Dr.WEB®

Агент для Windows

Защити созданное

Руководство пользователя

Dr.Web Агент для Windows
Версия 6.0.4
Руководство пользователя
26.08.2013

«Доктор Веб», Центральный офис в России
125124
Россия, Москва
3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: www.drweb.com
Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах вы можете найти на официальном сайте компании.

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

«Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Глава 1. Введение

1.1. Условные обозначения и сокращения

Условные обозначения

В данном Руководстве используются обозначения, приведенные в таблице 1.

Таблица 1. Условные обозначения

Обозначение	Комментарий
 Заметьте, что	Важное замечание или указание.
 Внимание	Предупреждение о возможных ошибочных ситуациях, а так же важных моментах, на которые следует обратить особое внимание.
Dr.Web Агент	Названия продуктов и компонентов **Dr.Web**.
Антивирусная сеть	Термин в позиции определения.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Применить	Названия кнопок, окон, пунктов меню и других элементов пользовательского интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`C:\Windows\`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте Руководства будут употребляться без расшифровки следующие сокращения:

- FDD – Floppy Disk Drive (гибкий магнитный диск – портативный магнитный носитель информации),
- GUI – Graphical User Interface (графический пользовательский интерфейс), GUI-версия программы – версия, использующая средства GUI,
- UAC – User Account Control (контроль учетных записей пользователей – компонент Microsoft Windows. Запрашивает подтверждение действий, требующих прав администратора, в целях защиты от несанкционированного использования компьютера),
- URL – Uniform Resource Locator (единый указатель ресурсов – стандартизированный способ записи адреса ресурса в сети Интернет),
- **ВСО Dr.Web – Всемирная Система Обновлений Dr.Web,**
- ОС – операционная система,
- ПО – программное обеспечение.

1.2. Антивирус Dr.Web® Enterprise Security Suite

Dr.Web Enterprise Security Suite предназначен для организации и управления единой и надежной комплексной антивирусной защитой компьютеров вашей организации.

Защищенные компьютеры объединяются в антивирусную сеть, которой управляет администратор через **Enterprise Сервер**. Защита компьютеров сотрудников автоматизирована и управляется централизованно, что обеспечивает надежный уровень безопасности при минимальном вмешательстве персонала.

Dr.Web Enterprise Security Suite решает следующие задачи:

- централизованная (без необходимости непосредственного доступа персонала) установка антивирусных пакетов на защищаемые компьютеры,
- централизованная настройка параметров антивирусных пакетов на защищаемых компьютерах,
- централизованное обновление вирусных баз и программного обеспечения на защищаемых компьютерах,
- мониторинг вирусных событий, а также состояния антивирусных пакетов и ОС на всех защищаемых компьютерах.

На защищаемые компьютеры устанавливается **Dr.Web Агент**. Данный компонент обеспечивает управление защитой компьютера и поддерживает связь с **Enterprise Сервером**, через который производятся обновления антивирусных программ и их компонентов, а также настройка основных параметров работы антивирусного ПО, установленного на компьютерах.

На компьютерах с установленным **Dr.Web Агентом** не должны быть установлены другие антивирусные программы, в том числе другие программы компании **Dr.Web**.

Настройки, доступные пользователю, описываются в разделе Управление Dr.Web Агентом.

Глава 2. Компонент Dr.Web Агент

2.1. Основные функции и параметры Dr.Web Агента

Защита компьютеров от вирусных угроз и спама производится посредством программ, входящих в состав антивирусного пакета **Dr.Web Enterprise Security Suite**.

Управление защитой компьютера и поддержка связи с **Enterprise Сервером** осуществляется посредством **Агента Dr.Web Enterprise Security Suite** (далее - **Dr.Web Агент**).

Dr.Web Агент выполняет следующие функции:

- производит установку, обновление и настройку антивирусного пакета **Dr.Web**, запуск сканирования, а также выполнение других заданий, сформированных **Enterprise Сервером**;
- позволяет вызывать компоненты антивирусного пакета **Dr.Web** через специальный интерфейс;
- передает результаты выполнения заданий **Enterprise Серверу;**
- передает **Enterprise Серверу** сообщения о возникновении заранее оговоренных событий в работе антивирусного пакета.

Пользователь может осуществлять следующие действия при помощи Dr.Web Агента:

- настраивать расписание проверки (сканирования) компьютера на вирусы;
- запускать при необходимости сканирование компьютера;
- изменять настройки отдельных компонентов **Антивируса Dr.Web**, в том числе, некоторые настройки самого **Агента**;

- просматривать статистику вирусных событий на компьютере и другую информацию об **Антивирусе Dr.Web**.

Изменение настроек **Агента** и компонентов комплекса возможно только при наличии у пользователя соответствующих прав. Более подробная информация приводится в описаниях настроек конкретных компонентов.

2.2. Системные требования

На рабочих станциях антивирусной сети, управляемой с помощью **Dr.Web**, не должно использоваться другое антивирусное ПО (в том числе ПО других версий антивирусных программ **Dr.Web**).

