ЗАНЯТИЕ №5-6: Встроенная защита в Windows от вредоносного ПО Windows Defender

СОДЕРЖАНИЕ

7. Встроенная защита в Windows от вредоносного ПО Windows Defender

В этом занятии будет рассмотрен «Защитник Windows» (Windows Defender). Этот продукт предлагается Microsoft как технология безопасности, защищающая компьютер от программ-шпионов и других видов нежелательных программ [1]. Предполагается, что этот программный продукт будет интегрирован в Windows Vista, а для пользователей Windows XP этот продукт будет доступен в виде отдельного дополнения [2]. На момент создания данного занятия, на сайте Microsoft доступна бета-версия 2, сборка 1347 этого продукта на английском, немецком и японском языках. После бета-тестирования программа будет переведена на другие языки [3]. Всё дальнейшей описание базируется на возможностях английской версии этой программы.

Прежде всего

Для изучения материалов этого занятия необходимо:

• компьютер под управлением операционной системы Windows XP Professional с настройками по умолчанию.

• выход в Интернет.

7.1. Введение

Microsoft предлагает следующее определение для «шпионского» ПО [4]:

«Шпионскими» называются программы, выполняющие определенные действия (например, показ рекламы, сбор личной информации или изменение настроек компьютера) без ведома и контроля пользователя.

Как указывается в [4,5], вероятными признаками наличия на вашем компьютере «шпионского» либо иного нежелательного программного обеспечения являются:

• Появление всплывающей рекламы, даже когда Вы не находитесь в Интернете.

• Домашняя страница или настройки поиска в обозревателе изменились без вашего ведома.

• Появление в обозревателе новых ненужных панелей инструментов, от которых трудно избавиться.

• Неожиданное значительное снижение производительности.

• Количество сбоев в работе компьютера неожиданно увеличилось.

Как указывается в [5], некоторые из программ-шпионов могут также выполнять следующее:

• регистрировать нажатия клавиш, что позволяет программам-шпионам перехватывать пароли и данные для входа в систему;

• собирать личные данные, такие как идентификационные номера, номера социального страхования (в США) или информацию о банковских счетах, и пересылать их третьим лицам;

• позволять удаленно управлять компьютером для получения доступа к файлам, установки и изменения программного обеспечения, а также использования компьютера для распространения вирусов и других действий.

Все формы программ-шпионов обладают одним общим признаком: они устанавливаются без ведома пользователя и не предоставляют ему сведений о своих действиях [5].

Для защиты от программ-шпионов и вирусов, компания Microsoft предлагает следующие технологии [1,2]:

• Защитник Windows (Windows Defender) (бета-версия 2) - инструмент защиты от «шпионского» ПО. Осуществляет не только поиск и удаление «шпионского» ПО, но и постоянный мониторинг действий пользователя и приложений с целью обнаружения попыток установки на компьютер нежелательного ПО. Основан на технологиях компании GIANT Company Software Inc., приобретенной Microsoft в декабре 2004 года [5,2].

• Windows Live Safety Center — веб-служба, обеспечивающая нормальную работу компьютера благодаря средствам сканирования, удаления нежелательных программ. Также позволяет выполнять резервное копирование файлов и дефрагментацию жестких дисков.

• Средство удаления вредоносных программ (Malicious Software Removal Tool) — средство безопасности, которое проверяет компьютер и удаляет обнаруженные вирусы и другие вредоносные программы. Основано на технологиях приобретенной Microsoft в июне 2003 года румынской антивирусной компании GeCAD.

• Windows Live OneCare - набор средств безопасности, которые почти не требуют вашего вмешательства в своей работе. Помимо антивирусной защиты, осуществляет на компьютере пользователя действия, необходимые для повышения производительности и для обеспечения сохранности данных (управление брандмауэром, резервное копирование, дефрагментация жестких дисков).

• Microsoft Client Protection - средство защиты рабочих, переносных компьютеров и файловых серверов от таких угроз, как программы-шпионы и rootkit, а также от вирусов и других традиционных способов атаки. В отличие от OneCare, данный продукт не содержит брандмауэра, средств мониторинга производительности и инструментов резервного копирования.

В табл. 7.1 приведены сравнительные характеристики перечисленных выше технологий защиты Microsoft от программ-шпионов и вирусов [1].

Таблица 7.1

Сравнение технологий защиты Microsoft от программ-шпионов и вирусов

Название продукта и целевые пользователи	**Сдерживание программ-шпионов и других нежелательных программ**		**Сдерживание вирусов и вредоносного ПО**		**Сканирование по расписанию**	**Предоставляется без дополнительной платы**
	Сканирование и удаление	Защита	Сканирование и удаление	Защита		
Защитник Windows (**бета- версия** 2) (**клиенты**)						
Windows Live Safety Center (**клиенты**)						
Malicious Software Removal Tool (**клиенты и предприятия**)						
Windows Live OneCare (**клиенты**)						
Microsoft Client Protection (**предприятия**)						

7.2. Установка Windows Defender

Для установки программы вам необходимы права администратора на локальном компьютере. Процесс инсталляции очень прост и после окончания не требует перезагрузки компьютера.

После установки, для запуска программы достаточно привилегий обычного пользователя, но некоторые действия могут требовать привилегий администратора.

7.2.1. Требования к системе

Как указывается в [6], минимальными требованиями для установки являются:

•Процессор -Intel Pentium с частотой не менее 233 МГц. Рекомендуется Pentium III.

•Операционная система: Microsoft Windows 2000 с пакетом обновления 4 (SP4) или более поздним, Windows XP с пакетом обновления 2 (SP2) или более поздним, Windows Server 2003 с пакетом обновления 1 (SP1) или более поздним.

- ОЗУ: не менее 64 МБ; рекомендуется 128 МБ.
- 20 МБ свободного места на жестком диске.
- Microsoft Internet Explorer 6.0 или выше.
- Подключение к Интернету со скоростью не менее 28,8 Кбит/с.
- Windows Installer версии 3.1 или выше.

7.2.2. Шаг 1. Загрузка Защитника Windows

Для установки приложения необходимо загрузить установщик с веб-узла центра загрузки Microsoft [7]. Для этого на «Домашней странице Защитника Windows» [3] щелкните по надписи «Загрузить здесь» (рис. 7.1).

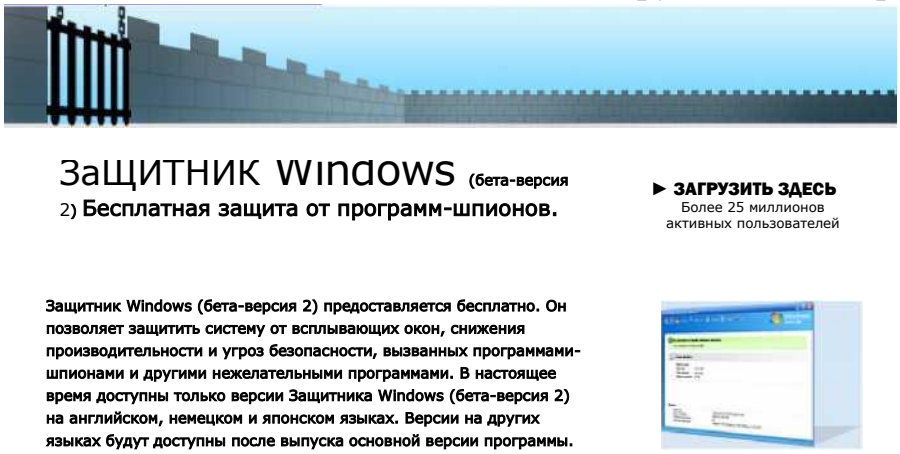


Рис. 7.1. Фрагмент домашней страницы Защитника Windows Защитник Windows является бесплатной программой для владельцев лицензионно чистой версии Windows. Поэтому на появившейся странице, перед загрузкой установщика, вам предлагается проверить подлинность вашей версии Windows. Об этом свидетельствует надпись «Validation Required» на странице загрузки (рис. 7.2) [7].

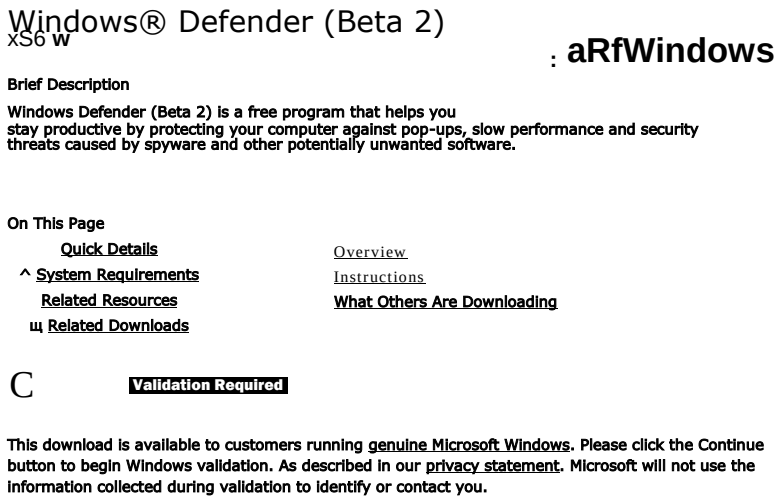


Рис. 7.2. Фрагмент страницы загрузки Защитника Windows Нажмите кнопку «Continue» для проверки операционной системы вашего компьютера. После этого вы перейдете на страницу установки компонента проверки подлинности Windows (the Genuine Windows Validation Component) (рис. 7.3). Этот компонент является элементом управления ActiveX под названием «Windows Genuine Advantage». В соответствии с настройками по умолчанию, в Internet Explorer (версия, входящая в состав Windows XP SP2) запрещена автоматическая установка элементов ActiveX. Об этом свидетельствует появившаяся панель информации со значком

Для продолжения установки необходимо выполнить щелчок левой кнопкой мыши по этой панели (рис. 7.3). В появившемся меню (рис. 7.4) выберите команду «Установить элемент управления ActiveX...».

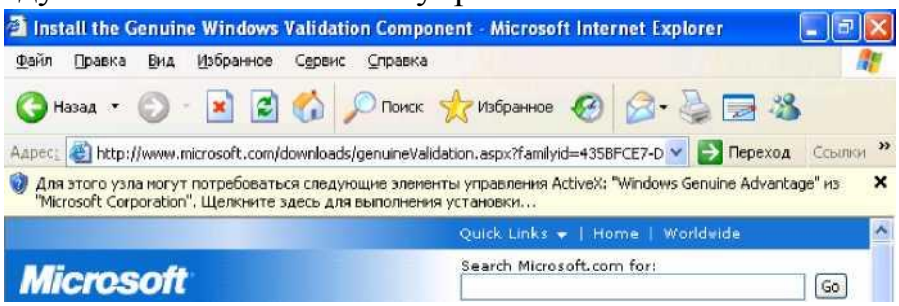


Рис. 7.3. Страница установки компонента проверки подлинности Windows

Рис. 7.4. Меню панели информации

После появления предупреждения системы безопасности об установке ActiveX компонента, нажмите кнопку «Установить» (рис. 7.5).

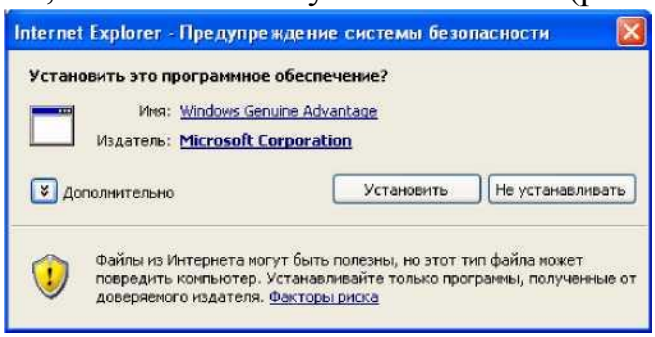


Рис. 7.5. Предупреждение системы безопасности

После успешной проверки вашей операционной системы, вы вернетесь на страницу загрузки Защитника Windows. Но внешний вид этой страницы теперь будет другой. Вместо кнопки «Continue» (рис. 7.2) будет кнопка «Download» (рис. 7.6).

