких разделов: Основные, Вкладки, Содержимое, Приложения, Приватность, Защита и Дополнительные. Названия разделов отображаются вверху окна, для перехода к разделу нужно щелкнуть мышью на его значке. Параметры выбранного раздела представлены в окне настроек (например, на рис. 1.7 отображаются параметры раздела Основные). Далее мы рассмотрим самые востребованные параметры настройки Mozilla

Firefox.

Раздел Основные содержит параметры, к которым пользователи обращаются в первую очередь. Например, многим сразу хочется отключить автоматическую загрузку стартовой страницы, которая предложена авторами программы по умолчанию. Для решения этой задачи нужно в разделе Основные в поле При запуске Firefox из раскрывающегося списка выбрать значение Показать пустую страницу (это значение выбрано на рис. 1.7). Если же вы хотите, чтобы при запуске программы автоматически загружалась какая-то страница, выберите в данном поле значение Показать домашнюю страницу, после чего в поле Домашняя страница введите ее точный адрес. В данном поле можно выбрать и еще одно значение — Показать окна и вкладки, открытые в прошлый раз: в данном случае при запуске Mozilla Firefox будет автоматически загружаться страница (или несколько страниц, открытых на разных вкладках), которые были открыты в момент завершения последнего сеанса работы с программой.

Если в разделе Основные установлен флажок Показывать окно загрузок при загрузке файла, то при попытке скачать какой-либо файл на экране отобразится окно загрузок, в котором нужно будет либо указать параметры загрузки, либо оставить

значения, предложенные по умолчанию. Чтобы по окончании всех текущих загрузок это окно закрывалось автоматически, установите флажок Закрывать его после завершения всех загрузок (он доступен только при установленном флажке Показывать окно загрузок при загрузке файла).

С помощью расположенного ниже переключателя указывается, каким образом программа должна определить место, в которое необходимо помещать загружаемые из Интернета объекты. Если переключатель установлен в положение Путь для сохранения файлов, то в расположенном справа поле нужно указать путь для сохранения, куда автоматически будут помещаться все загружаемые объекты. Чтобы ввести этот путь, нужно нажать расположенную справа кнопку Обзор, после чего в открывшемся окне указать требуемый каталог и нажать кнопку ОК. Если же выбран вариант Всегда выдавать запрос на сохранение файлов, то при каждой загрузке нужно будет вручную указывать путь для сохранения. По умолчанию переключатель установлен в положение Путь для сохранения файлов, а в расположенном справа поле указан путь Рабочий стол, но практика показывает, что большинство пользователей предпочитают пользоваться вторым вариантом, поскольку это позволяет соблюдать определенный порядок при скачивании файлов на компьютер, а не

загромождать ими Рабочий стол.

В разделе Вкладки, содержимое которого показано на рис. 1.8, выполняется настройка использования вкладок.

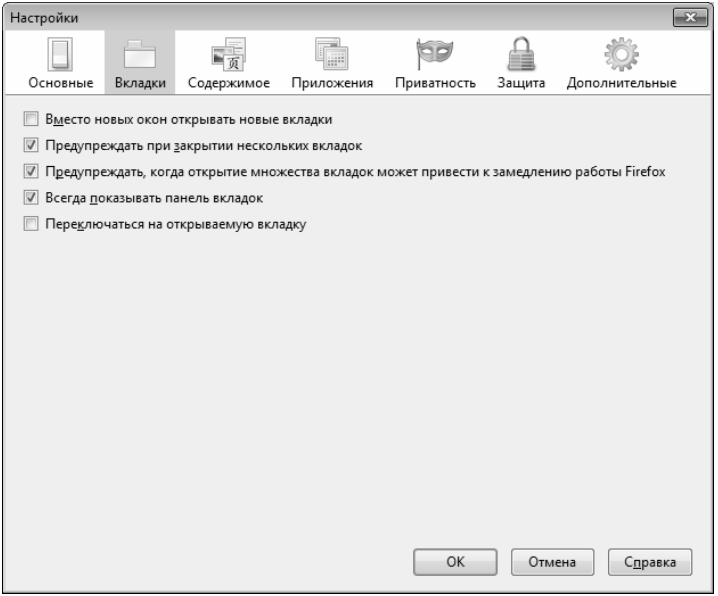

Рис. 1.8. Настройка Mozilla Firefox, раздел Вкладки

Если в данном разделе снят флажок Вместо новых окон открывать новые вкладки, то при щелчках на ссылках для перехода на новые страницы они будут открываться в новом окне. Если же этот флажок установлен, то для открытия

ссылок в текущем окне программы будут автоматически создаваться новые вкладки (иначе говоря, после щелчка мышью на ссылке в окне автоматически появится новая вкладка).