Для работы Dr.Web Агента и полного антивирусного пакета требуется:

1. Минимальные требования:
   - процессор Intel Pentium IV с частотой 1.6 ГГц;
   - объем оперативной памяти 512 МБ.
2. Рекомендуемые требования:
   - процессор Intel Pentium IV с частотой 2.4 ГГц и выше;
   - объем оперативной памяти не менее 1 ГБ.
3. Свободное место на жестком диске: не менее 250 МБ для исполняемых файлов + дополнительно для протоколов работы и временных файлов;
4. Операционные системы (см. Приложение В. Полный список поддерживаемых версий ОС):
   a) ОС Microsoft® Windows® 98, ОС Windows Me, ОС Windows NT4 (SP6a) и выше. При этом, в зависимости от ОС, могут быть установлены следующие компоненты:

Компонент	ОС
SpIDer Gate, **SelfPROtect**, **Офисный Контроль**, **Dr.Web Browser-Plugin для Outlook**	Windows 2000 с SP4 и выше.
SpIDer Guard NT4, **Dr.Web Сканер NT4**	• Windows 98, • Windows ME, • Windows NT4 (SP6a), • Windows 2000 с SP4 без Update Rollup1, • Windows XP без SP, а также с SP1, • Windows 2003 без SP.
FireWall, **SpIDer Guard G3**, **Dr.Web Сканер**	• Windows 2000 с SP4 и Update Rollup1, • Windows XP с SP2 и выше, • Windows 2003 с SP1 и выше, • Windows Vista и выше.
SpIDer Mail NT4	• Windows 98, • Windows NT4 с SP6a.
SpIDer Mail	Все поддерживаемые ОС, старше систем для версии **SpIDer Mail NT4**.

b) ОС Microsoft® Windows Mobile®;

c) ОС Novell® NetWare®;

d) ОС семейства UNIX®: ОС Linux®, ОС FreeBSD® или ОС Solaris™;

e) ОС Android;

f) Mac OS X.

5. Для подключаемого модуля **Dr.Web для Outlook** необходим установленный клиент Microsoft Outlook из состава MS Office:

- Outlook 2000 (Outlook 9),
- Outlook 2002 (Outlook 10 или Outlook XP),
- Office Outlook 2003 (Outlook 11),
- Office Outlook 2007,
- Office Outlook 2010.

6. Для корректной работы контекстной справки **Dr.Web Агент для Windows** необходим Windows® Internet Explorer® 6.0 и выше.

Описание функциональности **Агента** под ОС Windows Mobile и Novell NetWare приведено в руководствах пользователя **Dr.Web Агент для Windows Mobile** и **Dr.Web Агент для Novell NetWare**.

2.3. Установка и удаление антивирусного ПО

2.3.1. Установка Dr.Web Агента

Перед началом установки антивирусного ПО обратите внимание на раздел Системные требования.

Установка **Dr.Web Агента** должна выполняться пользователем с правами администратора данного компьютера.

Установка и удаление **Dr.Web Агента** и антивирусного пакета могут быть осуществлены двумя способами:

1. Удаленно - на **Сервере** через сеть. Производится администратором антивирусной сети. Вмешательство пользователя не требуется (подробное описание процесса *создания* антивирусной станции и удаленной установки антивирусного ПО приведено в руководстве администратора

Антивирус Dr.Web Enterprise Security Suite).

Удаленная установка **Dr.Web Агентов** возможна только на рабочие станции, работающие под управлением ОС Windows NT4 и старше.

2. Локально - на машине пользователя непосредственно. Может производится как администратором, так и пользователем. При этом для установки может использоваться:
   - Инсталляционный пакет `esinst.exe`.
   - Сетевой инсталлятор **Агента** `drwinst.exe`.

   Описание локальной установки и удаления антивирусного ПО приведено ниже.

2.3.1.1. Установка Dr.Web Агента при помощи Инсталляционного пакета

Если на рабочей станции уже установлено антивирусное ПО, то перед началом установки инсталлятор предпримет попытку его удалить. Если попытка окажется неудачной, вам будет необходимо самостоятельно удалить используемое на рабочей станции антивирусное ПО.

Для установки Агента и антивирусного пакета на рабочей станции:

1. Скачайте установочный файл **Агента**. Для этого перейдите по ссылке, полученной от администратора антивирусной сети.
2. Запустите скачанный файл `esinst.exe`. Откроется окно мастера установки **Антивируса Dr.Web**.
3. Перед началом инсталляции мастер установки попросит подтвердить, что у вас не установлены антивирусные программы. Убедитесь, что на вашем компьютере не используется другое антивирусное ПО (в том числе ПО других версий антивирусных программ **Dr.Web**), после

чего установите флаг **У меня на компьютере нет других антивирусов**. Нажмите на кнопку **Далее**.

4. В следующем окне будет предложен выбор варианта установки:
   - **Быстрая (рекомендуется)** - наиболее простой вариант установки. Все параметры задаются автоматически. Далее перейдите к шагу **9**.
   - **Выборочная** - вариант установки, при котором вы можете выбрать компоненты антивирусного ПО, устанавливаемого на компьютер.
   - **Административная** - наиболее полный вариант установки. Позволяет задать/изменить все параметры инсталляции и устанавливаемого антивирусного ПО.
5. Для вариантов установки **Выборочная** и **Административная**: в следующем окне вам будет предоставлен выбор компонентов антивирусного пакета **Dr.Web**. Установите флаги напротив тех компонентов, которые вы хотите установить на ваш компьютер.

   В разделе **Путь каталога установки** вы можете задать каталог, в который будет установлено антивирусное ПО. По умолчанию - это каталог `Dr.Web Enterprise Suite`, расположенный в каталоге `Program files` на системном диске. Для изменения пути установки нажмите на кнопку **Обзор** и укажите требуемый путь.

