Глава 12

Безопасность превыше всего

В этой главе...

- Борьба с компьютерными злоумышленниками
- Обзор компьютерных угроз
- Инструменты Internet Explorer
- Центр поддержки

Многие пользователи компьютеров постоянно живут в страхе, опасаясь, что с их компьютером в любой момент может произойти что-нибудь ужасное. Они боятся, что злодеи из Интернета доберутся до них и украдут ценную конфиденциальную информацию или сотрут их файлы, зашлют разрушительные вирусы или установят программы-шпионы. Доходит до того, что простое нажатие кнопки включения компьютера может вызывать чувство неуверенности и страха.

Не волнуйтесь! Включайте свой ПК без колебаний, сам по себе он никогда не причинит вам вреда. Действительно, в Интернете много злоумышленников, но это не так страшно, как может показаться. Чтобы предотвратить любые атаки с их стороны, просто воспользуйтесь информацией, изложенной в этой главе.

Борьба с компьютерными злоумышленниками

Windows 8 располагает несколькими инструментами, позволяющими нарушить планы злоумышленников и защитить компьютер от нежелательных вторжений.

- ✓ **Internet Explorer.** Эта программа, веб-браузер от Майкрософт, обладает множеством функций и инструментов, обеспечивающих безопасность компьютера. Так, особые предупреждения системы безопасности появляются, когда некое программное обеспечение из Интернета пытается установить себя на компьютере, а другие защитные меры предусматривают различные способы предостережения пользователя от посещения небезопасных веб-сайтов.
- ✓ **Windows Defender** (в предыдущих версиях — Защитник Windows). Данная служебная программа помогает обнаружить и удалить целый ряд вредоносных программ, в частности самозапускающихся и шпионских.

- ✓ **Брандмауэр Windows.** Помогает держать закрытыми “окна и двери”, через которые злоумышленники могут попытаться заразить ваш компьютер вирусами или шпионским ПО.
- ✓ **Утилита обновления Windows.** Очень важный инструмент, обеспечивающий своевременное обновление системного программного обеспечения компьютера с целью устранения найденных ошибок и закрытия обнаруженных прорех.
- ✓ **Система резервного копирования.** Для обеспечения действительной безопасности полезного содержимого вашего компьютера настоятельно рекомендуется регулярно выполнять его резервное копирование. При этом создаются копии файлов, обеспечивающие успешное восстановление потерянной информации в случае поломки оборудования или утраты данных по какой-то иной причине.
- ✓ **Антивирусные программы.** Чтобы бороться с вирусами, проникающими в компьютер через Интернет, электронную почту или внешние хранилища данных (DVD, флешки и т.д.), компьютеру нужна надежная антивирусная программа. Несмотря на то что в состав Windows такая программа не входит, ее можно найти и установить абсолютно бесплатно. (Обратитесь за информацией к разделу “Антивирусная защита” далее в этой главе.)

При использовании указанных выше средств компьютер будет надежно защищен, а его владелец — доволен и спокоен.

Помочь вам справиться с наплывом сомнительных программ из Интернета может провайдер услуг Интернета. Не стесняйтесь обращаться к нему за помощью, особенно в тех случаях, когда самостоятельные попытки устранить проблему оказываются безуспешными.

Благодаря разумным мерам предосторожности можно избежать многих угроз. Прислушивайтесь к предупреждениям браузеров и не посещайте подозрительных веб-узлов. Если вы не знаете отправителя пришедшего сообщения электронной почты, никогда не открывайте в нем вложений и не переходите по ссылкам в тексте, направляющих даже на известные вам сайты. В последнем случае вы можете стать жертвой так называемого *фишинга*, т.е. подмены сайта: ссылка направит вас на сайт, который выглядит в точности как указанный сайт-оригинал, но на самом деле является поддельной копией, предназначенной для сбора конфиденциальной информации, например номеров кредитных карт.