В процессе работы может возникать следующая ситуация: пользователь открыл несколько вкладок, затем одна из них ему оказалась не нужна, и он решил ее закрыть. Но машинально он закрывает не вкладку, а окно программы, в результате чего, разумеется, автоматически закрываются и все остальные вкладки. Во избежание подобных ситуаций в разделе Вкладки имеется флажок Предупреждать при закрытии нескольких вкладок: если он установлен, то в случае, когда пользователь пытается закрыть окно программы с открытыми несколькими вкладками, на экране будет отображаться соответствующее предупреждение с запросом на подтверждение данной операции. Окно со всеми вкладками будет закрыто только при положительном ответе на данный запрос.

Если в разделе Вкладки установлен флажок Всегда показывать панель вкладок, то панель вкладок в окне программы будет присутствовать постоянно, даже если ни одна страница не открыта (т. е. даже когда рабочая область пуста). Если же этот флажок снят, то панель вкладок будет появляться автоматически только после открытия

какой-либо страницы.

В разделе Содержимое (рис. 1.9) выполняется настройка отображения содержимого веб-страниц, а также некоторых параметров безопасности.

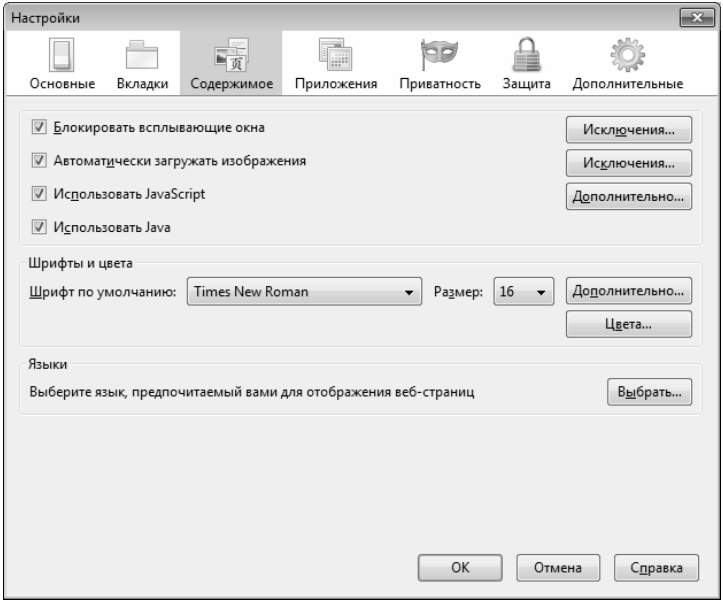

Рис. 1.9. Настройка Mozilla Firefox, раздел Содержимое

Если на данной вкладке установлен флажок Блокировать всплывающие окна, то программа будет автоматически блокировать всплывающие окна, которые почти всегда носят рекламный

характер и только мешают работе. Если вы хотите разрешить использование Java-сценариев, то установите соответствующие флажки.

С помощью параметра Шрифт по умолчанию осуществляется выбор шрифта, который будет использоваться по умолчанию для отображения веб-страниц. С помощью расположенной справа кнопки Размер выбирается подходящий размер шрифта, а с помощью кнопки Цвета осуществляется переход в режим настройки цветового оформления. Кнопка Дополнительно предназначена для перехода в режим настройки дополнительных параметров шрифта.

В разделе Приложения осуществляется выбор приложений, которые в процессе работы будут использоваться совместно с Интернет-обозревателем Mozilla Firefox. Как правило, то в данном разделе можно ничего не менять и оставить те значения параметров, которые предложены по умолчанию.

Параметры, находящиеся в разделе Защита, предназначены для обеспечения безопасности вашей работы в Интернете. Начинающим пользователям не рекомендуется менять значения этих параметров без серьезных на то оснований.

Многие дополнительные параметры настройки, в том числе и касающиеся безопасности работы в Интернете, вынесены в раздел

Дополнительные, содержимое которого показано на рис. 1.10.

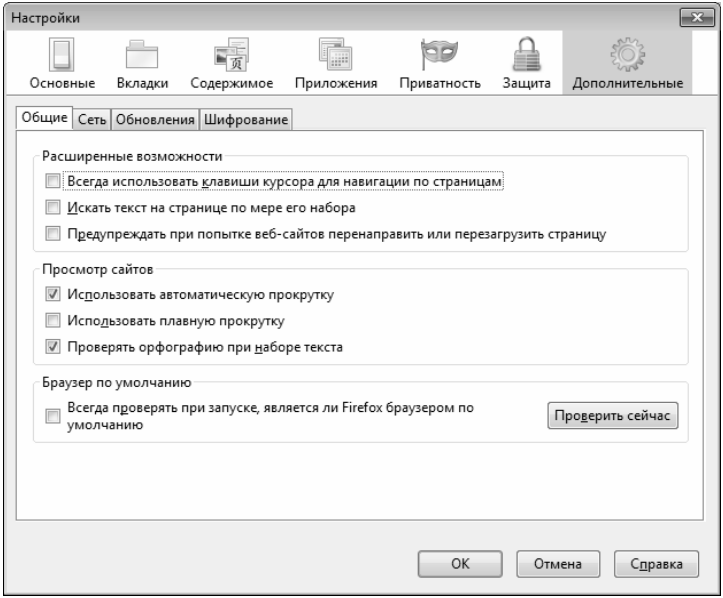

Рис. 1.10. Настройка Mozilla Firefox, раздел Дополнительные

Как видно на рисунке, содержимое раздела располагается на четырех вкладках: Общие, Сеть, Обновления и Шифрование.