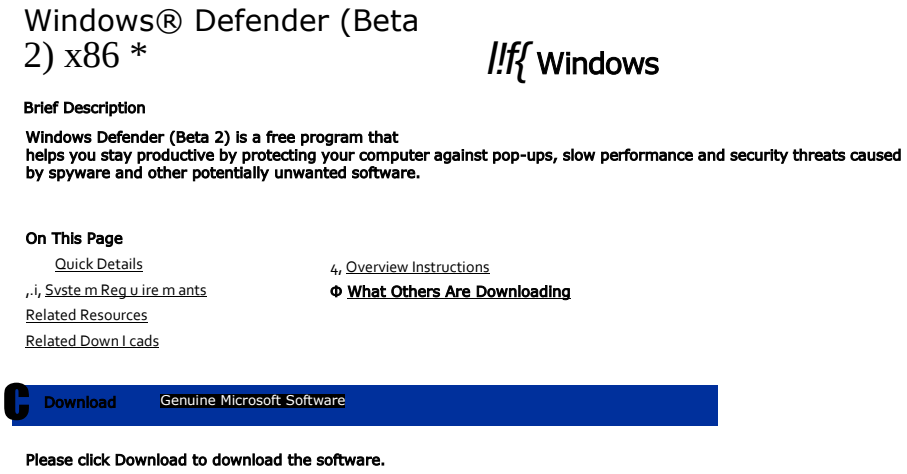


Рис. 7.6. Страница загрузки Защитника Windows после проверки ОС

Выберите язык интерфейса Защитника Windows с помощью параметра «Change Language» и нажмите кнопку «Download» (рис. 7.7). Как было указано ранее, на момент написания этого текста существовали версии Защитника Windows только на английском, немецком и японском языках.

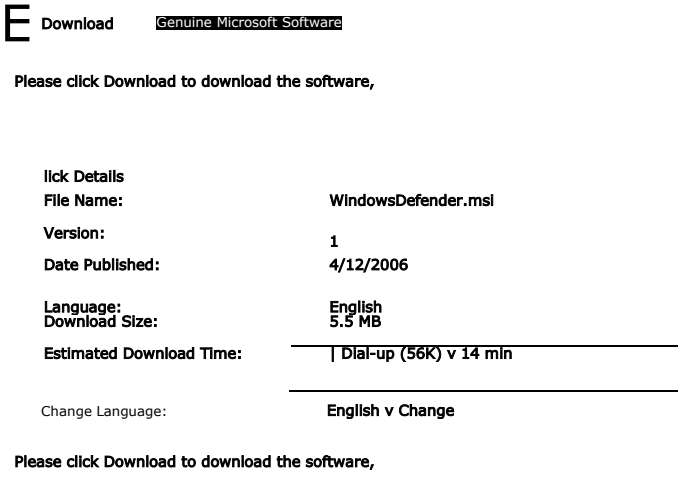


Рис. 7.7. Краткая информация о загружаемом файле После появления предупреждения системы безопасности, нажмите кнопку «Сохранить» (рис. 7.8) и выберите место для сохранения файла `WindowsDefender.msi`. Если во время установки Защитника Windows возникнут ошибки, вы всегда сможете запустить установку повторно, если сохраните установщик на диск.

Рис. 7.8. Предупреждение системы безопасности

7.2.3. Шаг 2. Запуск установщика Защитника Windows

После того как вы загрузили на свой компьютер установщик Защитника Windows, можно приступать к собственно установке. Запустите файл `WindowsDefender.msi`. Если после запуска вы увидите окно приветствия Мастера установки (см. рис. 7.9), то перейдите к шагу 5 (пункт 7.2.6). Если вы увидите сообщение об отсутствии Windows Installer 3.1 представленное на рис. 7.10, то перейдите к пункту 7.2.4. Если вы увидите сообщение о необходимости обновления службы Windows Update представленное на рис. 7.11, то перейдите к пункту 7.2.5.

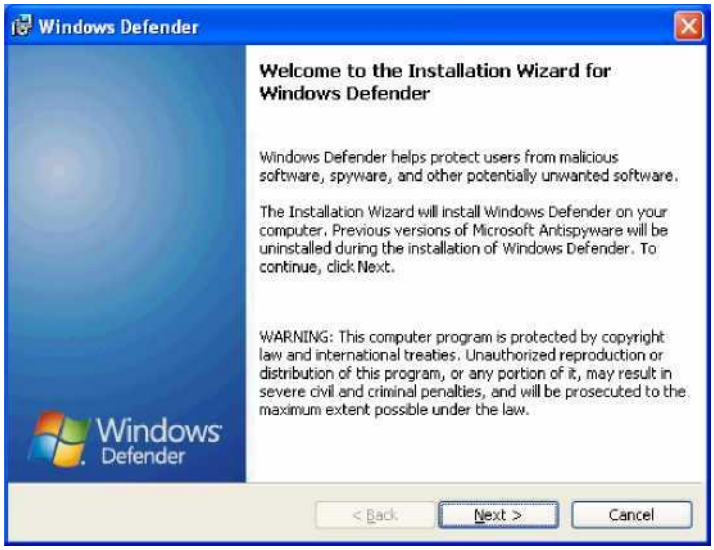


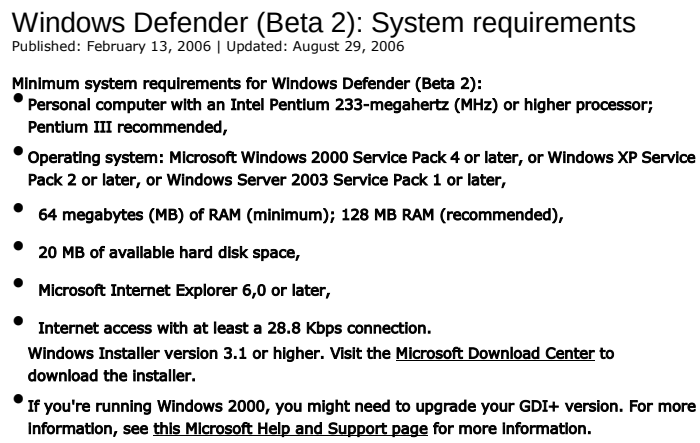
Рис. 7.9. Приветствие Мастера установки

Рис. 7.10. Сообщение об отсутствии Windows Installer 3.1

Рис. 7.11. Сообщение о необходимости обновить службу Windows Update

7.2.4. Шаг 3. Установка Windows Installer 3.1

Как указано на рис. 7.10 для установки Защитника Windows необходимо наличие на компьютере приложения Windows Installer версии 3.1 или выше. Чтобы получить подробные требования к установке, необходимо посетить сайт http://go.microsoft.com/fwlink/?LinkId=63848 (рис. 7.12). Кроме описанных ранее системных требований, на этой странице есть также ссылка на Microsoft Download Center (рис. 7.12). Перейдя по этой ссылке, вы получите возможность скачать на свой компьютер Windows Installer последней версии (рис. 7.13).



Windows Defender (Beta 2): System requirements

Published: February 13, 2006 | Updated: August 29, 2006

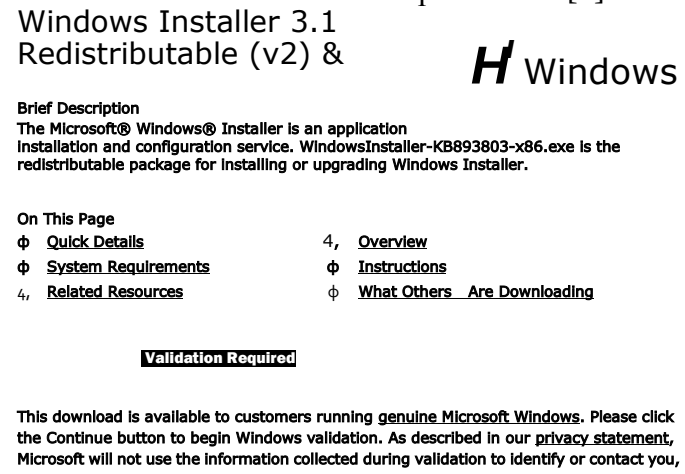
Minimum system requirements for Windows Defender (Beta 2):

- Personal computer with an Intel Pentium 233-megahertz (MHz) or higher processor; Pentium III recommended,
- Operating system: Microsoft Windows 2000 Service Pack 4 or later, or Windows XP Service Pack 2 or later, or Windows Server 2003 Service Pack 1 or later,
- 64 megabytes (MB) of RAM (minimum); 128 MB RAM (recommended),
- 20 MB of available hard disk space,
- Microsoft Internet Explorer 6,0 or later,
- Internet access with at least a 28.8 Kbps connection.

Windows Installer version 3.1 or higher. Visit the Microsoft Download Center to download the installer.

- If you're running Windows 2000, you might need to upgrade your GDI+ version. For more information, see this Microsoft Help and Support page for more information.

Рис. 7.12. Системные требования [8]



Windows Installer 3.1 Redistributable (v2) &

Windows

Brief Description

The Microsoft® Windows® Installer is an application installation and configuration service. WindowsInstaller-KB893803-x86.exe is the redistributable package for installing or upgrading Windows Installer.

On This Page

- Quick Details
- System Requirements
- Related Resources
- Overview
- Instructions
- What Others Are Downloading

Validation Required

This download is available to customers running genuine Microsoft Windows. Please click the Continue button to begin Windows validation. As described in our privacy statement, Microsoft will not use the information collected during validation to identify or contact you,

Рис. 7.13. Страница загрузки Windows Installer 3.1 Как вы видите на рис. 7.13, для загрузки Windows Installer 3.1 также требуется проверка подлинности операционной системы. Эта проверка выполняется аналогично описанной ранее на шаге 1 (см. п. 7.2.2). После её выполнения загрузите файл WindowsInstaller-KB893803-v2-x86.exe и запустите его. Следуйте инструкциям Мастера установки. По окончании установки, не забудьте перезагрузить компьютер.

Вернитесь к шагу 2 (п. 7.2.3) и попробуйте повторно начать установку Защитника Windows.

7.2.5. Шаг 4. Обновление службы Windows Update

Как указано на рис. 7.11, для установки Защитника Windows необходимо обновить на вашем компьютере службу Windows Update. Для этого запустите Internet Explorer и выполните команду меню «Сервис | Windows Update» или перейдите по адресу «http://windowsupdate.microsoft.com/». Через несколько секунд вы увидите предупреждение системы безопасности с предложением установить приложение Windows Update (рис. 7.14). Нажмите кнопку «Установить». Если после установки потребуется переза-

грузка - выполните её. Вернитесь к шагу 2 (п. 7.2.3) и попробуйте повторно начать установку Защитника Windows.

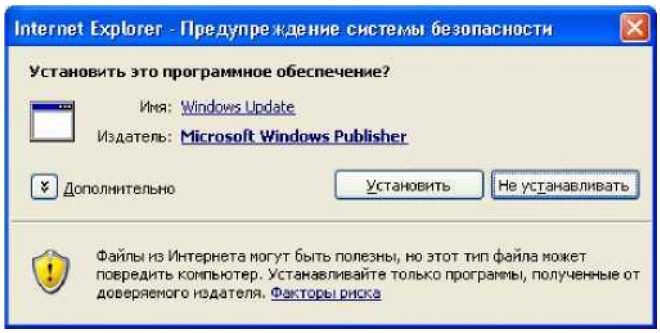


Рис. 7.14. Предупреждение системы безопасности

7.2.6. Шаг 5. Мастер установки Защитника Windows

После появления на экране окна приветствия Мастера установки (рис. 7.9), нажмите кнопку «Next». Прочтите лицензионное соглашение (рис. 7.15). Если Вы его принимаете, то выберите «I accept the terms in the license agreement» и нажмите кнопку «Next».

Рис. 7.15. Лицензионное соглашение

На следующей странице Вам будет предложено вступить в сообщество Microsoft SpyNet (рис. 7.16). Microsoft рекомендует выбрать первый вариант («Use recommended settings») [9]. В этом случае вы будите автоматически получать обновления информации о «шпионских» программах и вступите в сообщество Microsoft SpyNet.