   Нажмите на кнопку **Далее**.

   Далее для варианта установки **Выборочная** перейдите к шагу **9**.

6. Для варианта установки **Административная**: в следующем окне задайте настройки **Сетевого инсталлятора**:
   - В поле **Dr.Web Enterprise Server** задается сетевой адрес **Enterprise Сервера**, с которого будет производиться установка **Агента** и антивирусного пакета. Если при запуске инсталлятора вы задали адрес **Сервера**, то он будет автоматически занесен в данное поле.

При установке **Dr.Web Агента** при помощи инсталлятора, созданного в **Центре управления Dr.Web**, автоматически заполняется поле **Dr.Web Enterprise Server**.

Если вы заведомо не знаете адрес **Сервера**, нажмите на кнопку **Поиск**. Будет выведено окно для поиска активных **Enterprise Серверов** сети. Задайте необходимые параметры (в формате *<имя_сервера>*@*<IP-адрес>*/*<префикс_сети>*:*<порт>*) и нажмите кнопку **Поиск**. В списке найденных **Серверов** выберите тот, с которого будет устанавливаться антивирусное ПО, и нажмите на кнопку **ОК**.

- В поле **Dr.Web Enterprise Server публичный ключ** задается полный путь к публичному ключу (`drwcsd.pub`), расположенному на вашем компьютере (при запуске инсталлятора с **Сервера** по сети, ключ копируется во временные файлы ОС, а после инсталляции перемещается в каталог установки).
- В разделе **Использовать сжатие при закачке** выберите нужный для вас вариант компрессии трафика: **Да** - использовать сжатие, **Нет** - не использовать, **Возможно (по умолчанию)** - использование сжатия трафика зависит от настроек на **Сервере**.
- Флаг **Добавить Dr.Web Агент в список исключений Windows Firewall** предписывает добавление портов и интерфейсов, используемых **Агентом**, в список исключений сетевого экрана операционной системы (кроме ОС Windows 2000 и младше). Рекомендуется установить данный флаг. Это поможет избежать ошибок, например, при автоматическом обновлении компонентов антивируса и вирусных баз.
- При необходимости установите флаг **Зарегистрировать агент в списке установленных программ**.

Данная опция позволяет, в том числе, осуществлять удаление **Агента** и антивирусного пакета штатными средствами ОС Windows (см. п. Удаление Dr.Web Агента).

7. Для варианта установки **Административная**: в следующем окне задайте настройки **Агента**:
   - В разделе **Авторизация** задаются параметры авторизации **Агента** на **Сервере**. При выборе варианта **Автоматически (по умолчанию)** режим доступа станции будет определяться на **Сервере**. При выборе варианта **Ручная** необходимо задать параметры авторизации станции: ее **Идентификатор** на **Сервере** и **Пароль** доступа к нему. При этом станция получит доступ без ручного подтверждения администратором на **Сервере**.

При установке **Dr.Web Агента** при помощи инсталлятора, созданного в **Центре управления Dr.Web**, автоматически заполняются поля **Идентификатор** и **Пароль** для варианта авторизации **Ручная**.

   - В разделах **Сжатие** и **Шифрование** задаются соответствующие режимы для трафика между **Сервером** и **Агентом** (подробнее см. п. **Использование шифрования и сжатия трафика** в руководстве администратора **Антивирус Dr.Web Enterprise Security Suite**).

   Нажмите **Далее**.

8. Начнется установка **Агента** и антивирусных компонентов (не требует вмешательства пользователя).
9. После завершения инсталляции мастер установки сообщит о необходимости перезагрузить компьютер. Нажмите кнопку **Готово** для завершения работы мастера установки.
10. Перезагрузите компьютер.

При установке антивирусного пакета, в состав которого входит компонент **Dr.Web Firewall**, для завершения установки потребуются две перезагрузки станции.

При этом, под ОС Windows Vista и Windows Server 2008 после второй перезагрузки не будет запущена служба **Планировщика заданий** ОС Windows, заблокированная компонентом **Dr.Web Firewall**. Функциональность восстанавливается после автоматического создания предустановленного правила компонентом **Dr.Web Firewall**, разрешающего запуск службы **Планировщика**, и последующего перезапуска **Планировщика**, в частности после перезагрузки станции.

2.3.1.2. Установка Dr.Web Агента при помощи Сетевого инсталлятора

Если сетевой инсталлятор запущен в режиме нормальной инсталляции (т.е. без ключа `-uninstall`) на станции, на которой уже была проведена установка **Агента**, это не приведет к выполнению каких-либо действий. Инсталлятор завершит работу и отобразит окно со списком допустимых ключей.

Перед началом новой инсталляции необходимо удалить установленный **Агент**.

Установка при помощи Сетевого инсталлятора возможна в двух основных режимах:

1. В фоновом режиме.
2. В графическом режиме.