Чтобы при работе в Интернете вас случайно не перенаправили на вредоносный или просто ненужный вам сайт, установите на вкладке Общие

флажок Предупреждать при попытке веб-сайтов перенаправить или перезагрузить страницу. При каждом запуске программы можно проверять, является ли Mozilla Firefox обозревателем, используемым по умолчанию — для этого достаточно установить соответствующий флажок, расположенный в области Браузер по умолчанию.

На вкладке Сеть можно указать размер дискового пространства, выделяемого для хранения кэша (по умолчанию — 50 Мб). Здесь же путем установки соответствующего флажка можно включить настройку, при которой программа будет предупреждать вас обо всех случаях, когда веб-сайт будет запрашивать разрешение на сохранение данных для последующего автономного просмотра.

На вкладке Обновления содержатся параметры, определяющие порядок поиска и установки обновлений Mozilla Firefox в Интернете. Если установлены флажки Браузера Firefox, Установленных дополнений и Поисковых плагинов, то программа будет автоматически искать соответствующие обновления при каждом подключении к Интернету. Если же вы не желаете расходовать свой Интернет-трафик на эти цели — снимите данные флажки. Отметим, что вы в любой момент можете просмотреть журнал обновлений — для этого достаточно нажать кнопку Показать журнал обновлений. Если на данной вкладке

установлен флажок Браузера Firefox, то становятся доступными для редактирования еще два параметра — переключатель При обнаружении обновлений для Firefox и флажок Предупреждать, если при данном действии будут отключены какие-либо дополнения, который доступен только в том случае, когда переключатель установлен в положение Автоматически загружать и устанавливать дополнения. Если же переключатель установлен в положение Предоставлять выбор действия пользователю, то при обнаружении обновлений пользователю будет предложено выбрать вариант дальнейших действий.

Что касается вкладки Шифрование, то в большинстве случаев рекомендуется оставить значения параметров, предложенные по умолчанию. С помощью этих параметров определяются протоколы, а также определяется порядок отправки личного сертификата (автоматически или по запросу, причем по умолчанию предлагается второй вариант). Кнопки, расположенные на данной вкладке, позволяют перейти в режим более тонкой настройки параметров шифрования, но опять же — если вы не являетесь специалистом в этом вопросе, то экспериментировать не рекомендуется.

Все изменения, выполненные во всех разделах окна настройки программы, вступают в силу только

после нажатия кнопки ОК. С помощью кнопки Отмена осуществляется выход из данного режима без сохранения выполненных изменений.

Глава 2. Спам, вирусы, компьютерный шпионаж

В данной главе мы поговорим о таких явлениях, как навязчивая реклама и спам, компьютерный шпионаж, и, конечно, не оставим без внимания тему компьютерных вирусов. Кроме этого, мы научимся самостоятельно бороться со всеми перечисленными явлениями.

Компьютерные вирусы

Наверное, невозможно сегодня встретить пользователя компьютера, который не слышал бы о компьютерных вирусах. Эти вредоносные программы в огромном количестве «представлены» в Интернете, и их количество растет с каждым днем. Самое неприятное, что многие распространители вирусов успешно применяют в своей практике передовые достижения IT-индустрии — в результате то, что должно

служить во благо пользователям, в конечном итоге может обернуться для них большими проблемами.

Что же включает в себя понятие «компьютерный вирус»? Многие специалисты расходятся во мнениях на этот счет и предлагают разные формулировки. Мы же будем считать, что вирус — это вредоносная программа, проникающая на компьютер без ведома пользователя (хотя, возможно, при невольном его участии) и выполняющая определенные действия разрушительной направленности, нередко умеющая размножаться и самораспространяться.

Первый компьютерный вирус был написан в начале 80-х годов прошлого столетия. Тогда это не было попыткой навредить кому-либо, а сделано просто из интереса. Этот вирусописатель явно не подумал о возможных последствиях: сегодня известно несколько миллионов вирусов, и их количество растет с каждым днем.

Каковы же причины возникновения вирусов? Когда-то это было не более чем шалостью. Постепенно пользователи, умеющие писать вирусы, стали применять свое умение на практике, и вирусы стали создаваться с конкретными целями. Например, сотрудник, вынужденный уволиться с работы и считающий себя обиженным, с помощью вируса мог «отомстить» своему бывшему работодателю либо коллегам по работе. Кстати,

подобные ситуации возникали и в корпорации Microsoft — известны случаи, когда бывшие ее сотрудники создавали вирусы, используя свои знания уязвимых мест операционной системы Windows либо офисных приложений.