Рис. 7.16. Предложение вступить в сообщество Microsoft SpyNet

Сообщество Microsoft SpyNet (или сеть голосования) позволяет входящим в неё пользователям получать информацию о программах, которые были запрещены, удалены или разрешены другими пользователями при работе с Защитником Windows. Кроме того, ваши решения по этому вопросу также будут доступны другим пользователям. Данные о решениях пользователей отображаются в Защитнике Windows (бета-версия 2) в виде графика, который содержит информацию о процентном соотношении людей, разрешивших, запретивших или удаливших конкретную программу [10].

Если вы не хотите вступать сообщество Microsoft SpyNet, но желаете получать обновления информации о «шпионских» программах, то выберите вариант «Install definition updates only».

При выборе варианта «Ask me later» вы не будете получать обновления и вступать в сообщество Microsoft SpyNet.

Выберите первый вариант и нажмите кнопку «Next». На следующей странице вам будет предложено выбрать тип установки: полная («Complete») или выборочная («Custom») (рис. 7.17). Выберите вариант «Complete» и нажмите кнопку «Next».

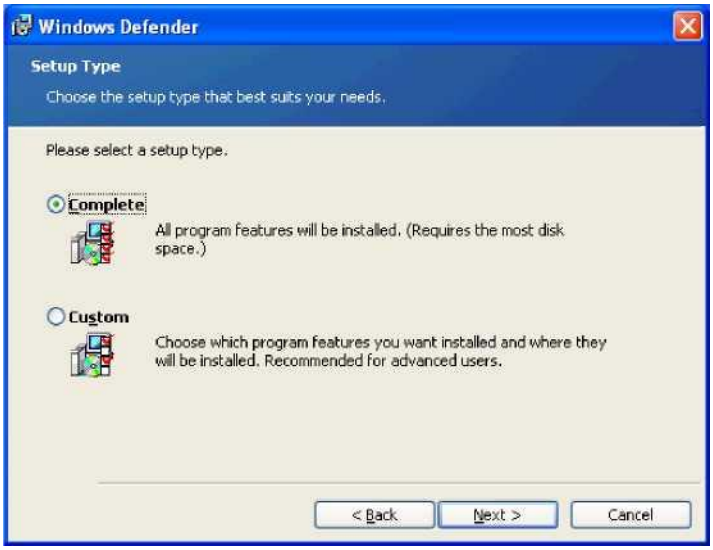


Рис. 7.17. Выбор типа установки

На следующем экране вам будет сообщено о готовности к установке Защитника Windows (рис. 7.18). Нажмите кнопку «Install».

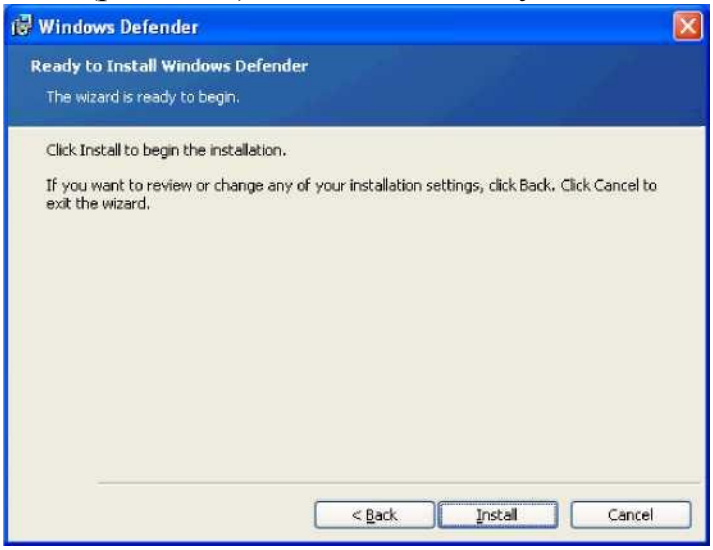


Рис. 7.18. Готовность к установке

После завершения установки появится соответствующая страница с предложением проверить наличие обновлений информации о «шпионских» программах и запустить быстрое сканирование вашего компьютера (рис. 7.19). Нажмите кнопку «Finish».

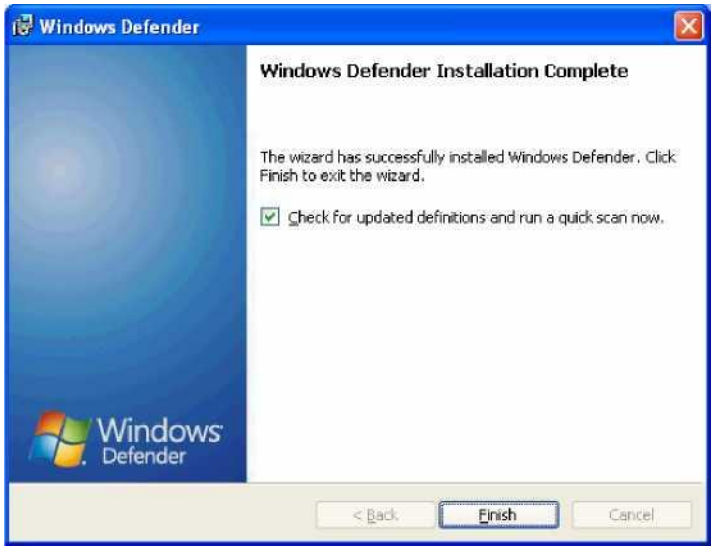


Рис. 7.19 Успешное завершение установки Для запуска Защитника Windows в меню «Пуск» выберите пункт «Все программы», а затем - пункт «Windows Defender» (Защитник Windows) (рис. 7.20).

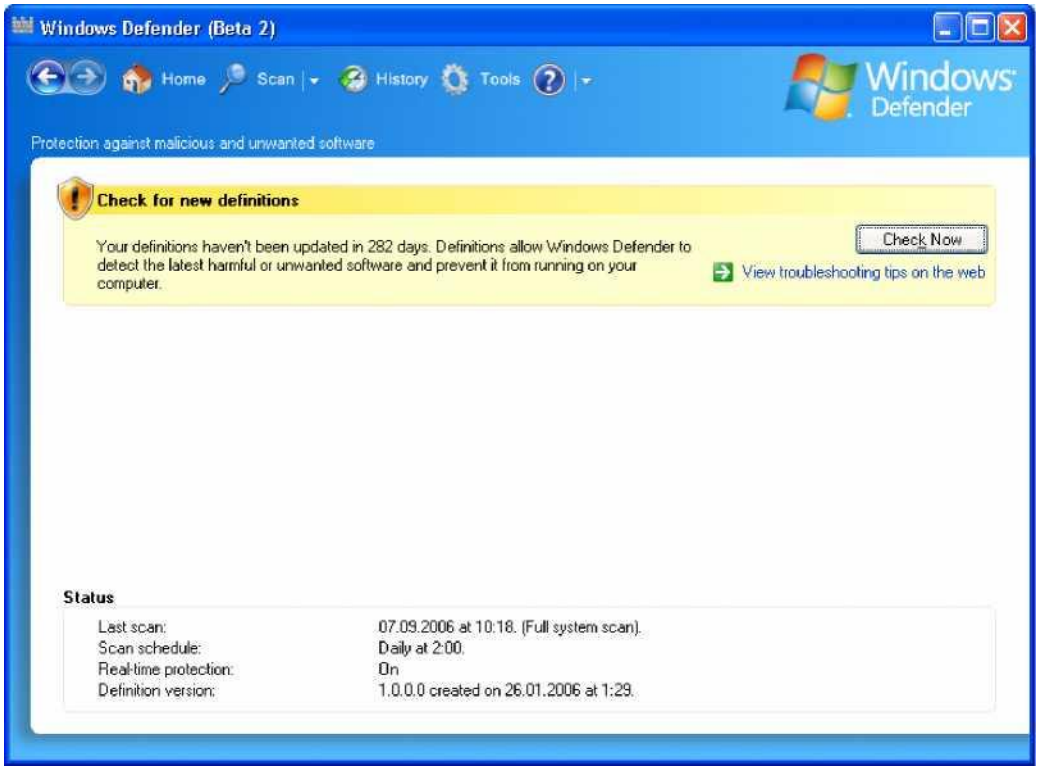


Рис. 7.20 Главное окно Защитника Windows.

7.3. Настройки Windows Defender

Для просмотра и изменения параметров работы Защитника Windows на панели инструментов выберите «Tools» (Сервис) (рис. 7.20) и в появившейся странице (см. рис. 7.21) выберите пункт «Options».

Рис. 7.21 Страница «Tools» (Сервис)

Настройки Защитника Windows состоят из пяти разделов:

• Automatic scanning (автоматическое сканирование) (рис. 7.22).

• Default actions (действия по умолчанию) (рис. 7.23).

• Real-time protection options (настройки постоянной защиты или защита в реальном времени) (рис. 7.24).

• Advanced options (расширенные настройки) (рис. 7.25).

• Administrator options (настройки Администратора) (рис. 7.26).

Если Вы измените любой из параметров, то для сохранения этих изменений, необходимо нажать кнопку «Save» внизу экрана.

Рассмотрим каждый из этих разделов более подробно.

7.3.1. Automatic scanning (автоматическое сканирование)

В этом разделе сосредоточены настройки планирования проверки компьютера на наличие программ-шпионов и других потенциально нежелательных программ. Параметр «Automatically scan my computer (recommended)» (Автоматически сканировать мой компьютер [рекомендуется]) позволяет включить автоматическую проверку компьютера (рис. 7.22).

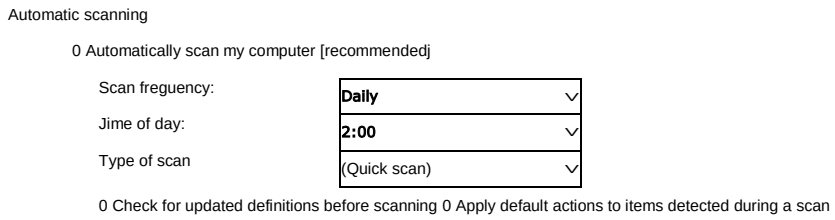


Рис. 7.22 Настройки автоматического сканирования

Параметр «Scan frequency:» (частота сканирования) позволяет задать периодичность автоматического сканирования. Доступны варианты: «Daily» (ежедневно), «Понедельник», «Вторник», ..., «Воскресенье».

Параметр «Time of day:» (время дня) определяет время начала сканирования.

Параметр «Type of scan:» (тип сканирования) позволяет выбрать, какая проверка будет выполняться: «Quick scan» (быстрая проверка) или «Full system scan» (полная проверка системы). При быстрой проверке проверяются те области компьютера, которые наиболее подвержены воздействию нежелательного программного обеспечения. При полной проверке системы проверяются все файлы на жестком диске и все выполняемые в данный момент программы. При этом возможно замедление работы компьютера до завершения сканирования. Microsoft рекомендует запланировать ежедневную быструю проверку, а в случае подозрения на заражение компьютера программами-шпионами - выполнять полную проверку системы [11].

Параметр «Check for updated definitions before scanning» позволяет перед сканированием компьютера проверить наличие обновлений информации о нежелательных программах на сервере обновлений Windows.

Параметр «Apply default actions to items detected during a scan» позволяет при обнаружении нежелательного программного обеспечения выполнять действия по умолчанию заданные в следующем разделе (см. след. пункт). Если этот параметр выключен, то при обнаружении программ- шпионов и других потенциально нежелательных программ Защитник Windows будет запрашивать у пользователя что необходимо сделать с обнаруженным подозрительным объектом.

7.3.2. Default actions (действия по умолчанию).

В этом разделе Вы можете определить, какие действия необходимо выполнять при обнаружении подозрительных объектов (рис. 7.23). Для различных типов предупреждений (high - высокий, medium - средний, low - низкий) вы можете задать свой вариант реагирования. Доступны следующие варианты:

• Definition recommended action (установлено рекомендованное действие).

• Ignore (игнорировать подозрительный объект и разрешить ему выполняться).

• Remove (удалить объект и не допустить его выполнение).