Установка Dr.Web Агента в фоновом режиме инсталлятора

Чтобы установить Dr.Web Агента на рабочую станцию в фоновом режиме инсталлятора:

1. С компьютера, на который будет устанавливаться антивирусное ПО, запустите программу `drwinst.exe`, которую можно найти по одному из следующих путей:
   - В сетевом каталоге установки **Агента**. При установке **Сервера** это подкаталог `Installer` (по умолчанию скрытый разделяемый ресурс) каталога установки **Сервера**, в дальнейшем его можно переместить.
   - На инсталляционной странице **Центра Управления Dr.Web**, которая доступна на любом компьютере, имеющем сетевой доступ к **Enterprise Серверу**, по адресу:
     `http://`*<Адрес_Сервера>*`:`*<номер_порта>*`/install/`
     где в качестве *<Адрес_Сервера>* укажите IP-адрес или DNS-имя компьютера, на котором установлен **Enterprise Сервер**. В качестве *<номер_порта>* укажите порт номер `9080` (или `9081` для https).

   По умолчанию программа `drwinst`, запущенная без параметров, использует режим **Multicast** для сканирования сети на наличие активных **Enterprise Серверов**.

При использовании режима **Multicast** для поиска активных **Серверов**, установка **Агента** будет производиться с первого найденного **Сервера**. При этом, если имеющийся `pub`-ключ не соответствует ключу **Сервера**, установка завершится с ошибкой. В этом случае явно укажите адрес **Сервера** при запуске инсталлятора (см. ниже).

Также команду `drwinst` можно запускать с дополнительными параметрами:

- В случае, когда режим **Multicast** не используется, при установке **Агента** рекомендуется использовать имя **Сервера** (предварительно зарегистрированное в службе DNS):

  `drwinst` *<DNS_имя_Сервера>*

  Это упростит процесс настройки антивирусной сети, связанный с процедурой переустановки **Enterprise Сервера** на другой компьютер.

- Вы также можете использовать явное указание адреса **Сервера**, например:

  `drwinst 192.168.1.3`

- Использование ключа `-regagent` позволяет при установке зарегистрировать **Агент** в списке установки и удаления программ.

- Для запуска инсталлятора в графическом режиме, используйте параметр `-interactive`.

Полный список параметров **Сетевого инсталлятора** приведен в Приложении **Н4. Сетевой инсталлятор** в руководстве администратора **Антивирус Dr.Web Enterprise Security Suite**.

2. После завершения работы инсталлятора, на компьютер будет установлено ПО **Агента** (но не антивирусный пакет).
3. После подтверждения станции на **Сервере** (если этого требуют настройки **Сервера**) антивирусный пакет будет автоматически установлен.
4. Перезагрузите компьютер по требованию **Агента**.

При установке антивирусного пакета, в состав которого входит компонент **Dr.Web Firewall**, для завершения установки потребуются две перезагрузки станции.

При этом, под ОС Windows Vista и Windows Server 2008 после второй перезагрузки не будет запущена служба **Планировщика заданий** ОС Windows, заблокированная компонентом **Dr.Web Firewall**. Функциональность восстанавливается после автоматического создания предустановленного правила

компонентом **Dr.Web Firewall**, разрешающего запуск службы **Планировщика**, и последующего перезапуска **Планировщика**, в частности после перезагрузки станции.

Установка Dr.Web Агента в графическом режиме инсталлятора

Чтобы установить Dr.Web Агента на рабочую станцию в графическом режиме инсталлятора:

1. С компьютера, на который будет устанавливаться антивирусное ПО, запустите программу `drwinst.exe` с параметром `–interactive`. Программу `drwinst.exe` можно найти по одному из следующих путей:
   - В сетевом каталоге установки **Агента**. При установке **Сервера** это подкаталог `Installer` (по умолчанию скрытый разделяемый ресурс) каталога установки **Сервера**, в дальнейшем его можно переместить.
   - На инсталляционной странице **Центра Управления Dr.Web**, которая доступна на любом компьютере, имеющем сетевой доступ к **Enterprise Серверу**, по адресу:
     `http://`*<Адрес_Сервера>*`:`*<номер_порта>*`/install/`
     где в качестве *<Адрес_Сервера>* укажите IP-адрес или DNS-имя компьютера, на котором установлен **Enterprise Сервер**. В качестве *<номер_порта>* укажите порт номер `9080` (или `9081` для https).

   Откроется окно мастера установки антивируса **Dr.Web**.
2. Перед началом инсталляции мастер установки попросит подтвердить, что на компьютере не установлены антивирусные программы. Убедитесь, что на компьютере не используется другое антивирусное ПО (в том числе ПО других версий антивирусных программ **Dr.Web**), после чего установите флаг **У меня на компьютере нет других антивирусов**. Нажмите на кнопку **Далее**.
3. В следующем окне будет предложен выбор варианта установки:

- **Быстрая (рекомендуется)** - наиболее простой вариант установки. Все параметры задаются автоматически. Далее перейдите к шагу **7**.
- **Выборочная** - вариант установки, при котором пользователь может выбрать компоненты антивирусного ПО, устанавливаемого на компьютер.
- **Административная** - наиболее полный вариант установки. Позволяет задать/изменить все параметры инсталляции и устанавливаемого антивирусного ПО.

4. Для вариантов установки **Выборочная** и **Административная**: в следующем окне вам будет предоставлен выбор компонентов антивирусного пакета **Dr.Web**. Установите флаги напротив тех компонентов, которые вы хотите установить на ваш компьютер.

   В разделе **Путь каталога установки** вы можете задать каталог, в который будет установлено антивирусное ПО. По умолчанию - это каталог `Dr.Web Enterprise Suite`, расположенный в каталоге `Program files` на системном диске. Для задания/изменения пути по умолчанию, нажмите на кнопку **Обзор** и укажите требуемый путь.