В настоящее время в мире развелось великое множество «вирусописателей». Одни из них занимаются созданием и распространением вирусов в качестве хобби, другие просто желают сделать «всем плохо», третьи хотят отомстить, четвертые имеют вполне конкретные коммерческие цели — хищение информации либо денежных средств, вывод из строя сетей, веб-ресурсов и т. п. за солидное вознаграждение (в частности, это одно из проявлений современной конкурентной борьбы), и др.

Виды компьютерных вирусов

Специалисты выделяют несколько категорий компьютерных вирусов, среди которых можно выделить следующие: файловые вирусы, сетевые вирусы (черви), загрузочные вирусы, макровирусы и так называемые «троянские кони» (трояны).

Файловые вирусы были широко распространены в конце 80-х — начале 90-х годов прошлого столетия. Их отличительная черта — то, что они активизируются при запуске

инфицированной программы. При этом программный код вируса скрывается либо в исполняемом файле, либо в динамических библиотеках (dll). После активизации такой вирус способен инфицировать и иные приложения, установленные на компьютере.

Стоит отметить, что время файловых вирусов уже практически ушло. Исключением являются вирусы, которые по своей природе относятся к скриптам. Такие вирусы обычно прячутся в веб-страницах, их программный код написан с использованием скриптового языка программирования (один из самых известных таких языков — JavaScript).

Одним из наиболее неприятных и опасных видов вредоносного программного обеспечения по праву считаются сетевые вирусы (черви). Уже по названию нетрудно догадаться, что их «среда обитания» — это локальная сеть. Сетевому червю для распространения по локальной сети достаточно попасть в один компьютер — и уже через короткое время вся сеть будет инфицирована.

ВНИМАНИЕ

Нередки случаи, когда сетевые вирусы используют хитроумную приманку для того, чтобы пользователь выполнил их активизацию. Например, на рабочем столе

зараженного компьютера может внезапно появиться значок с изображением стодолларовой купюры и азартным названием вроде **Вы выиграли приз** , **Возьми меня** или т. п. Если на этом значке щелкнуть мышью (а это первое естественное желание у подавляющего большинства пользователей, и об этом прекрасно осведомлены разработчики вредоносного программного обеспечения), то сетевой червь моментально активизируется и начинает распространение по всем компьютерам, подключенным к локальной сети.

Характерной особенностью загрузочных вирусов является то, что они заражают загрузочную область диска. Действует такой вирус примерно так: при загрузке операционной системы сведения из зараженной загрузочной области попадают в память компьютера. После этого инфицируются загрузочные области всех доступных дисков (как жестких, так и гибких). Правда, в настоящее время подобные вирусы встречаются очень редко, поскольку их основной метод размножения — через загрузочные гибкие диски, а таким способом компьютеры сегодня почти никто не загружает (исключением могут являться различного рода нештатные ситуации).

Большинство независимых исследователей сходятся во мнении, что немалая опасность в ближайшем будущем будет исходить от макровирусов. Конструктивно они подобны файловым вирусам, так как тоже прячутся в программном коде. «Ореол обитания» макровирусов — это макросы, то есть приложения, написанные на языке программирования Visual Basic Application. Макросы используются в программах офисного пакета MS Office для расширения их имеющихся функциональных возможностей.

Еще одним опасным видом вирусов являются так называемые «троянские кони», попросту говоря — трояны. Их отличительной особенностью является то, что они обычно не вредят компьютеру либо хранящейся в нем информации. Основная цель этих вирусов — предоставление к данному компьютеру удаленного доступа через Интернет, используя который злоумышленник может осуществлять с инфицированным компьютером любые действия: уничтожать и записывать данные, редактировать настройки, запускать программы, и т. д.

Главное коварство «троянских коней» состоит в том, что пользователь инфицированного компьютера может ничего не подозревать о том, что его компьютер используется в каких-то целях

(рассылка спама, реклама порнографических сайтов, рассылка призывов к массовым противоправным действиям, и т. п.). Для надежного противодействия троянам мало установить антивирусную программу — необходимо еще иметь на компьютере сетевой экран (файрволл).

Также здесь можно отметить бессмысленные, шутливые и т. п. вирусы — они, как правило, не осуществляют особых деструктивных действий, а просто периодически выдают на экран сообщения о каких-либо несуществующих «катаклизмах» в компьютере (например, Ваш компьютер заражен вирусом; через 15 минут начнется автоматическое форматирование диска С). Не исключено, что, получив такое сообщение, испуганный пользователь начнет лихорадочно сохранять всю более-менее ценную информацию на внешних носителях, да и вообще сделать массу ненужных действий. Возможно также, что, не дождавшись обещанного форматирования диска, пользователь сам запустит этот процесс — как говорится, «от греха подальше» (такое паникерство обычно свойственно новичкам).