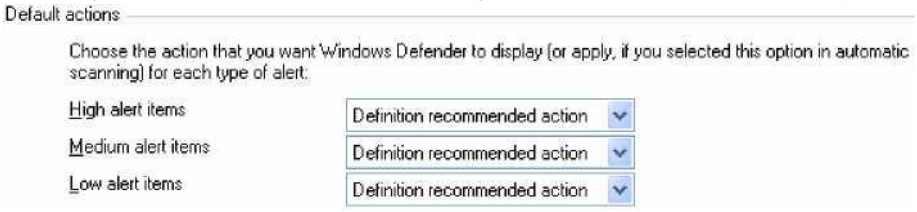


Рис. 7.23 Действия по умолчанию

7.3.3. Real-time protection options (настройки постоянной защиты).

В этом разделе находятся настройки связанные с защитой в реальном времени (рис. 7.24).

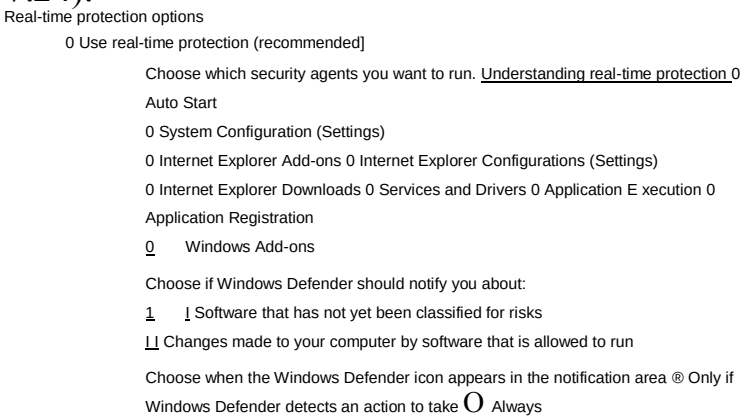


Рис. 7.24 Настройки защиты в реальном времени

Защита в реальном времени (постоянная защита) контролирует состояние важнейших компонентов операционной системы (ОС). Когда посторонние программы производят изменения в настройках ОС или пытаются установиться на компьютер, защита в реальном времени фиксирует эти действия и уведомляет об этом пользователя [10].

Параметр «Use real-time protection (recommended)» (использовать защиту в реальном времени [рекомендуется]) позволяет включить или выключить постоянную защиту.

Ниже перечислены агенты безопасности, контролирующие различные компоненты ОС. Вы можете включить или выключить нужные Вам компоненты, но Microsoft рекомендует не выключать защиту в реальном времени и использовать все существующие агенты безопасности. В табл. 7.2. представлено назначение каждого агента, взятое из встроенной помощи Защитника Windows.

Таблица 7.2

Агенты безопасности защиты в реальном времени

Агент	Назначение
Auto Start	Контроль списка программ автоматически запускающихся при старте компьютера
System Configuration (settings)	Контроль настроек связанных с безопасностью Windows
Internet Explorer Add-ons	Контроль программ, которые автоматически запускаются при старте Internet Explorer
Internet Explorer Configurations (settings)	Контроль настроек безопасности Internet Explorer
Internet Explorer Downloads	Контроль файлов и программ, которые спроектированы для работы с Internet Explorer (например, элементы управления ActiveX и программы установки программного обеспечения из Интернета)
Services and Drivers	Контроль служб и драйверов
Application Execution	Контроль запускающихся программ и действий, которые они выполняют
Application Registration	Контроль утилит и файлов операционной системы предназначенных для запуска программ (например, по расписанию)
Windows Add-ons	Контроль дополнений (также известных как программные утилиты) для Windows

Следующие два параметра определяют, будет ли Защитник Windows уведомлять пользователя:

•о программном обеспечении, которое ещё не было классифицировано по степени риска от его использования (параметр «Software that has not yet been classified for risks»);

•об изменениях выполненных на Вашем компьютере разрешенным программным обеспечением (параметр «Changes made to you computer by software that is allowed to run»).

Следующий параметр («Choose when the Windows Defender icon appears in the notification area») определяет, когда будет появляться значок Защитника Windows в области уведомления (правая нижняя часть экрана). Вариант «Always» соответствует постоянному наличию значка. Вариант «Only if Windows Defender detects an action to take» соответствует отображению значка только в случае возникновения какого-либо события. Например, когда Защитник Windows давно не соединялся с сервером обновлений Windows и не скачивал новые описания нежелательных программ.

7.3.4. Advanced options (расширенные настройки)

В этом разделе (рис. 7.25) находятся следующие параметры, название которых говорит само за себя:

•«Scan the contents of archived files and folders for potential threats» (сканировать содержимое архивных файлов и папок в поисках потенциальной угрозы). К сожалению, в справке Защитника Windows отсутствует информации о типах поддерживаемых архивов.

•«Use heuristics to detect potentially harmful or unwanted behavior by software that hasn’t been analyzed for risks» (использовать эвристический анализ для обнаружения потенциально опасных или нежелательных про

грамм, которые ещё не были проанализированы разработчиком Защитника Windows).

• «Do not scan these files or location» (не сканировать указанные файлы или папки). Для задания списка файлов или папок, не подлежащих проверке, нажмите кнопку «Add...». Кнопка «Remove» позволяет удалить из этого списка ранее указанные файлы или папки.

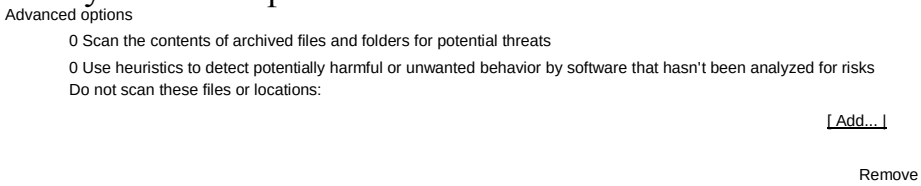


Рис. 7.25 Расширенные настройки

7.3.5. Administrator options (настройки Администратора)

В этом разделе (рис. 7.26) находятся следующие настройки:

• «Use Windows Defender» (включить Защитника Windows). Если этот параметр включен - все пользователи будут получать предупреждения в случае обнаружения шпионского ПО или выполнения нежелательных действий. Защитник Windows будет периодически проверять наличие обновлений на сервере обновлений Windows, регулярно проверять Ваш компьютер и автоматически удалять нежелательное ПО обнаруженное при сканировании.

• «Allow users to use Windows Defender» (разрешить пользователям использовать Защитник Windows). Если этот параметр включен, пользователи, не обладающие административными привилегиями, смогут взаимодействовать с Защитником Windows.

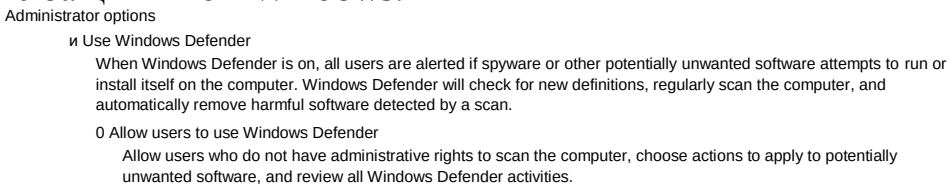


Рис. 7.26 Настройки Администратора

7.4. Обновление Windows Defender

Защитник Windows работает тем эффективнее, чем большей информацией о существующих в мире шпионских и прочих нежелательных программах он обладает. Эту информацию Windows Defender получает с сервера обновлений Windows (Windows Update). Соответственно, если Ваш компьютер настроен на автоматическое обновление («Пуск», «Панель управления», «Центр обеспечения безопасности», рис. 7.27) и периодиче-

ски получает обновления с сервера Windows Update, то Защитник Windows будет также получать свои обновления.

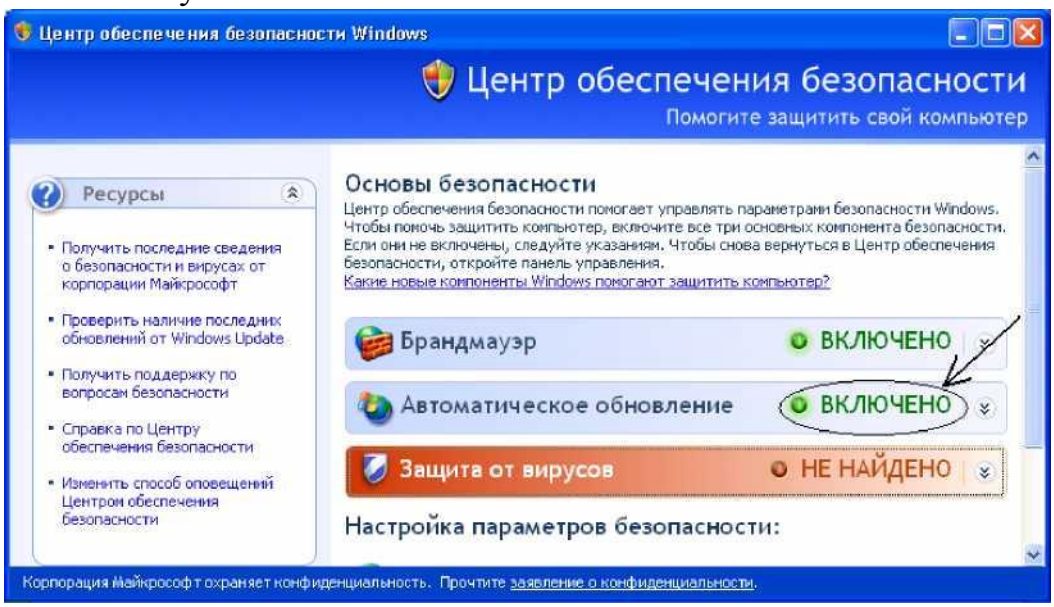


Рис. 7.27 Автоматическое обновление включено Информация о том, какая версия информационных баз сейчас используется Защитником Windows, отображается на главной странице (рис. 7.28). После установки Защитника Windows (Beta 2), версия информационных баз (Definition version) 1.0.0.0. Они созданы 26.01.2006 (рис. 7.28). Если Защитник Windows считает, что базы устарели, то на главной странице появляется предупреждение (рис. 7.28).

Рис. 7.28 Главная страница Защитника Windows Для того чтобы скачать свежие обновления с сервера Microsoft, нажмите кнопку «Check Now». В области уведомления (правая часть панели задач) появится значок с сообщением «Windows Defender is connecting to the Internet to acquire new definitions and engine upgrades» (рис. 7.29). Сообщение говорит о том, что Защитник Windows соединяется с Интернет для по-

лучения новых определений и обновления модуля обнаружения нежелательного ПО.

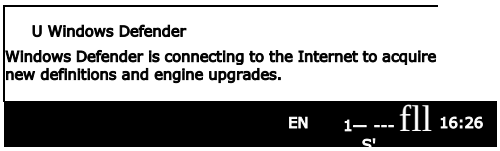


Рис. 7.29 Сообщение о соединении с Интернет

Примечание: На самом деле, если в Вашей организации развернут внутренний сервер обновлений (например, Microsoft Windows Server Update Services, WSUS) и Ваш компьютер для получения обновлений настроен на соединение с этим сервером, то Защитник Windows будет соединяться не с Интернет, а с внутренним сервером обновлений. Настройка внутреннего сервера обновлений не входит в тему данного занятия. Однако отметим, что сервер WSUS по умолчанию не скачивает из Интернета обновления определений для Защитника Windows и его необходимо соответствующим образом настраивать.

После успешного получения последних обновлений, в области уведомления появится сообщение «Windows Defender is up-to-date with definitions and engine upgrades» (Защитник Windows содержит последние определения и обновления модуля обнаружения нежелательного ПО) (рис. 7.30).

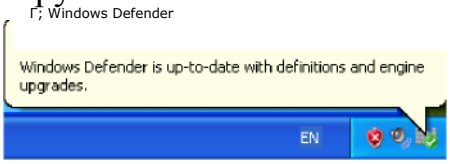


Рис. 7.30 Сообщение об успешности получения обновлений После этого, главная страница изменит своё содержание (см. рис. 7.31).