Обзор компьютерных угроз

Как правило, различные виды *вредоносного программного обеспечения* имеют названия, понятные только посвященными и не раскрывающие суть потенциальной опасности. Поэтому ниже приводится перечень таких названий с необходимыми разъяснениями.

- ✓ **Фишинг.** Этот термин применяют к практике рассылки сообщений электронной почты, направляющих получателя на поддельные веб-страницы, выдающие себя за веб-страницы банков или интернет-магазинов. Цель — выудить ценную информацию, в частности номера банковских счетов, кредитных карт и соответствующие пароли. Жертва обмана сама предоставляет эти данные без какого-либо опасения, поскольку такие электронные сообщения и веб-страницы выглядят вполне правдоподобно и не вызывают сомнений в их подлинности. Тем не менее это не так.
- ✓ **Всплывающие окна.** Всплывающие окна нельзя назвать зловредной программой, но иногда они могут очень раздражать, особенно когда заполняют экран в большом количестве или содержат что-либо для вас неприятное. Трудно понять, какой здравомыслящий менеджер может предположить, что подобные раздражающие действия способны подвигнуть людей к покупке, но, к сожалению, так бывает. Однако в наших силах остановить этот процесс.
- ✓ **Шпионское ПО.** Достаточно обширная категория разнообразного программного обеспечения, предназначенного для отслеживания ваших действий в Интернете. При этом преследуется чисто коммерческая цель: выясняя, какие сайты вы посещаете, создатели таких программ продают собранную информацию рекламным компаниям, которые затем засыпают вас рекламным спамом.
- ✓ **Троянские программы.** Получили свое название за то, что выдают себя не за тех, кем являются на самом деле. Например, экранные заставки, бесплатно распространяемые в Интернете, наряду с основной своей функцией использует ваш компьютер в качестве ретранслятора порнографических картинок.
- ✓ **Вирус.** Вредоносная программа, которая “живет” в компьютере без вашего ведома и “заражает” его содержимое. Эта программа может быть приведена в действие в любой момент, при этом она полностью захватывает управление компьютером, изменяет направление интернет-трафика, использует ваш компьютер для рассылки спама или наносит ему какой-либо другой вред.
- ✓ **Червь.** Представляет собой саморазмножающийся вирус, который рассылает свои копии другим пользователям из вашего списка контактов.

Инструменты Internet Explorer

Браузер Internet Explorer обладает целым рядом встроенных средств обеспечения безопасности, а также предусматривает дополнительные меры защиты, делающие ваше пребывание в Интернете максимально безопасным. Перечень всех средств безопасности довольно обширен, поэтому здесь мы рассмотрим только две наиболее неприятные угрозы — всплывающие окна и фишинг.

Блокирование всплывающих окон

Чтобы в Internet Explorer настроить функцию блокирования всплывающих окон, выполните следующие действия.

1. **Запустите Internet Explorer.**
2. **Щелкните на кнопке Сервис панели инструментов.**
   На экране появится раскрывающееся меню Сервис.
3. **Выберите команду Свойства обозревателя.**
   Отобразится окно Свойства обозревателя.
4. **В этом окне перейдите на вкладку Конфиденциальность и установите флажок параметра Включить блокирование всплывающих окон, после чего щелкните на кнопке Да для подтверждения своего выбора.**

При включенном блокировании всплывающих окон подавляются практически все всплывающие окна. А это значит, что вы пропускаете мимо все рекламные сообщения.

Когда обозреватель блокирует всплывающее окно, над той частью окна, где просматривается веб-страница, отображается предупреждающий баннер следующего содержания: Всплывающее окно заблокировано. Для просмотра этого окна или дополнительных параметров щелкните здесь.

- ✓ Режим блокирования всплывающих окон может подавить вывод некоторых полезных элементов просматриваемых веб-страниц, например всплывающих окон демонстрации видео, окон меню или дополнительных информативных окон. В таких случаях для этих веб-страниц можно *разрешить* отображение всплывающих окон. Для этого щелкните на приведенном выше предупреждающем баннере и выберите в меню команду Временно разрешить всплывающие окна.
- ✓ Средство блокирования всплывающих окон не в состоянии заблокировать некоторые всплывающие окна с анимацией. Поэтому, если блокирование окон включено, а всплывающие окна по-прежнему появляются на экране, просто смиритесь с этой ситуацией, здесь IE уже бессилен.