Как защититься от компьютерных вирусов

Для борьбы с вредоносным программным обеспечением в настоящее время существует

немало специально предназначенных программных средств, относящихся к категории антивирусов.

Высокой степенью эффективности отличается удобная и недорогая антивирусная программа NOD 32. Ее автором и разработчиком является известная компания ESET, занимающая одну из лидирующих позиций на рынке программного обеспечения. NOD 32 успешно справляется с различного рода вирусами, шпионскими и рекламными модулями, червями, троянами и прочими вредоносными программами. Кроме этого, NOD 32 является надежным сетевым экраном, блокируя любое проникновение в компьютер извне. Среди прочих преимуществ данного продукта стоит отметить простоту и удобство в эксплуатации, а также то, что его функционирование не замедляет работу операционной системы.

Еще один полезный и эффективный защитный продукт — программа Virus Scan, разработчиком которой является американская корпорация McAfee. В данной программе, как и во многих других, реализовано два основных направления — для домашних пользователей и для офисного применения. Для предварительного знакомства с ее возможностями предоставляется бесплатная демонстрационная версия, которую можно скачать с сайта разработчика. Программа обладает достаточно удобным, современным и

эргономичным пользовательским интерфейсом, а также простым и понятным инструментарием. Антивирусную программу Virus Scan можно приобрести как отдельно, так и в комплексе с другими программами от этого же разработчика, предназначенными для защиты компьютера и информации — в частности, с антиспамовым фильтром и файрволом. Управление всеми режимами осуществляется из одного интерфейса, а переключение между ними выполняется с помощью соответствующих инструментов.

Одним из распространенных и эффективных антивирусных средств является программа Avast. Как показывает практика, она способна распознавать и успешно бороться с вирусами, перед которыми оказываются бессильны иные антивирусные программы. Отметим, что Avast — это не только собственно антивирус, но еще и сканер электронной почты, а также надежный сетевой экран. В настоящее время имеется как платная, так и бесплатная версия этой программы.

Программа Panda Antivirus — еще один представитель семейства антивирусных продуктов. Ее разработчиком является испанская фирма Panda Software. В состав программы входят модули сканирования и мониторинга (эти функции в Panda Antivirus объединены в одну), модуль почтового сканирования (для проверки электронной

корреспонденции) и модуль автоматического обновления антивирусных баз.

Отличительной чертой программы является то, что после установки ее практически не нужно настраивать. Конечно, при необходимости пользователь может изменить любые параметры настройки в соответствии со своими потребностями, но предлагаемые значения по умолчанию подобраны настолько оптимально, что в большинстве случаев программу можно использовать сразу после установки. Это и является одним из приоритетных направлений, заложенных в программе — она должна быть проста и удобна в применении даже для неопытных и начинающих пользователей.

Особо следует отметить возможность программы восстанавливать поврежденную вирусом систему. Иначе говоря, после обнаружения вируса и его обезвреживания (удаления, лечения и др.) программа ликвидирует все сделанные им изменения в системных файлах, системном реестре, настройках системы и т. д., и возвращает операционную систему в то состояние, в котором она была до появления вируса.

Еще одной популярной антивирусной программой является «Антивирус Касперского», автором и разработчиком которой является лаборатория Касперского. Первый релиз продукта

увидел свет еще в 1994 году. С тех пор «Антивирус Касперского» претерпел множество изменений и к настоящему времени стал качественным современным средством защиты. Стоимость программы и комплект поставки зависят от того, какую конфигурацию приобретает пользователь.

Также немалой популярностью пользуется антивирус, который называется Dr.Web. Он относится к числу первых российских продуктов аналогичного назначения, и сегодня считается одним из самых эффективных. Отметим, что от многих конкурентов Dr.Web выгодно отличается высоким быстродействием. Параметры сканирования устанавливаются в настройках программы. В частности, там указываются объекты, которые нужно проверить, определяется порядок действия в случае обнаружения вируса (переименовать зараженный объект, удалить его либо вылечить, или поместить в указанную папку), устанавливается количество ресурсов компьютера, выделяемых на сканирование, и др.

Антивирусное приложение Norton Antivirus также имеет немалое число поклонников во всем мире. Ее автором является знаменитая корпорация Symantec. Продукт выпускается в разных конфигурациях — для домашних пользователей и для офисного применения. Средняя стоимость «домашней» версии составляет около 50 долларов

США. Программа имеет приятный и эргономичный пользовательский интерфейс — по мнению многих пользователей, он выглядит намного современнее, чем интерфейсы конкурентов, но на момент написания данной книги русский язык в ней не поддерживается. Отличительной чертой Norton Antivirus является наличие очень мощной функциональности проверки электронной почты (многие конкуренты по этому показателю уступают). При этом поддерживается работа со всеми наиболее популярными почтовыми программами — Outlook Express, Microsoft Outlook, The Bat и др. Использование программы практически полностью исключает возможность приема и отправки зараженных вирусами электронных сообщений. Обнаруженные в процессе сканирования вирусы и зараженные файлы помещаются в специальную папку, где пользователь может досконально с ними разобраться и, в зависимости от полученного результата — либо удалить их, либо отменить решение Norton Antivirus о причислении их к числу вирусов.