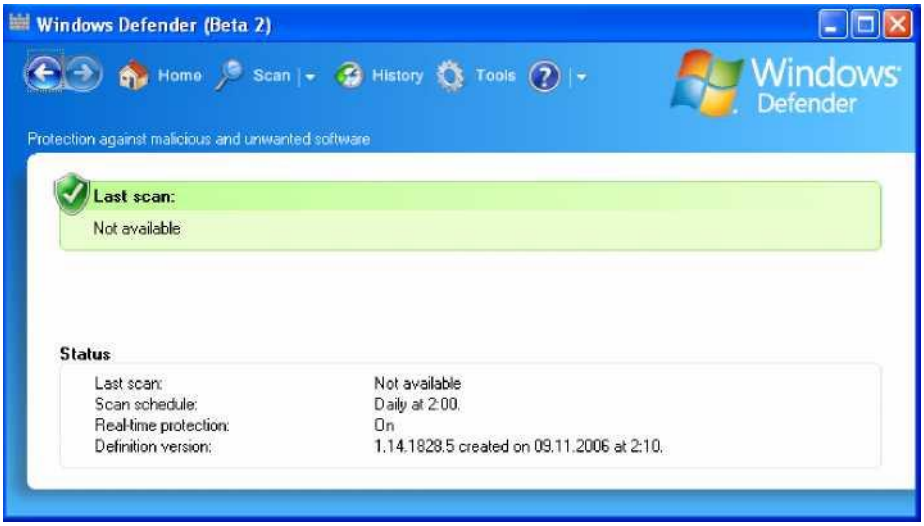


Рис. 7.31 Главная страница Защитника Windows

7.5. Проверка компьютера

Для того чтобы проверить Ваш компьютер на наличие шпионского и другого нежелательного ПО необходимо выполнить сканирование с помощью Защитника Windows. Существует три типа сканирования:

- Quick Scan (быстрое сканирование).
- Full Scan (полное сканирование).
- Custom Scan... (выборочное сканирование).

При быстрой проверке проверяются те области на жестком диске, заражение которых программами-шпионами наиболее вероятно [11]. В этом режиме проверяются не только системные папки Windows, но и важные для безопасности ветки реестра. В режиме полной проверки проверяются не только все файлы на жестком диске, но и все выполняемые в данный момент программы. Как указывается в [11], при выполнении полной проверки компьютера возможно замедление работы системы. Поэтому рекомендуется настроить Защитник Windows на ежедневную быструю проверку, а при подозрении на заражение компьютера программами-шпионами, выполнять полную проверку системы.

Выборочное сканирование позволяет провести сканирование только выбранных дисков и папок.

Для выбора нужного Вам режима сканирования компьютера, нажмите треугольник (П) рядом с кнопкой «Scan» на панели задач Защитника Windows. Если сразу нажать кнопку «Scan», то будет выполнена быстрая проверка компьютера (рис. 7.32).

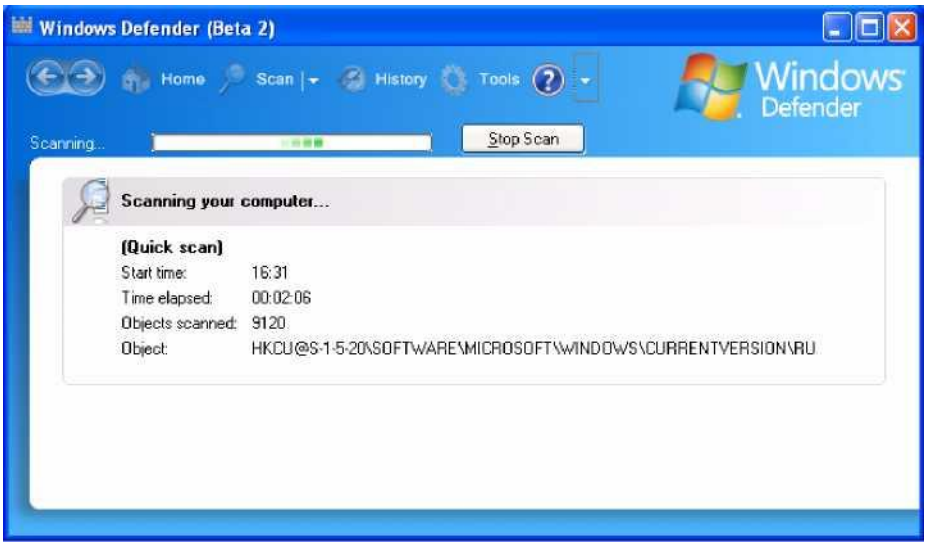


Рис. 7.32 Быстрая проверка компьютера

После её выполнения на экран будет выведена статистка проверки. На рис. 7.33 представлен результат проверки не обнаружившей подозрительных объектов.

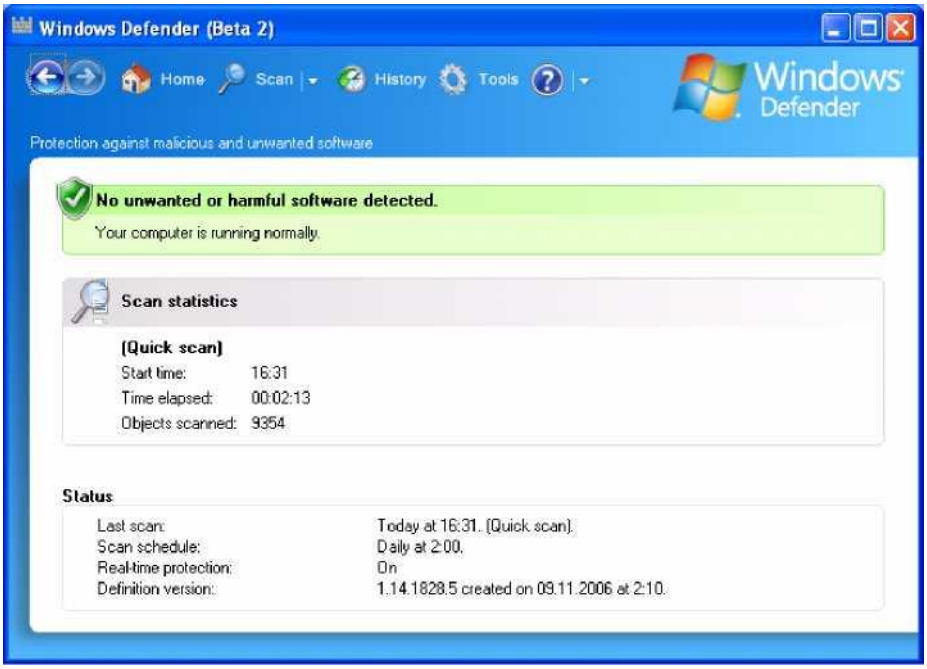


Рис. 7.33 Результат быстрой проверки

7.5.1. Обнаружение подозрительных действий

Для того чтобы получать уведомления обо всех подозрительных действиях, совершаемых на Вашем компьютере, необходимо в разделе «Choose if Windows Defender should notify you about:» включить параметр «Software that has not yet been classified for risks» (см. п. 7.3.3). В этом случае, Защитник Windows будет предупреждать Вас обо всех подозрительных действиях. Иначе (по умолчанию этот параметр выключен), он будет предупреждать Вас только о тех действиях (и тех программах), информация о которых входит в определения (definitions), созданные разработчиками Защитника Windows.

На рис. 7.34 представлено сообщение об обнаруженных подозрительных действиях. Для того чтобы узнать, что обнаружил Защитник Windows, необходимо щелкнуть по этому сообщению или дважды щелкнуть левой кнопкой мыши по значку Защитника Windows. На экране появится окно с указанием обнаруженных событий (рис. 7.35),

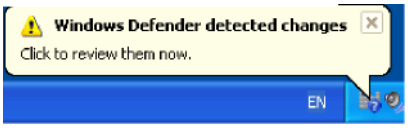


Рис. 7.34 Обнаружены подозрительные действия

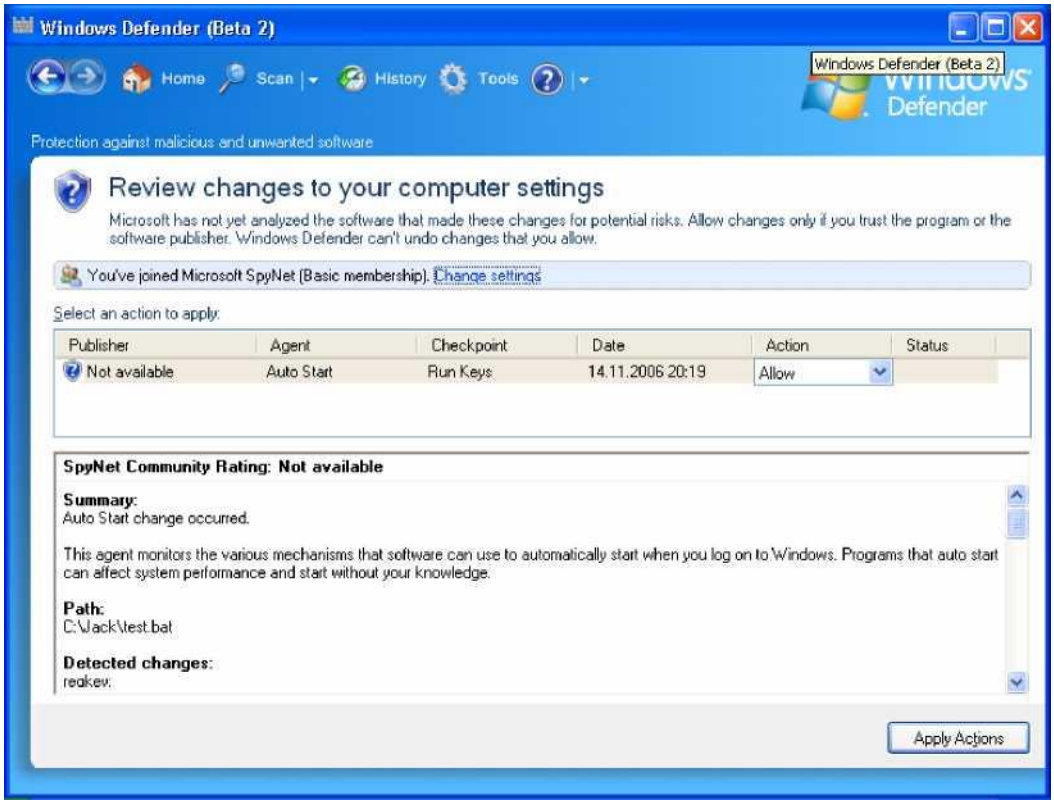


Рис. 7.35 Выбор действия

Обнаруженные события перечислены в виде таблицы в средней части экрана. В нижней части экрана, для выделенного в данный момент события, отображается более подробная информация (рис. 7.36). В разделе «Summary» отображается общая информация по событию. Далее идет более подробное описание. В разделе «Path» указывается расположение файла вызвавшего данное событие. В разделе «Detected changes» - зафиксированные в системе изменения. В разделе «Advice» дается совет: что в данном случае следует предпринять.

Summary:
Auto Start change occurred.

This agent monitors the various mechanisms that software can use to automatically start when you log on to Windows. Programs that auto start can affect system performance and start without your knowledge.