   Нажмите на кнопку **Далее**.

   Далее для варианта установки **Выборочная** перейдите к шагу **7**.

5. Для варианта установки **Административная**: в следующем окне задайте настройки **Сетевого инсталлятора**:

   - В поле **Dr.Web Enterprise Server** задается сетевой адрес **Enterprise Сервера**, с которого будет производиться установка **Агента** и антивирусного пакета. Если при запуске инсталлятора вы задали адрес **Сервера**, то он будет автоматически занесен в данное поле. Если вы заведомо не знаете адрес **Сервера**, нажмите на кнопку **Поиск**. Будет выведено окно для поиска активных **Enterprise Серверов** сети. Задайте необходимые параметры (в формате *<имя_сервера>*@*<IP-адрес>*/*<префикс_сети>*:*<порт>*) и

нажмите кнопку **Поиск**. В списке найденных **Серверов** выберите тот, с которого будет устанавливаться антивирусное ПО, и нажмите на кнопку **ОК**.

- В поле **Dr.Web Enterprise Server публичный ключ** задается полный путь к открытому ключу шифрования (`drwcsd.pub`), расположенному на компьютере пользователя (при запуске инсталлятора с **Сервера** по сети, ключ копируется во временные файлы ОС, а после перемещается в каталог установки).
- В разделе **Использовать сжатие при закачке** выберите нужный для вас вариант компрессии трафика: **Да** - использовать сжатие, **Нет** - не использовать, **Возможно (по умолчанию)** - использование сжатия трафика зависит от настроек на **Сервере**.
- Флаг **Добавить Dr.Web Агент в список исключений Windows Firewall** предписывает добавление портов и интерфейсов, используемых **Агентом**, в список исключений сетевого экрана операционной системы. Рекомендуется установить данный флаг. Это поможет избежать ошибок, например, при автоматическом обновлении компонентов антивируса и вирусных баз.
- При необходимости установите флаг **Зарегистрировать агент в списке установленных программ**.

Данная опция позволяет, в том числе, осуществлять удаление **Агента** и антивирусного пакета штатными средствами ОС Windows (см. п. Удаление Dr.Web Агента).

6. Для варианта установки **Административная**: в следующем окне задайте настройки **Агента**:
   - В разделе **Авторизация** задаются параметры авторизации **Агента** на **Сервере**. При выборе варианта **Автоматически (по умолчанию)** параметры авторизации (идентификатор и пароль) будут автоматически сгенерированы на **Сервере**, при этом режим доступа станции будет определяться на **Сервере**. При выборе варианта **Ручная** необходимо

задать параметры авторизации станции: ее **Идентификатор** на **Сервере** и **Пароль** доступа к нему. При этом станция получит доступ без ручного подтверждения администратором на **Сервере**.

- В разделах **Сжатие** и **Шифрование** задаются соответствующие режимы для трафика между **Сервером** и **Агентом** (подробнее см. п. **Использование шифрования и сжатия трафика** в руководстве администратора **Антивирус Dr.Web Enterprise Security Suite**).

Нажмите **Далее**.

7. Начнется установка **Dr.Web Агента**. После установки **Агента** нажмите кнопку **Готово** для завершения работы мастера установки.
8. После подтверждения станции на **Сервере** (если этого требуют настройки **Сервера** и если на шаге **6** при **Административной** установке не был выбран вариант авторизации **Ручная**), антивирусный пакет будет автоматически установлен.
9. Перезагрузите компьютер по требованию **Агента**.

При установке антивирусного пакета, в состав которого входит компонент **Dr.Web Firewall**, для завершения установки потребуются две перезагрузки станции.

При этом, под ОС Windows Vista и Windows Server 2008 после второй перезагрузки не будет запущена служба **Планировщика заданий** ОС Windows, заблокированная компонентом **Dr.Web Firewall**. Функциональность восстанавливается после автоматического создания предустановленного правила компонентом **Dr.Web Firewall**, разрешающего запуск службы **Планировщика**, и последующего перезапуска **Планировщика**, в частности после перезагрузки станции.

2.3.2. Удаление Dr.Web Агента

Для возможности локального удаления **Агента** и антивирусного пакета, данная опция должна быть разрешена администратором на **Сервере**.

После удаления антивирусного ПО ваш компьютер не будет защищен от вирусов и других вредоносных программ.

Удаление антивирусного ПО станции (**Dr.Web Агента** и антивирусного пакета) можно осуществить двумя способами:

1. Используя штатные средства ОС Windows.
2. При помощи инсталлятора Агента.

Удаление штатными средствами ОС Windows

Данный метод удаления доступен только в том случае, если при установке **Агента** с помощью графического инсталлятора был установлен флаг **Зарегистрировать агент в списке установленных программ**.

Если **Агент** был установлен в фоновом режиме инсталлятора, то удаление антивирусного ПО штатными средствами будет доступно только если при инсталляции был использован ключ `-regagent`.

Для удаления антивирусного ПО выберите:

- Для ОС Windows 98, Windows NT4, Windows ME, Windows 2000: **Пуск** → **Настройка** → **Панель управления** → **Установка и удаление программ**.
- Для ОС Windows XP, Windows 2003 (в зависимости от вида меню **Пуск**):
  - Меню "Пуск": **Пуск** → **Панель управления** →

Установка и удаление программ.