Как предотвратить заражение компьютера

Несмотря на обилие антивирусного ПО, стопроцентной защиты от вирусов сегодня не

существует. Тем не менее, соблюдение перечисленных ниже правил поможет многократно снизить риск заражения.

♦ Если возможности используемой антивирусной программы предусматривают использование постоянного мониторинга, то данный режим обязательно должен быть включен при работе в Интернете. Это поможет своевременно обнаружить зараженные файлы, пытающиеся проникнуть в компьютер.

♦ Ни в коем случае нельзя запускать внезапно появляющиеся иконки и значки на рабочем столе — многие вирусы (особенно это относится к сетевым червям) специально помещают на рабочий стол заманчивую иконку, при щелчке на которой вирус активизируется и начинает распространяться по сети.

♦ Периодически нужно выполнять полное сканирование компьютера хорошей антивирусной программой. Периодичность сканирования зависит от того, как часто и с какой загрузкой работает компьютер, а также — выходит ли пользователь в Интернет.

♦ При получении из Интернета либо локальной сети файлов каких-либо приложений пакета Office (Word, Excel и др.) следует в первую очередь проверить их надежной антивирусной программой, и лишь затем открывать. Такие файлы

могут содержать макровирусы — это один из наиболее распространенных и коварных видов вирусов.

♦ То же самое относится и к другим скачиваемым из Интернета файлам (дистрибутивы либо исполняемые файлы приложений, самораспаковывающиеся архивы и др.) — перед выполнением их обязательно нужно проверить антивирусом (не забыв перед этим обновить антивирусные базы).

♦ Избегайте компьютеров «общего пользования» — т. е. установленных в студенческих аудиториях, в Интернет-кафе, и т. п. За день таким компьютером воспользуется неизвестно сколько человек, и любой из них может занести вирус со своей дискеты либо компакт-диска. Поэтому записывать с такого компьютера информацию на свою дискету — примерно то же самое, что в разгар эпидемии гриппа посещать многолюдные места.

♦ При работе с внешними носителями информации (дискеты, компакт-диски и др.) обязательно проверять их на наличие вирусов антивирусной программой (особенно если это не собственный диск либо дискета, либо если он новый).

♦ При работе с файлами, расположенными в Интернете, настоятельно рекомендуется не

запускать их сразу, а предварительно сохранить на своем компьютере и проверить антивирусной программой.

♦ Еще раз напомним, что по окончании работы в Интернете необходимо обязательно отключить шнур, соединяющий компьютер с Интернетом — если этого не сделать, то вирус может проникнуть даже в выключенный компьютер.

Компьютерный шпионаж

Основное отличие шпионских модулей Spyware от компьютерных вирусов заключается в том, что они, как правило, не наносят вреда программному обеспечению и данным, хранящимся в компьютере (если не считать того, что на них отвлекается определенное количество ресурсов оперативной памяти и места на жестком диске). Задача шпионских модулей заключается в том, чтобы собирать некоторую информацию о пользователе (адреса электронной почты, содержимое жесткого диска, список посещаемых страниц в Интернете, информация личного характера и т. д.) и отправлять ее по определенному адресу. При этом пользователь даже не подозревает, что за ним ведется своего рода тайное

наблюдение. Полученная таким способом информация может использоваться в самых разнообразных целях, которые могут быть как относительно безобидными (анализ посещаемости тех либо иных сайтов), так и весьма опасными (например, если полученная информация будет использована в противозаконных целях либо в ущерб пользователю).

Каким образом же шпионские модули проникают в компьютер? В большинстве случаев это происходит в процессе инсталляции нужных и полезных приложений, которые пользователь устанавливает самостоятельно. Есть, например, бесплатные программы, которые можно использовать только вместе с встроенной программой-шпионом; если же шпион будет удален, то и основную программу использовать будет невозможно. Кроме этого, нужно соблюдать внимание при установке программ: некоторые шпионы проникают в компьютер, например, после того, как пользователь, не задумываясь, утвердительно ответил на какой-либо запрос, который появился на экране в процессе инсталляции. Некоторые разработчики вставляют в дистрибутив своих продуктов собственную программу-шпиона, а некоторые обращаются за помощью к фирмам, которые создают и поставляют программы-шпионы разработчикам программного

обеспечения. Кроме этого, программы-шпионы могут проникать в компьютер из Интернета (от подобных проникновений и защищает брандмауэр).