Path:
C:\Jack\test.bat

Detected changes:
regkey:
HKCU@S-1-5-21-776561741-1343024091-854245398-1004\Software\Microsoft\Windows\CurrentVersion\RunWtest.bat

runkey:
HKCU@S-1-5-21-776561741-1343024091-854245398-1004\Software\Microsoft\Windows\CurrentVersion\RunWtest.bat

file:

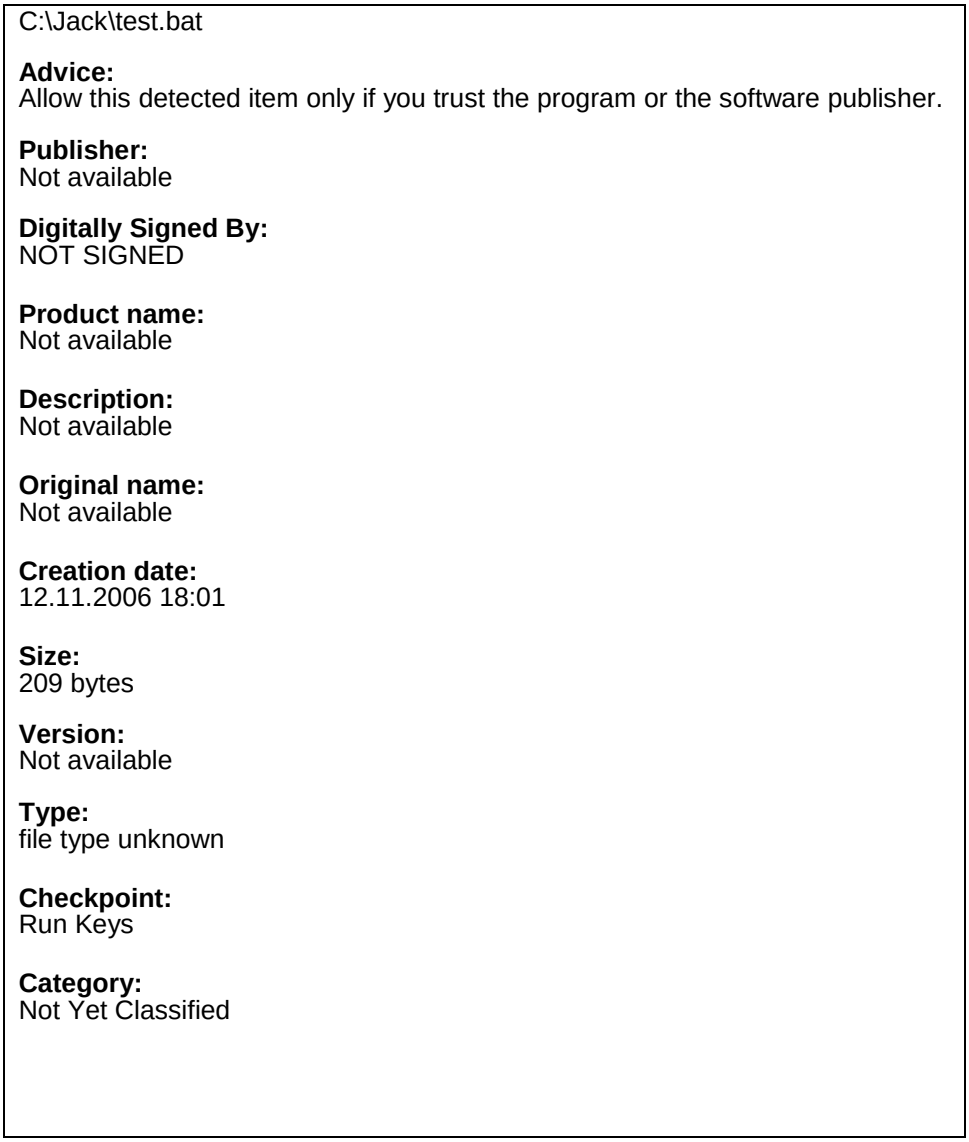


Рис. 7.36 Подробное описание подозрительного события Если Вы доверяете разработчику той программы, которая вызвала это событие, то в столбце «Action» выберите вариант «Allow» (рис. 7.35). Иначе выберите вариант «Block». В последнем случае, действия, которые были выполнены указанной программой, будут отменены. После выбора нужных действий для всех событий, нажмите кнопку «Apply Actions». Если указанное Вами действие (Block или Allow) удалось выполнить, в столбце «Status» будет выведено «Succeeded» (Рис. 7.37).

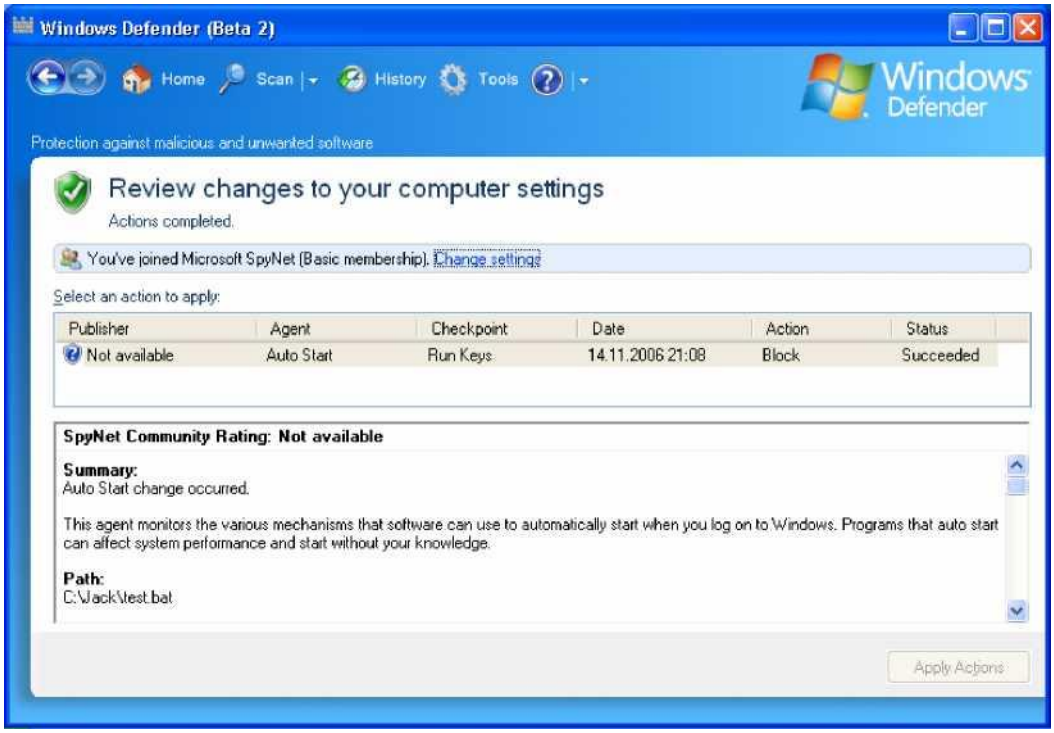


Рис. 7.37 Ваши действия были применены

7.5.2. Обнаружение программ-шпионов

В предыдущем пункте был описан пример обнаружения так называемого «не классифицируемого события». У такого события в разделе «**Category:**» (категория) отображается «Not Yet Classified» (см. рис. 7.36). По умолчанию, пользователю о таких событиях не сообщается (см. п. 7.5.1), но они фиксируются в окне «History» (История). Если информация о приложении или событии существует в информационных базах (определениях) Защитника Windows, то предупреждение о таком событии выглядит иначе (см. рис. 7.38).

Рис. 7.38 Сообщение с уровнем «Medium»

В данном случае Защитник Windows зафиксировал событие с предупреждающим уровнем (Alert level) «Medium» (средний) (рис. 7.38). Как

указывается в справке, уровни предупреждения (alert levels) помогают пользователю принять правильное решение о том, как реагировать на обнаруженное шпионское или нежелательное ПО. Не смотря на то, что Защитник Windows будет рекомендовать Вам удалить (кнопка «Remove All») программу, не все обнаруженные программы являются опасными или не желательными. В табл. 7.3 представлена информация, помогающая Вам решить что делать, если Защитник Windows обнаружил не желательное ПО на Вашем компьютере.

Таблица 7.3

Уровни предупреждения

Уровень предупреждения	Что означает	Что делать
Severe (Тяжелый**)**	Широко распространенные или исключительно опасные программы (например, вирусы или черви), которые наносят ущерб вашей личной информации и защите вашего компьютера. Эти программы могут повредить ваш компьютер.	Немедленно удалите эту программу.
High (Высокий**)**	Программы, которые могут собирать Вашу личную информацию и повредить ваш компьютер. Например, без Вашего ведома или согласия собирают информацию или меняют настройки Вашего компьютера.	Немедленно удалите эту программу.
Medium (Средний**)**	Программы, которые могут влиять на Вашу личную информацию или выполнять изменения на Вашем компьютере.	Просмотрите подробности этого предупреждения, чтобы выяснить, почему это программа была обнаружена. Если Вам не нравятся те действия, которые выполняет эта программа или Вы не доверяете разработчику этой программы, решите: заблокировать или удалить эту программу.
Low (Низкий**)**	Потенциально нежелательные программы, которые могут собирать информацию о Вас, Вашем компьютере или изменять настройки Вашего компьютера, но об этих действиях сообщается в лицензионном соглашении при их установке.	Такие программы обычно неопасны при выполнении на Вашем компьютере, если только они не были установлены без Вашего ведома. Если вы не уверены, разрешать ли работу такой программы, просмотрите подробности этого предупреждения и определите, доверяете ли Вы разработчику этой программы.
Not yet classified (не классифицируемый**)**	Обычно не опасные программы, если только они не были установлены без Вашего ведома.	Если Вы знаете эту программы и доверяете её разработчику, разрешите её выполнение. Иначе, просмотрите подробности этого предупреждения, для того чтобы принять обоснованное решение. Если Вы вступили в сообщество Microsoft SpyNet, проверьте рейтинг сети голосования, чтобы узнать доверяют ли этой программе другие пользователи.

Для того чтобы просмотреть подробности этого события, подведите курсор к строке с названием обнаруженной программы. Появится всплывающее сообщение с описанием обнаруженной программы и советом от

разработчиков Защитника Windows (рис. 7.39). Если Вы нажмете кнопку «Remove All» (Удалить Всё), то Защитник Windows попытается удалить обнаруженную программу. Об успешности этого действия можно будет судить, просмотрев окно «History» (История). Если Вы нажмете кнопку «Ignore» (Игнорировать), Защитник Windows ничего не будет делать с обнаруженной программой, о чем также появится сообщение в окне «History».

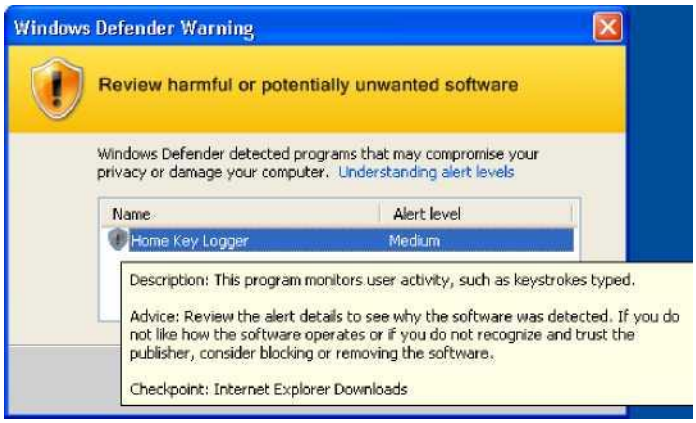


Рис. 7.39 Описание обнаруженной программы Описанный выше пример показывает реакцию Защитника Windows на операцию записи на диск программы установщика. В случае обнаружения реально работающей в данный момент (т.е. уже установленной на Вашем компьютере) программы, окно с предупреждением будет иметь дополнительную кнопку «Review» (см. рис. 7.40). При нажатии на эту кнопку появится главное окно Защитника Windows с возможностью не только удалить обнаруженную программу (кнопка «Remove All»), но и просмотреть подробности обнаруженного события (рис. 7.41). Для этого необходимо
щелкнуть по надписи J Review items detected by real-time protection, g результате, На экране появится окно с подробным описанием события и с возможностью выбора нужного действия (рис. 7.42).