- Классическое меню "Пуск": **Пуск** → **Настройка** → **Панель управления** → **Установка и удаление программ**.

◆ Для ОС Windows Vista и Windows 7 (в зависимости от вида меню **Пуск**):

- Меню "Пуск": **Пуск** → **Панель управления** → **Программы и компоненты**, далее в зависимости от вида Панели управления:
  - Классический вид: **Программы и компоненты**.
  - Домашняя страница: **Программы** → **Программы и компоненты**.
- Классическое меню "Пуск": **Пуск** → **Настройка** → **Панель управления** → **Программы и компоненты**.

◆ Для ОС Windows 8:

- Откройте **Панель управления** любым удобным способом, например, через пункт **Панель управления** в контекстном меню, вызываемом правым щелчком мыши по левому нижнему углу экрана или через **Charms bar** → **Параметры** → **Панель управления**. Далее в зависимости от типа настройки **Просмотр** для Панели управления:
  - Мелкие/крупные значки: **Программы и компоненты**.
  - Категория: **Программы** → **Удаление программ**.

В открывшемся списке выберите строку **Dr.Web Agent** и нажмите на кнопку **Удалить** (или **Заменить/Удалить** для более ранних версий ОС Windows). Антивирусное ПО станции будет удалено.

Удаление при помощи инсталлятора

Удаление при помощи сетевого инсталлятора

Для того чтобы удалить ПО **Dr.Web Агента** и антивирусный пакет на рабочей станции при помощи сетевого инсталлятора **Агента**, необходимо выполнить в каталоге установки **Агента** (по умолчанию – `C:\Program Files\DrWeb Enterprise Suite`) команду `drwinst` с параметром `-uninstall` (или с параметрами `-uninstall -interactive`, если требуется обеспечить контроль за ходом удаления).

Удаление при помощи инсталляционного пакета

Для того чтобы удалить ПО **Dr.Web Агента** и антивирусный пакет при помощи инсталляционного пакета, запустите установочный файл `esinst.exe` той версии продукта, которая у вас установлена. Откроется окно мастера удаления **Антивируса Dr.Web**. Для начала процесса удаления антивирусного ПО нажмите кнопку **Далее**.

2.4. Запуск и останов интерфейса Dr.Web Агента

Запуск **Dr.Web Агента** осуществляется автоматически после его установки, а также каждый раз после загрузки ОС Windows.

Запущенный **Dr.Web Агент** в среде ОС Windows выводит значок  в область уведомления Панели задач.

Команда **Выход** в контекстном меню **Агента** только удаляет значок из области уведомлений **Панели задач**. **Агент** при этом продолжает работу.

Значок **Агента** автоматически выводится в область **Панели задач** при запуске **Агента** после загрузки ОС Windows.

Для отображения значка **Агента** (если значок был удален при помощи команды **Выход**) без перезагрузки компьютера достаточно запустить интерфейс **Агента** следующим образом:

- Для ОС младше Windows 8: **Пуск** → **Программы** → **Dr.Web Enterprise Suite** → пункт **Start AgentUI**.
- Для ОС Windows 8: меню **Приложения** (открывается через пункт Все приложения на панели приложений стартового экрана) → раздел **Dr.Web Enterprise Suite** → пункт **Start AgentUI**.

Для запуска интерфейса Агента от имени пользователя с административными правами:

- для ОС младше Windows Vista:
  1. Нажмите на пункт **Start AgentUI** (см. выше) правой кнопкой мыши и в контекстном меню выберите опцию **Запуск от имени**.
  2. В открывшемся окне введите данные (логин и пароль) нужной вам учетной записи и нажмите **ОК**.
  3. Интерфейс **Агента** будет запущен от имени указанного пользователя.
- для ОС Windows Vista и старше:
  1. В контекстном меню значка **Агента** выберите пункт **Администратор**.
  2. При условии включенного UAC подтвердите запрос на запуск приложения от имени администратора.
  3. Интерфейс **Агента** будет запущен от имени администратора.

2.5. Управление Dr.Web Агентом

Запущенный **Dr.Web Агент** в среде ОС Windows выводит значок  в область уведомлений **Панели задач**.

При наведении курсора мыши на значок **Агента**, выводится всплывающее информационное окно, содержащее сводные

данные по вирусным событиям, состоянию компонентов антивирусного ПО и дате последнего обновления (см. также п. Информационные сообщения).

Доступные для изменения и просмотра функции **Dr.Web Агента** вызываются из контекстного меню значка **Dr.Web Агента**. Для этого следует нажать правой кнопкой мыши на значок и выбрать необходимую команду.