Борьба с фишингом

С помощью *фишинга* аферисты довольно эффективно вынуждают вас делать то, чего вы никогда бы не сделали по собственной воле. Веб-страница, выглядящая довольно правдоподобно, на самом деле является ненастоящей. Браузер Internet Explorer автоматически борется с такими жуликами. Проверьте правильность настроек этой функции, выполнив следующие действия.

1. **Щелкните на кнопке Сервис панели инструментов.**
   Подсказка: это кнопка с пиктограммой шестеренки в верхнем правом углу окна обозревателя.

2. **Выберите команду Безопасность.**
3. **Выберите в подменю Безопасность команду Включить фильтр SmartScreen.**
   Если в подменю Безопасность вместо указанной присутствует команда Отключить фильтр SmartScreen, значит, функция борьбы с фишингом SmartScreen уже активизирована и ничего делать не нужно.
4. **При желании в подменю Безопасность можно выбрать команду Проверить веб-сайт для проверки безопасности посещенного вами сайта.**

Фильтр *SmartScreen* предупреждает вас о таких ссылках на веб-страницы, которые могут быть потенциально опасными. Такая ссылка обещает переход на одну веб-страницу, хотя на самом деле предполагает переход совсем на другую. Подобные ссылки могут вести на веб-сайты, небезопасные для личной информации пользователя. В любом случае вы предупреждены.

Никогда не теряйте бдительности, целиком полагаясь на функцию фильтрации SmartScreen в Internet Explorer. Определенные криминальные элементы как раз и рассчитывают на такое поведение, чтобы реализовать свои коварные замыслы. Финансовые учреждения никогда не пересылают жизненно важную информацию по электронной почте. Если у вас возникли хотя бы малейшие сомнения по поводу той или иной полученной информации, перезвоните банковскому работнику, чтобы подтвердить факт отправки вам этого сообщения. Если эта информация не подтвердится, значит, вы получили письмо-фальшивку. Как, говорится, береженого Бог бережет.

Центр поддержки

В Windows 8 все вопросы безопасности решаются в одном месте, в окне Центр поддержки (рис. 12.1). Здесь отображаются основные параметры текущего состояния системы безопасности компьютера, а также перечисляются вопросы или проблемы, требующие разрешения.

Чтобы открыть окно Центр поддержки, откройте обычную панель управления, выберите в списке Просмотр значение Крупные значки и щелкните на значке Центр поддержки. Другой вариант: чтобы быстро запустить панель управления, нажмите комбинацию клавиш <Win+R>, введите в открывшемся окне значение `control` и нажмите <Enter>.

В окне Центр поддержки особо важные пункты отмечены красным флажком, а менее важные — оранжевым.

- ✓ Всегда придерживайтесь инструкций и рекомендаций, предлагаемых в окне Центр поддержки.
- ✓ Периодически открывайте окно Центр поддержки с целью контроля состояния дел. Например, если ваша программа антивирусной защиты устареет, в этом окне появится соответствующее сообщение. В таком случае эту программу следует обновить. Дополнительные сведения по данной теме можно найти ниже, в разделе “Антивирусная защита” этой же главы.