Рис. 7.40 Обнаружение исполняемой программы

Рис. 7.41 Сообщение об обнаруженном событии

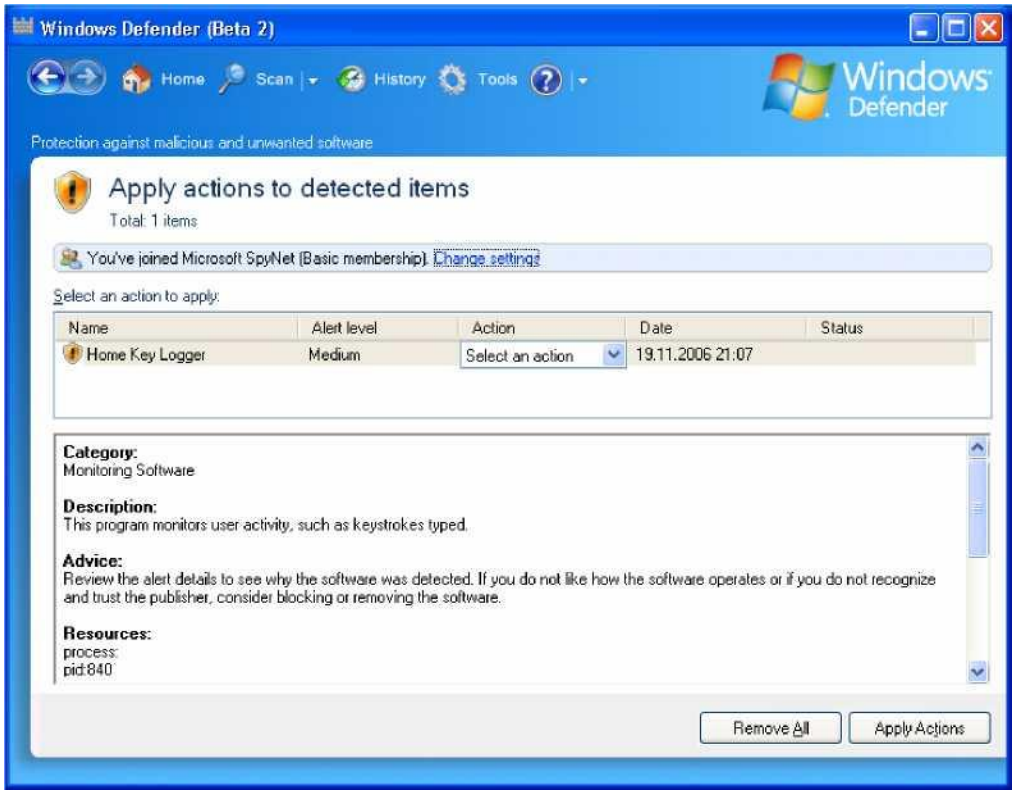


Рис. 7.42. Выберите нужное действие

Возможны следующие действия:

•Ignore (игнорировать подозрительный объект и разрешить ему выполняться).

• Quarantine (переместить подозрительный объект на карантин).

•Remove (удалить подозрительный объект и не допустить его выполнение).

• Always allow (разрешить подозрительному объекту выполняться и занести его в список разрешенных программ(allowed list)).

7.5.3. Работа с карантином

При перемещении подозрительной программы на карантин, Защитник Windows перемещает её в другое место на компьютере и препятствует её работе до тех пор, пока Вы не решите удалить или восстановить её[12].

Для просмотра объектов находящихся на карантине, необходимо на панели инструментов выбрать «Tools» (Сервис) (рис. 7.20) и в появившейся странице (см. рис. 7.21) выбрать пункт «Quarantined items» (рис. 7.43).

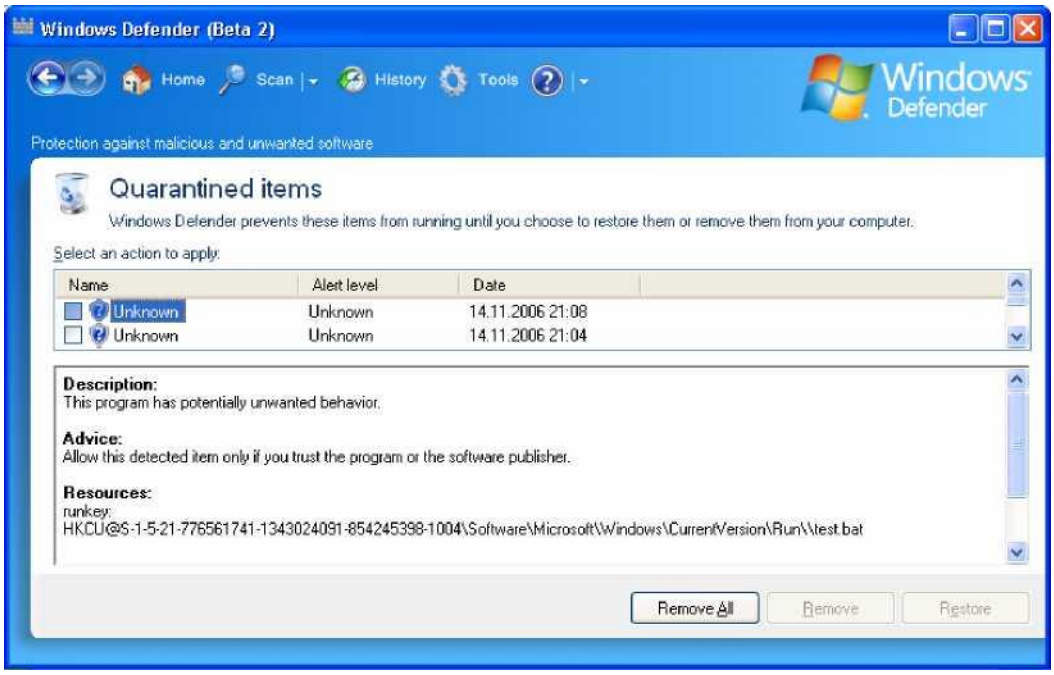


Рис. 7.43. Список объектов на карантине

Для того чтобы удалить все объекты, находящиеся на карантине, необходимо просто нажать внизу кнопку «Remove All». Для того чтобы удалить или восстановить только некоторые объекты, находящиеся на карантине, необходимо выделить их (т.е. отметить их галочками) и нажать одну из кнопок:

• Remove (удаление с компьютера выделенных объектов).

•Restore (восстановление в первоначальное местоположение выделенных объектов).

7.5.4. Работа со списком разрешенных объектов

При выборе действия «Always allow», обнаруженный объект заносится в список разрешенных программ (allowed list). Для просмотра этого списка, необходимо на панели инструментов выбрать «Tools» (Сервис) (рис. 7.20) и в появившейся странице (см. рис. 7.21) выбрать пункт «Allowed items» (рис. 7.44).

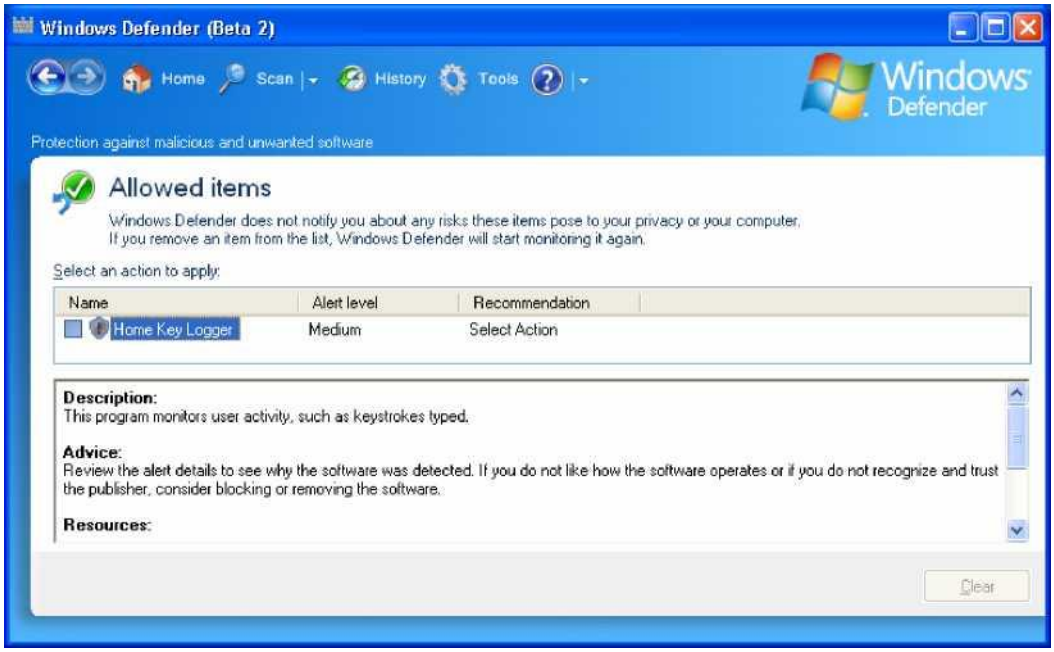


Рис. 7.44 Список разрешенных объектов

Если Вы удалите программу из этого списка, то Защитник Windows снова начнет контролировать действия, выполняемые этой программой. Для удаления программы из списка необходимо выделить её (поставить галочку) и нажать внизу кнопку «Clear».

7.5.5. Использование обозревателя программ (Software Explorer)

На странице «Tools» (см. рис. 7.21) кроме уже рассмотренных средств, присутствует утилита Software Explorer, которая позволяет просматривать подробную информацию о запущенных на компьютере программах. Эта утилита (см. рис. 7.45) помогает контролировать следующие элементы [13]:

Рис. 7.45 Обозреватель программ

• Startup Programs. Программы автозагрузки, т.е. программы, запускаемые одновременно с началом работы системы Windows. Для программ в этой категории доступны следующие действия: «Remove» - удалить, «Disable» - запретить и «Enable» - разрешить.

• Currently Running Programs. Программы, выполняемые в данный момент (отображаются на экране или работают в фоновом режиме). Для некоторых программ в этой категории доступна операция «End Process» - завершить процесс. Кроме того, существует возможность запустить диспетчер задач с помощью кнопки «Task Manager».

• Network Connected Programs. Программы, работающие с сетью. Т.е. программы или процессы, которые могут устанавливать соединение с Интернетом или другой сетью. Для программ в этой категории доступны следующие действия: «End Process» - завершить процесс, «Block Connection» - заблокировать соединение.

• Winsock Service Provider. Поставщики услуг Winsock. Это программы, которые обеспечивают низкоуровневые сетевые службы и службы связи для систем Windows и программ, работающих с Windows[13].

Примечание: Чтобы воспользоваться некоторыми функциями обозревателя программ, нужно обладать правами Администратора.

В зависимости от выбранной категории, по каждой программе в Software Explorer можно просмотреть следующие сведения (см. табл. 7.4).

Таблица 7.4

Сведения, отображаемые в обозревателе программ [13]

| **Параметр** | **Описание** |

Auto Start (Автозагрузка)	Показывает, зарегистрирована ли программа для автоматического запуска при запуске операционной системы.
Startup Type (Тип запуска)	Адрес регистрации программы для автоматического запуска (реестр или папка автозагрузки).
Ship with OS (Поставка вместе с операционной системой)	Показывает, была ли данная программа установлена в ходе установки операционной системы Windows.
Classification (Классификация)	Показывает, представляет ли программа угрозу конфиденциальным сведениям или безопасности компьютера.
Digitally Signed By (Автор цифровой подписи)	Имеет ли программное обеспечение цифровую подпись, если да, то принадлежит ли эта подпись производителю, указанному в списке. Если нет, то не рекомендуется доверять сведениям о производителе, предоставляемым с программным обеспечением, и следует просмотреть дополнительную информацию, прежде чем признать данное программное обеспечение надежным.

7.6. Лабораторная работа. Установка и использование Защитника Windows.

В этой лабораторной работе вы установите Защитника Windows, проверите дату последнего обновления, проведете проверку компьютера и обнаружите подозрительные действия.

7.6.1. Упражнение 1. Подготовительные действия

Вы скопируете потенциально нежелательное программное обеспечение Home Key Logger (клавиатурный шпион) на свой компьютер и создадите командный файл с подозрительными действиями (он регистрирует себя в реестре для автоматического запуска при каждом старте операционной системы).