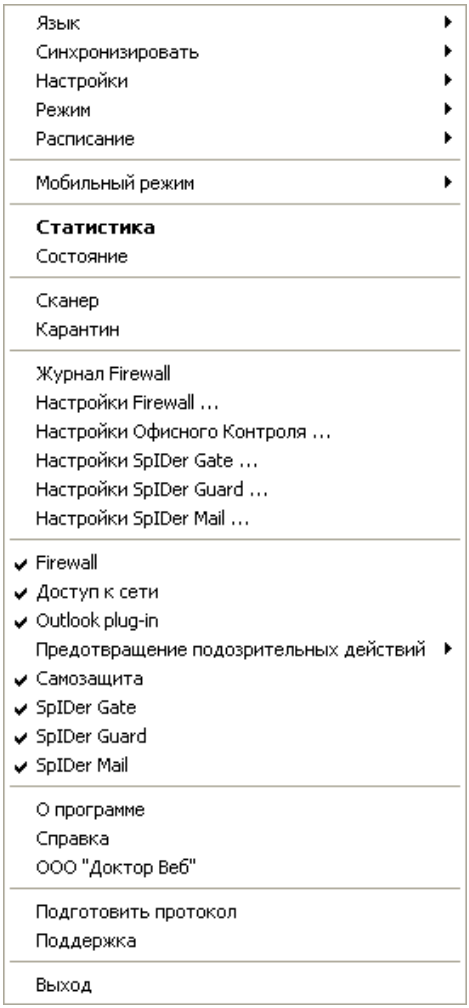

Рисунок 2-1. Контекстное меню Dr.Web Агента.

В состав контекстного меню входят пункты:

- **Выход** - убрать значок **Dr.Web Агента** из области уведомлений на **Панели задач** (см. п. Запуск и останов интерфейса Dr.Web Агента).

- **Поддержка** - перейти на веб-страницу технической поддержки компании **«Доктор Веб»** для получения технической поддержки абонента.
- **Подготовить протокол** - создать архив (в формате zip) с набором файлов протокола и информацией о системе для отправки в службу технической поддержки.
- **ООО "Доктор Веб"** - перейти на сайт компании **«Доктор Веб»**.
- **Справка** - вызов Справки **Dr.Web Агента**.
- **О программе** - просмотреть информацию о программе и ее версии. Также из информационного окна можно перейти на веб-страницу компании **«Доктор Веб»** и на веб-страницу технической поддержки компании **«Доктор Веб»**.
- **SpIDer Mail** - включить/выключить почтовый монитор **SpIDer Mail**.

  SpIDer Mail автоматически проверяет все обращения любых почтовых программ вашего компьютера к серверам электронной почты.

- **SpIDer Guard** - включить/выключить файловый монитор **SpIDer Guard**.

  SpIDer Guard проверяет "на лету" все открываемые файлы и постоянно отслеживает действия запущенных процессов, характерные для вирусов.

- **SpIDer Gate** - включить/выключить HTTP-монитор **SpIDer Gate**.

  SpIDer Gate помогает защитить ваш компьютер от вредоносных программ, которые могут распространяться при сетевом взаимодействии по протоколу HTTP.

- **Самозащита** - включить/выключить системный монитор **SelfPROtect**.

  Этот компонент обеспечивает защиту файлов и каталогов **Dr.Web** от несанкционированного или невольного вмешательства. Например, удаления вирусами. При включенном системном мониторе доступ к указанным ресурсам имеют только программы **Dr.Web**.

- В выпадающем списке **Предотвращение подозрительных действий** доступны следующие опции:
  - **Запрещать модификацию системного файла HOSTS** устанавливает запрет на внесение изменения в файл HOSTS, который используется операционной системой для упрощения доступа к сети Интернет: для преобразования текстовых имен некоторых сайтов в соответствующие им IP-адреса. Изменение файла HOSTS может свидетельствовать о действии вредоносных программ.
  - **Запрещать модификацию важных объектов Windows** устанавливает запрет на изменение критически важных объектов операционной системы (реестр и т.п.).
- **Outlook plug-in** - включить/выключить подключаемый модуль **Dr.Web для Outlook**.

  Dr.Web для Outlook осуществляет проверку электронной почты, получаемой/отправляемой при помощи почтовой программы Microsoft Outlook.
- **Доступ к сети** - при наличии этого флага доступ к локальной сети и Интернету разрешен, иначе - заблокирован.
- **Firewall** - включить/выключить Сетевой экран **Dr.Web Firewall**.

  Сетевой экран **Dr.Web Firewall** предназначен для защиты вашего компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети.

Подробная информация об остальных пунктах меню приведена в следующих главах данного Руководства. Для перехода к нужному разделу, нажмите на соответствующий пункт контекстного меню на рисунке 2-1.

Состав настроек, доступных через контекстное меню значка **Dr.Web Агента**, может различаться в зависимости от конфигурации рабочей станции. Администратор антивирусной сети может ограничить права пользователя на управление и настройку антивирусных средств, установленных на компьютере пользователя.

Если какие-либо пункты контекстного меню недоступны, возможны два варианта:

1. Права, позволяющие изменять данные настройки, отключены на **Сервере** администратором антивирусной сети.
2. У пользователя нет прав администратора на данном компьютере.

Контекстное меню **Агента**, запущенного без прав администратора под ОС Windows Vista и старше, содержит дополнительный пункт **Администратор** (см. рис. 2-2). Данный пункт меню позволяет запустить **Dr.Web Агент** с правами администратора данного компьютера для возможности полного доступа к функциональности **Агента**: станут активны все пункты меню, разрешенные на **Enterprise Сервере**.

Контекстное меню **Агента**, запущенного с правами администратора под ОС Windows Vista и старше, при условии включенного UAC, содержит пункт **Пользователь** для запуска **Агента** без административных прав (от имени пользователя).