Классификация шпионского ПО

В настоящее время существует несколько видов шпионского ПО. Например, у многих злоумышленников пользуются популярностью так называемые кейлоггеры — клавиатурные шпионы. Их характерной особенностью является то, что они могут иметь как программное, так и аппаратное исполнение. Главная задача клавиатурного шпиона — собирать и высылать своему заказчику информацию обо всех нажатиях клавиш на компьютере, за которым ведется слежка. Это один из самых опасных видов шпионских модулей, поскольку он способен похищать секретную информацию, вводимую пользователем с клавиатуры: логины и пароли, пин-коды кредитных карт, конфиденциальную переписку, и т. д. Часто кейлоггеры используются для похищения программных кодов создаваемого программного обеспечения.

Если клавиатурный шпион имеет аппаратное исполнение, то обнаружить его несложно. Просто следите за своим компьютером, если в помещение, где он находится, имеют доступ другие лица (это

особенно актуально по отношению к офисным компьютерам). Следите за тем, чтобы между клавиатурой и системным блоком не появилось какое-то устройство (обычно аппаратный кейлоггер имеет небольшие размеры, меньше спичечного коробка), а при обнаружении непонятных устройств немедленно обратитесь к системному администратору.

Если же кейлоггер представляет собой программу, то для его обнаружения и нейтрализации используйте специальное программное обеспечение категории AntiSpyware.

Еще один известный вид шпионского ПО — сканер жесткого диска. Этот шпион тщательно изучает все содержимое жесткого диска вашего компьютера (какие программы установлены, какие файлы и папки хранятся, и др.) и отсылает собранные сведения своему хозяину.

Информацию о том, чем вы занимаетесь на компьютере, может собирать экранный шпион. Сущность его состоит в том, что он периодически через определенные промежутки времени (которые заданы злоумышленником) делает снимки экрана (на компьютерном сленге — скриншоты), и отсылает их хозяину. Кстати, этот вид шпионов иногда используется в офисах: с его помощью начальство узнает, чем занимаются подчиненные во время работы.

Также немалой популярностью у злоумышленников пользуются так называемые «прокси-шпионы». После того как такой spyware проникает в компьютер, то этот компьютер будет выполнять роль прокси-сервера (о том, что представляет собой прокси-сервер, мы говорили ранее). На практике это означает, что злоумышленник при работе в Интернете сможет прикрываться вашим именем, и если его действия будут носить деструктивный или противозаконный характер — отвечать придется именно вам. Самый типичный пример — когда с зараженного компьютера рассылается спам, что может привести к появлению проблем со своим провайдером.

Еще один популярный у злоумышленников вид spyware — это почтовые шпионы. Их главная задача — сбор сведений об адресах электронной почты, хранящихся в данном компьютере, и отсылка этой информации хозяину. Сведения собираются обычно в почтовых программах и адресных книгах, а также органайзерах. Такая информация имеет высокую ценность для тех, кто занимается рассылкой спама. Кроме этого, почтовые шпионы могут вести откровенно деструктивную деятельность: менять содержимое писем, вставлять в них рекламные блоки, и т. д.

Кейлоггер, или клавиатурный шпион

Несмотря на то, что выше мы уже упоминали о клавиатурных шпионах, на них имеет смысл остановиться подробнее. В первую очередь это обусловлено тем, что клавиатурные шпионы являются одними из самых коварных из всего многообразия шпионских модулей и программ.

В общем случае клавиатурному шпиону можно дать следующее определение:

Клавиатурный шпион — это программа либо устройство, с помощью которого осуществляется постоянное наблюдение за всеми нажатиями клавиш на клавиатуре (а во многих случаях — и за всеми щелчками мыши) с целью получения информации обо всех набираемых пользователем текстах. Зачем это нужно? Ответ на данный вопрос у каждого злоумышленника свой: одному нужно перехватывать чужие почтовые сообщения, другому — получить номера кредитных карт, третьему — взломать пароли, четвертому — украсть у разработчика исходные тексты еще не вышедшей программы, а пятому — все вместе взятое, и еще что-нибудь.

Характерной особенностью клавиатурных шпионов является то, что они могут выступать не только в виде внедренного в компьютер вредоносного программного обеспечения, но и в

виде отдельных устройств. Такие устройства обычно устанавливаются между клавиатурой и системным блоком и, поскольку имеют весьма небольшие размеры, могут долго оставаться незамеченными. Однако чтобы установить такое устройство, необходим доступ к компьютеру в отсутствие пользователя. Поэтому на домашних компьютерах такой вид клавиатурных шпионов встречаются редко, чаще — на офисных и рабочих компьютерах, а также на компьютерах «общественного пользования»: в студенческих аудиториях, на почте, в интернет-клубах и др. Чтобы своевременно обнаружить такой «сюрприз», рекомендуется почаще обращать внимание на то, не появилось ли новое устройство между клавиатурой и системным блоком.