1. Зарегистрируйтесь в системе как пользователь с правами администратора.
2. Скопируйте на рабочий стол архив с программой Home Key Logger (http://www.spvarsenal.com/cqi-bin/load.pl7familv-kevloqqer--webroot--otherproducts282)
3. С помощью проводника в корневой папке диска C: создайте папку «Test».
4. Выполните «Пуск» - «Выполнить» - «cmd».
5. Для создания командного файла c:\test\risk.bat, в командной строке выполните следующие действия:
```
c:
cd \test
copy con risk.bat
{Ctrl+Z}{Enter}
Exit
```
6. С помощью проводника откройте папку `C:\Test`. На файле `risk.bat` нажмите правую кнопку мыши. В появившемся контекстном меню выберите команду «Изменить».
7. После открытия Блокнота, наберите следующую команду (в одну строку):
```
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"
/v risk.bat /t REG SZ /d "C:\Test\risk.bat"
```

8. Сохраните изменения (команда меню «Файл | Сохранить») и закройте Блокнот.

7.6.2. Упражнение 2. Установка Защитника Windows

Вы выполните установку Защитника Windows на свой компьютер.

1. Зарегистрируйтесь в системе как пользователь с правами администратора и подключитесь к Интернету (если это ещё не сделано).
2. С помощью Internet Explorer откройте «Домашнюю страницу Защитника Windows» (http://www.microsoft.com/rus/athome/security/spyware/software/default.mspx) и щелкните по надписи «Загрузить здесь».
3. При появлении на странице надписи «Validation Required», щелкните кнопку «Continue».
4. При появлении в Internet Explorer панели информации со значком ***Щ*** о необходимости установки элемента управления ActiveX «Windows Genuine Advantage», щелкните левой кнопкой мыши по этой панели и выберите команду «Установить элемент управления ActiveX...».
5. При появлении предупреждения системы безопасности об установке ActiveX компонента, нажмите кнопку «Установить».
6. После успешной проверки лицензии Вашей ОС, выберите язык интерфейса Защитника Windows с помощью параметра «Change Language» и нажмите кнопку «Download» рядом с надписью «Genuine Microsoft Software». Примечание: Дальнейшие шаги предполагают, что Вы выбрали английский язык интерфейса.
7. После появления предупреждения системы безопасности, нажмите кнопку «Сохранить» (рис. 7.8) и выберите место для сохранения файла `WindowsDefender.msi`. Если во время установки Защитника Windows возникнут ошибки, вы всегда сможете запустить установку повторно, если сохраните установщик на диск.
8. Запустите файл `WindowsDefender.msi`. Если после запуска вы увидите окно приветствия Мастера установки, то перейдите к пункту 11. Если вы увидите сообщение об отсутствии Windows Installer 3.1, то перейдите к пункту 9. Если вы увидите сообщение о необходимости обновления службы Windows Update, то перейдите к пункту 10.
9. Установите приложение Windows Installer 3.1. Для этого посетите сайт http://go.microsoft.com/fwlink/?LinkId=63848 описывающий требования к установке Защитника Windows. Как указывается на этой странице, посетите Центр загрузки Microsoft, чтобы установить Windows Installer. Для этого перейдите по ссылке «Microsoft Download Center» и следуйте инструкциям по загрузке и установке Windows Installer. Если необходимо, перезагрузите компьютер и вернитесь к п.8.
10. Обновите на Вашем компьютере службу Windows Update. Для этого воспользуйтесь либо внутренним сервером обновлений в Вашей орга

низации (если он существует), либо в Internet Explorer выполните команду меню «Сервис | Windows Update». Следуйте инструкциям на экране для обновления службы Windows Update. Если необходимо, перезагрузите компьютер и вернитесь к п.8.

11. После появления на экране окна приветствия Мастера установки, нажмите кнопку «Next». Прочтите лицензионное соглашение и если Вы его принимаете, то выберите «I accept the terms in the license agreement» и нажмите кнопку «Next».
12. На следующей странице выберите вариант «Use recommended settings» и нажмите кнопку «Next».
13. На следующей странице выберите вариант полной установки «Complete» и нажмите кнопку «Next».
14. При появлении сообщения о готовности к установке Защитника Windows, нажмите кнопку «Install».
15. После успешной установки, отключите параметр «Check for updated definitions and run a quick scan now» и нажмите кнопку «Finish».

7.6.3. Упражнение 3. Обновление определений Защитника Windows

Вы выполните обновление определений Защитника Windows.

1. Зарегистрируйтесь в системе как пользователь с правами администратора и подключитесь к Интернету (если это ещё не сделано).
2. Запустите Защитник Windows (Пуск - Все программы - Windows Defender).
3. В разделе «Status» проверьте версию установленных обновлений и дату их создания (Параметр «Definition version:»).
4. Щелкните по треугольнику **(В)** рядом со знаком помощи (^Ep). В появившемся списке выберите команду «About Windows Defender». В появившемся окне нажмите кнопку «Check for Updates».
5. Дождитесь появления сообщения «Windows Defender is up-to-date with definitions and engine upgrades».
6. На главной странице (возникает по нажатию кнопки «Home») проверьте версию установленных обновлений и дату их создания.

7.6.4. Упражнение 4. Быстрое сканирование компьютера

Вы выполните быструю проверку Вашего компьютера с помощью Защитника Windows и удалите обнаруженное нежелательное ПО.

1. Зарегистрируйтесь в системе как пользователь с правами администратора.
2. Запустите Защитник Windows (Пуск - Все программы - Windows Defender).
3. Щелкните по треугольнику (Э) рядом с надписью «Scan». В появившемся списке выберите команду «Quick Scan».

4. После окончания сканирования, при появлении раздела «Review potentially unwanted items», щелкните ПО надписи В Review items detected ***by*** scanning..
5. На странице «Scan Results» просмотрите все обнаруженные объекты и для каждого выберите желаемое действие.
6. Посмотрите расположение обнаруженного объекта «Home Key Logger» (раздел «Resources:»). Для этого объекта выберите действие «Remove» и нажмите внизу кнопку «Apply Actions».
7. После появления в столбце «Status» сообщения «Succeeded», проверьте, что объект действительно удален с диска.

7.6.5. Упражнение 5. Обнаружение подозрительных действий

Вы включите получение уведомлений обо всех подозрительных событиях и посмотрите реагирование Защитника Windows на некоторые из них.

1. Зарегистрируйтесь в системе как пользователь с правами администратора.
2. Для того чтобы получать уведомления обо всех подозрительных действиях, совершаемых на Вашем компьютере, необходимо в разделе «Choose if Windows Defender should notify you about:» включить параметр «Software that has not yet been classified for risks». Для этого на странице «Tools» выберите раздел «Options» и там включите указанный выше параметр.
3. Запустите редактор реестра для контроля происходящих действий. Для этого выполните «Пуск» - «Выполнить» - «regedit». Откройте ключ «Мой компьютер\HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVersion\Run».
4. С помощью Проводника запустите на выполнение командный файл «C:\Test\risk.bat».
5. При появлении в области уведомлений (правый нижний угол экрана) сообщения «Windows Defender detected changes», щелкните по нему левой кнопкой мыши.
6. В открывшемся окне Защитника Windows, просмотрите описание обнаруженного события.
7. С помощью редактора реестра, проверьте появление значения «risk.bat».
8. В столбце «Action», выберите действие «Block» и нажмите кнопку «Apply Actions».
9. После отображения статуса «Succeeded», проверьте в редакторе реестра, что значение «risk.bat» действительно удалено (если необходимо, выполните команду «Вид | Обновить» в редакторе реестра).
10. Закройте все открытые окна.

7.7. Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал.

1. Дайте определение термину «шпионская» программа.

2. Перечислите действия, которые могут выполнять программы-шпионы.

3. Перечислите вероятные признаки наличия на компьютере «шпионского» либо нежелательного ПО.

4. Перечислите технологий Microsoft обеспечивающие защиту компьютеров от программ-шпионов и других нежелательных программ.

5. Перечислите технологий Microsoft обеспечивающие защиту компьютеров от вирусов и вредоносного ПО.

6. Что такое сообщество Microsoft SpyNet?

7. Какие функции выполняет обозреватель программ (Software Explorer) входящий в состав Защитника Windows?

7.8. Резюме

«Шпионские» программы — одна из самых неприятных проблем, с которыми сейчас сталкиваются пользователи компьютеров. Во всем мире программы-шпионы считаются серьезной проблемой, которая угрожает подорвать доверие общества к компьютерным технологиям [14].

Одним из решений, предлагаемых компанией Microsoft для защиты компьютера от программ-шпионов и других нежелательных программ, является Защитник Windows (Windows Defender). Этот продукт интегрирован в Windows Vista, а для пользователей Windows XP доступен в виде отдельного бесплатного дополнения [2].

Защитник Windows (бета-версия 2) помогает пользователям обнаружить, а затем отключить или удалить с компьютера известные программы-шпионы и другие, потенциально нежелательные программы [14].

В тоже время, Windows Defender не является антивирусной программой и обеспечивает защиту только от одного из подмножеств существующих вредоносных программ. Он не защищает компьютер от вирусов, троянских программ, червей и т.д. Для защиты от этих угроз пользователь может выбрать решение как от самой Microsoft (например, Microsoft One- Care), так и от стороннего производителя [15].

7.9. Литература

1. Сравнение Защитника Windows (бета-версия 2) с другими антишпионскими программами корпорации Майкрософт и технологиями защиты от вирусов.- Microsoft, 13 февраля 2006 г. (http://www.microsoft.com/rus/athome/security/spyware/software/about/productcomparisons.mspx)

2. *ЕлмановаН.* Инструменты Microsoft для защиты от вредоносного ПО: ближайшее будущее // КомпьютерПресс.- 2006 .- №5.- С. 162-164.

3. Домашняя страница защитника Windows.- Microsoft, 2006 (http://www.microsoft.com/rus/athome/security/spyware/software/default.mspx)

4. Что делать для защиты от «шпионских» и иных нежелательных программ.- Microsoft, 5 января 2005 г. (http://www.microsoft.com/rus/athome/security/spyware/spywarewhat.mspx)

5. Стратегия корпорации Майкрософт по защите от программ-шпионов.- Microsoft, 13 февраля 2006 г. (http://www.microsoft.com/rus/athome/security/spyware/software/msft/strategy.mspx)

6. Защитник Windows (бета-версия 2) Требования к системе.- Microsoft, 13 февраля 2006 г. (http://www.microsoft.com/rus/athome/security/spyware/software/about/sysreq.mspx)

7. Download details: Windows Defender (Beta 2).- Microsoft, 12 апреля 2006. (http://www.microsoft.com/downloads/details.aspx?FamilyId=435BFCE7-DA2B-4A6A-AFA4-F7F14E605A0D&displaylang=en)

8. Windows Defender (Beta 2): System requirements.- Microsoft, 29 August 2006. (http://www.microsoft.com/athome/security/spyware/software/about/sysreq.mspx)

9. Установка и настройка Защитника Windows (бета-версия 2) .- Microsoft, 13 февраля 2006. (http://www.microsoft.com/rus/athome/security/spyware/software/support/howto/download.mspx)

10. Часто задаваемые вопросы о Защитнике Windows (бета-версия 2).- Microsoft, 13 февраля 2006. (http://www.microsoft.com/rus/athome/security/spyware/software/about/faq.mspx)

11. Проверка компьютера на наличие программ-шпионов с помощью Защитника Windows (бета-версия 2).- Microsoft, 13 февраля 2006. (http://www.microsoft.com/rus/athome/security/spyware/software/support/howto/scan.mspx)

12. Как удалять или восстанавливать элементы на карантине с помощью Защитника Windows (бета-версия 2).- Microsoft, 13 февраля 2006. (http://www.microsoft.com/rus/athome/security/spyware/software/support/howto/quarantined.mspx)

13. Использование обозревателя программ Защитника Windows (бета-версия 2).- Microsoft, 13 февраля 2006. (http://www.microsoft.com/rus/athome/security/spyware/software/support/howto/softwareexplorer.mspx)

14. Стратегия корпорации Майкрософт по защите от программ-шпионов.- Microsoft, 13 февраля 2006. (http://www.microsoft.com/rus/athome/security/spyware/software/msft/strategy.mspx)

15. *КасперскаяН.* Безопасность от Microsoft: шаг к обновленному миру?- Лаборатория Касперского, 2006. (http://www.kaspersky.ru/reading_room?chapter=207367336)