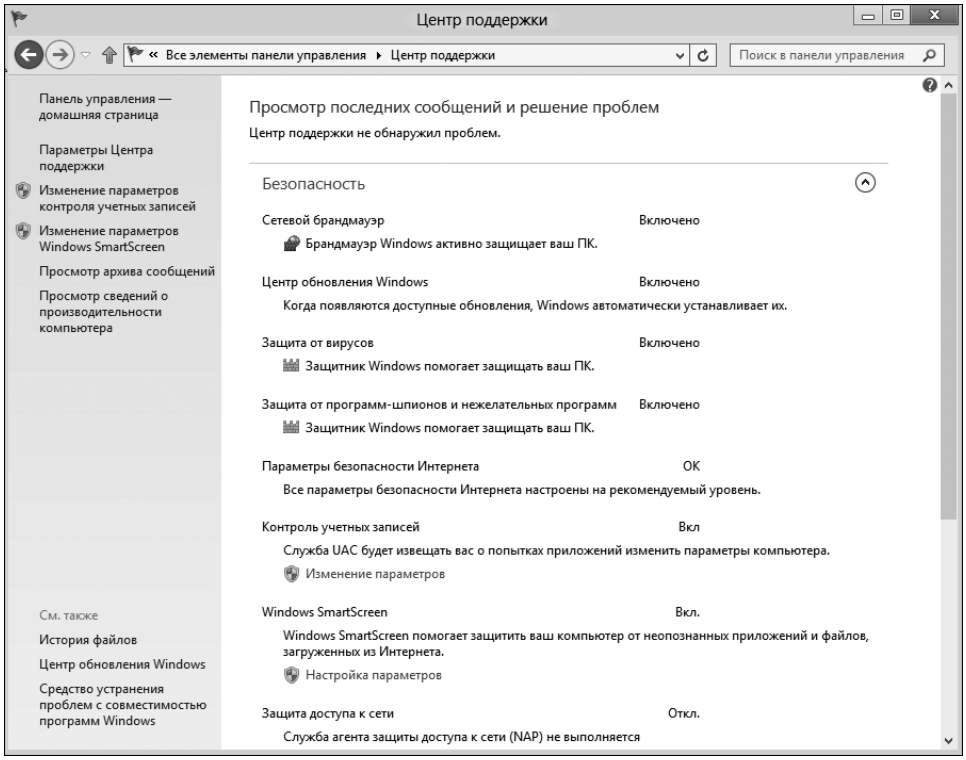

Рис. 12.1. Так выглядит окно Центр поддержки

Брандмауэр Windows

На компьютере, имеющем доступ к Интернету, брандмауэр призван ограничивать этот доступ для нежелательных гостей, пытающихся проникнуть в ваш компьютер. Он представляет собой что-то вроде фильтра, назначение которого состоит в блокировании внешних несанкционированных вторжений и контроле данных, выходящих из вашего компьютера. Брандмауэр эффективно закрывает “окна и двери”, остававшиеся открытыми со времен изобретения Интернета и делающие компьютеры уязвимыми для внешних атак.

В состав Windows входит брандмауэр, названный соответственно Брандмауэр Windows. Чтобы его запустить, в окне панели управления выберите категорию Система и безопасность, а затем щелкните на заголовке Брандмауэр Windows. В результате откроется окно Брандмауэр Windows, показанное на рис. 12.2.

Обратите внимание на то, что брандмауэр Windows имеет только два состояния — Включено и Отключено. Для изменения настройки щелкните на ссылке Включение и отключение брандмауэра Windows, находящейся в левой части окна брандмауэра Windows (см. рис. 12.2).

Если брандмауэр обнаружит попытку доступа к компьютеру из Интернета или, наоборот, какой-то программы из компьютера в Интернет, на экране появится предупреждающее всплывающее окно. Можете либо разрешить доступ указанной программе, щелкнув

на кнопке Разрешить доступ, либо заблокировать, щелкнув на кнопке Отмена. Однако не спешите принимать решение немедленно, сначала подумайте. Если вы знаете, что это за программа и, что еще важнее, почему она пытается подключиться к Интернету, разрешите ей это сделать. Обычный пример — одна из установленных у вас программ пытается подключиться к Интернету для проверки наличия обновлений. Понятно, что в этом нет ничего плохого или опасного.