Достаточно широко распространены в настоящее время так называемые перехватывающие клавиатурные шпионы. Такие шпионы в большинстве случаев представляют собой программу, состоящую из исполняемого файла с расширением *.exe, и dll-библиотеки, с помощью которой осуществляется управление процессами записи информации. Перехватывающий клавиатурный шпион без проблем запоминает практически любой набранный текст: документы, письма, исходные коды программ (данная возможность нередко используется для кражи

исходников еще не вышедших программ), номера кредитных карт, пароли (в том числе и самозаполняющиеся) и т. д.

Клавиатурный шпион (имеется в виду программа, а не устройство) может проникнуть в компьютер разными способами: например, как и любой другой шпионский модуль — в составе какой-либо устанавливаемой на компьютер бесплатной программы (как правило — от неизвестного либо сомнительного разработчика), либо через программу обмена сообщениями, и т. д. В последнее время нередки случаи, когда для «получения» в свой компьютер клавиатурного шпиона достаточно было просто зайти на определенный сайт.

Стопроцентной защиты от клавиатурных шпионов, как и от других вредоносных программ, в настоящее время не существует — ведь известно, что на каждое противоядие можно найти новый яд. Однако при соблюдении мер предосторожности можно свести к минимуму их вероятность их появления на компьютере.

Что касается аппаратных клавиатурных шпионов, то для защиты от них рекомендуется по возможности минимизировать доступ к компьютеру посторонних лиц — это в первую очередь относится к компьютерам, которые установлены на рабочих местах (разумеется, не нужно впадать при

этом в крайности — например, системного администратора отгонять от компьютера не стоит). Ну и, конечно, периодически нужно проверять, не появилось ли между клавиатурой и системным блоком какое-нибудь неизвестное устройство. Иногда это касается и домашних компьютеров — вспомните, кто имеет доступ к вашему компьютеру? Одно дело — если только вы, и другое — если, например, к вашему сыну-студенту периодически приходят «продвинутые» в компьютерном отношении друзья и возятся около компьютера. В последнем случае вполне возможно, что вам потехи ради (или с более серьезными намерениями) вставят какого-нибудь «жучка».

Что же делать, если предполагается, что в компьютер уже проник клавиатурный шпион? Конечно, в первую очередь необходимо просканировать компьютер специально предназначенной программой. Для поиска и уничтожения клавиатурных шпионов можно использовать некоторые программы из числа тех, что предназначены для борьбы и с другими Spyware; кроме этого, есть программы, специализирующиеся именно на клавиатурных шпионах (одна из таких программ рассматривается чуть ниже). Однако бывают ситуации, когда выполнение немедленного сканирования невозможно, и в то же время необходимо срочно

выполнить какие-либо действия с конфиденциальными данными. Как же поступить в таком случае?

При возникновении подобных ситуаций рекомендуется использовать так называемую виртуальную клавиатуру. Виртуальная клавиатура — это программа, интерфейс которой представляет собой изображение клавиатуры, а ввод нужных символов осуществляется с помощью мыши. Поскольку принцип действия большинства клавиатурных шпионов заключается в перехвате вводимых с клавиатуры символов, то использование виртуальной клавиатуры достаточно эффективно.

Однако необходимо учитывать, что некоторые клавиатурные шпионы снимают копии экрана еще и после каждого щелчка мыши. Для защиты от таких шпионов предусмотрены виртуальные клавиатуры, в которых для ввода символа достаточно просто подвести указатель мыши к соответствующей позиции. Благодаря этому можно ввести информацию без единого щелчка мышью.

При частой или регулярной работе с конфиденциальными данными рекомендуется постоянно использовать виртуальную клавиатуру — ведь никогда нельзя полностью быть уверенным в том, что в компьютер не проник клавиатурный шпион.

Для борьбы с клавиатурными шпионами можно использовать программы, предназначенные для борьбы и с другими Spyware (описание некоторых из них приведено выше), а также специализированные программы, которые называются анти-кейлоггеры. Одной из таких программ является Anti-keylogger, которую разработали российские специалисты.

Характерной особенностью программы Anti-keylogger является то, что для ее работы не предусмотрено использование сигнатурных баз. Это позволяет ей выявлять и блокировать любые виды клавиатурных шпионов, как известные большинству аналогичных программ, так и нет.

Программа обладает простым и дружественным пользовательским интерфейсом. В разделе **Опции** предусмотрена возможность настройки параметров работы программы. Кроме этого, в разделе **Лист исключений** реализована возможность ведения списка исключений; в этот список можно включать программы, которые не должны распознаваться как клавиатурные шпионы.

Помимо программы Anti-keylogger, в Интернете можно найти еще множество программ (как платных, так и бесплатных), специально предназначенных для борьбы с клавиатурными шпионами.