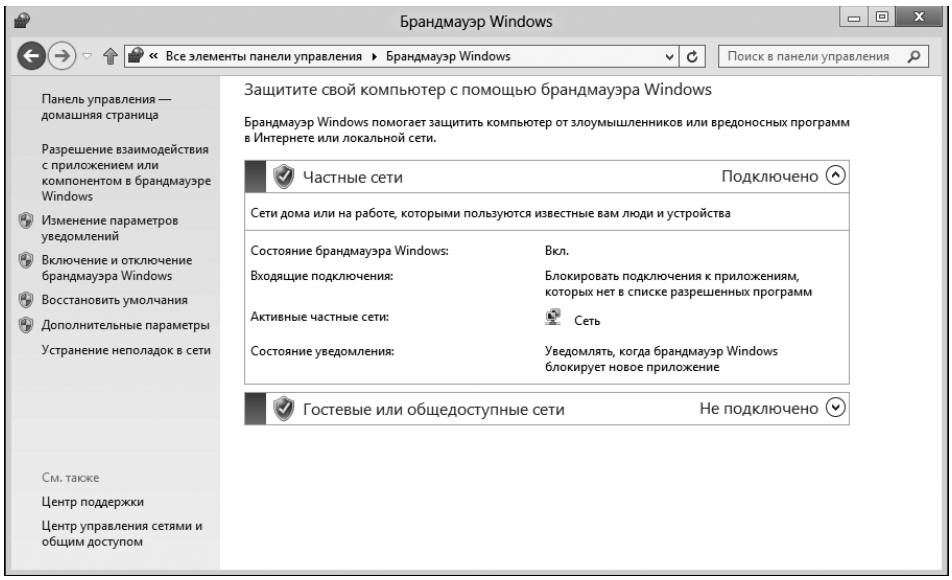

Рис. 12.2. Окно брандмауэра Windows

Если у вас появятся сомнения в эффективности работы брандмауэра Windows, протестируйте его. Многие имеющиеся в Интернете программы способны протестировать брандмауэр вашего компьютера на предмет обнаружения его слабых мест. Одну из таких программ, ShieldsUP!, можно найти на поисковом веб-сайте Gibson Research Web по адресу `http://grc.com`.

Программа Windows Defender

Программа Windows Defender (в предыдущих версиях она называлась Защитник Windows) сканирует компьютер на предмет обнаружения вредоносных программ, известных как “шпионское ПО”. Сведения о возникающих проблемах выводятся в окно Центр поддержки (см. рис. 12.1).

В Windows 8 программа Windows Defender запускается автоматически. Чтобы открыть окно программы Windows Defender, выполните следующие действия.

1. **Нажмите комбинацию клавиш <Windows+Q>, чтобы открыть окно поиска.**
2. **На открывшейся панели в поле Поиск введите слова `Windows Defender`.**
3. **В списке результатов поиска выберите значение Windows Defender.**

   Нажмите клавишу <Enter>, чтобы открыть окно программы.

Главное окно программы Защитник Windows довольно скучное, правда, до тех пор, пока у вас не возникли проблемы. В противном случае в нем просто будет представлен отчет о корректной работе вашего компьютера. Можете закрыть это окно.

- ✓ Существуют и другие антишпионские программы, которые обычно можно найти в различных наборах программ, предназначенных для обеспечения безопасности.
- ✓ Можно запускать несколько антишпионских программ одновременно, например Защитник Windows и какую-нибудь другую. Однако больше двух подобных программ запускать не рекомендуется: нет особого смысла перегружать компьютер обилием антишпионского ПО.

Антивирусная защита

В Windows 8 программа Windows Defender позиционируется как полноценная антивирусная программа, во всяком случае в окне Центр поддержки она считается таковой. Однако вам никто не мешает значительно улучшить защиту своего коимпьютера, установив антивирусную программу от стороннего разработчика, например антивирус Касперского, Dr. Web, Norton AntiVirus, Avast! или Comodo (выберите любую из них). Кстати, последние две программы абсолютно бесплатные.

Установить антивирусную программу очень просто. Найдите выбранный тип программы в Интернете, скачайте и установите ее. Настоятельно рекомендуем загружать антивирусные программы только с официальных сайтов их разработчиков!

Установленная антивирусная программа сканирует компьютер на предмет обнаружения инфицирования вирусами. Программа имеет два режима работы.

Активное сканирование. В режиме активного сканирования (Active Scan) программа просматривает каждый подозрительный файл в компьютере на наличие вирусов. Все файлы компьютера сканируются на регулярной основе.

Перехват. В режиме перехвата (Interception) антивирусная программа сканирует входящие сообщения электронной почты, файлы, передаваемые из других компьютеров, а также всю информацию, загружаемую из Интернета. Вирусы, пытающие прорваться в ваш компьютер, задерживаются и не пропускаются.

Названия “Активное сканирование” и “Перехват” я придумал сам. В вашей антивирусной программе они могут называться иначе, но смысл от этого не изменится.

- ✓ Если антивирусная программа сообщает об опасности инфицирования, не игнорируйте это сообщение! Немедленно поместите инфицированный файл на карантин или удалите его.
- ✓ Применяя режим карантина, антивирусная программа изолирует и блокирует инфицированный файл, не допуская проникновение вируса в компьютер. Файл, помещенный на карантин, не удаляется, но система становится защищенной. При желании этот файл можно удалить позже.

Можно одновременно установить две антивирусные программы, хотя их одновременное использование не допускается – в режиме перехвата может работать *только одна* программа. А вот сканировать компьютер можно с помощью двух и более программ, выполняющихся последовательно одна за другой. В этом случае проблемы, пропущенные одной программой, могут быть обнаружены и исправлены другой.

> ✓ Чтобы открыть окно антивирусной программы, щелкните на ее значке в области уведомлений панели задач.

Причины широкого распространения вирусов кроются в человеческой психологии. Многие пользователи знают, что нельзя открывать сомнительные почтовые вложения, тем не менее вирусы продолжают успешно распространяться именно этим способом. Самым лучшим антивирусным инструментом является ваша собственная голова. Только ваши внимание, бдительность и здравый смысл помогут предотвратить попадание вирусов в компьютер. Конечно, антивирусные программы необходимы, но не настолько, чтобы считаться жизненно важными.

Контроль учетных записей пользователя

В попытках сделать ОС Windows более безопасной Майкрософт предоставила пользователям новую функцию — *Контроль учетных записей пользователя* (User Account Control — UAC). При любой попытке что-либо изменить в Windows (например, какой-либо режим или параметр настройки) или загрузить ту или иную программу из Интернета эта система отображает диалоговые окна с различными предупреждениями. Типичное окно с предупреждением от системы контроля учетных записей пользователя показано на рис. 12.3.

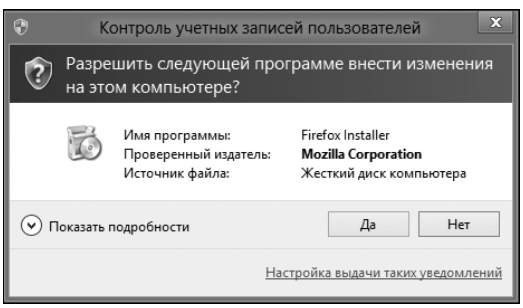

Рис. 12.3. Типичное окно предупреждения системы контроля учетных записей пользователя

Признак работы системы контроля учетных записей — ссылка или кнопка с изображением щита. При появлении предупреждающего сообщения щелкните на кнопке Да (Yes), если действие ожидаемое и требуемое. При необходимости введите пароль администратора, после чего щелкните на кнопке OK.

При появлении неожиданного предупреждающего сообщения системы контроля учетных записей внимательно ознакомьтесь с ситуацией и в случае несанкционированных действий щелкните на кнопке Нет (No). Например, если, работая в Интернете, вы получаете предупреждение об установке того или иного программного обеспечения или изменении вашей домашней страницы, без колебаний щелкайте на кнопке Нет!