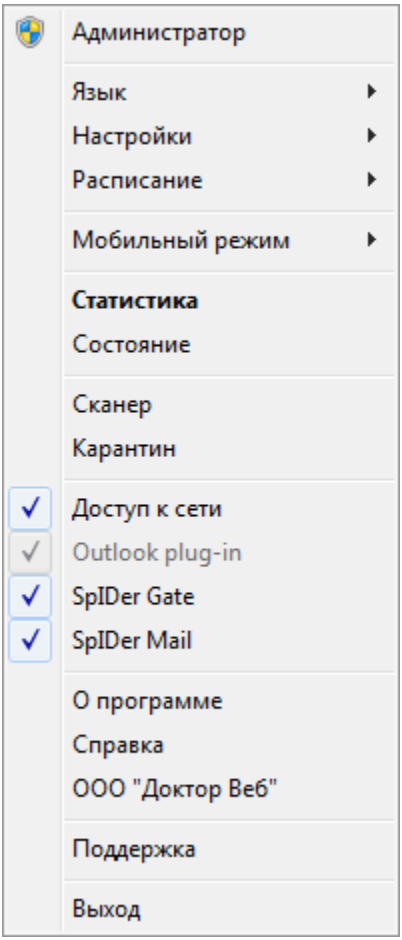

Рисунок 2-2. Контекстное меню Dr.Web Агента под пользователем ОС Windows 7

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

Вид значка **Dr.Web Агента** зависит от того, установлено ли соединение рабочей станции с **Сервером**, и других параметров. Возможные варианты и соответствующие им состояния компонентов приведены в таблице 2.

Таблица 2. Возможные виды значка и соответствующие им состояния компонентов

Значок	Описание	Состояние
	Черный рисунок на зеленом фоне.	**Агент** работает нормально и связывается с **Сервером**.
	Красные стрелки на фоне значка.	Отсутствует подключение к **Серверу**.
	Восклицательный знак в желтом треугольнике на фоне значка.	**Агент** запрашивает перезагрузку компьютера, либо отключены компоненты **SelfPROtect** или **Spider Guard**.
	Фон значка меняет цвет с зеленого на красный.	Произошла ошибка при обновлении компонентов пакета.
	Фон значка постоянно красного цвета.	**Агент** остановлен или не работает.
	Фон значка желтого цвета.	**Агент** работает в мобильном режиме.

Глава 3. Функциональность Dr.Web Агента

3.1. Настройка языка интерфейса

Смена языка интерфейса всех антивирусных компонентов осуществляется только при помощи **Dr.Web Агента**.

Для смены языка интерфейса **Dr.Web Агента** и компонентов антивирусного пакета **Dr.Web** выберите в контекстном меню значка **Агента** пункт меню **Язык**. В выпадающем списке укажите необходимый язык интерфейса.

3.2. Обновление антивирусного ПО

Как только появляются обновления антивирусного ПО **Dr.Web**, производится их автоматическая загрузка и установка. Однако в критических ситуациях вы можете вручную обновить компоненты ПО (предварительно посоветовавшись с администратором).

Запуск обновления антивирусного ПО, установленного на вашем компьютере, осуществляется при помощи пункта контекстного меню **Синхронизировать**.

- Когда фон значка **Агента** меняет цвет с зеленого на красный, вы должны принудительно синхронизировать компоненты, обновление которых прошло с ошибкой. Для этого выберите пункт **Только сбойные компоненты** команды контекстного меню **Синхронизировать**.

- Если необходимо обновить все установленные компоненты антивируса (например, в ситуации когда **Агент** долгое время не подключался к **Серверу** и т.д.), выберите **Все компоненты** команды контекстного меню **Синхронизировать**.

При принудительной синхронизации всех компонентов потребуется две перезагрузки станции. Следуйте указаниям **Агента**.

3.3. Настройки Dr.Web Агента

Доступ к настройкам **Dr.Web Агента** осуществляется при помощи команды **Настройки** контекстного меню **Агента**.

В выпадающем списке меню **Настройки** вы можете отметить тип сообщений о вирусных событиях на вашем ПК, которые вы хотите получать. Для этого установите флаг напротив соответствующего пункта меню (нажмите на пункт левой кнопкой мыши):

- **Важные оповещения** - получать только важные оповещения. К таковым относятся сообщения:
  - об ошибках при запуске какого-либо из компонентов антивирусного ПО;
  - об ошибках обновления антивирусного ПО или какого-либо из его компонентов, отображается сразу после ошибочного завершения процедуры обновления;
  - о необходимости перезагрузки компьютера после обновления, отображается сразу после обновления;
  - о необходимости ожидания сообщения о требовании перезагрузки для окончании установки компонентов.
- **Малозначительные оповещения** - получать только малозначительные оповещения. К таковым относятся сообщения:
  - о запуске удаленного сканирования;
  - о завершении удаленного сканирования;

- о запуске обновления антивирусного ПО или какого-либо из его компонентов;
- об успешном завершении обновления антивирусного ПО или какого-либо из его компонентов (без необходимости перезагрузки).

◆ **Оповещения о вирусах** - получать только оповещения о вирусах. К данному типу оповещений относятся сообщения об обнаружении вируса (вирусов) одним из компонентов антивирусного ПО.

Если вы хотите получать все группы сообщений, установите все три флага. В противном случае будут выводиться только сообщения указанных групп (см. также п. Информационные сообщения).

Чтобы включить режим синхронизации системного времени с **Сервером**, установите флаг **Синхронизировать время**. В данном режиме **Агент** периодически устанавливает системное время на вашем компьютере в соответствии со временем на **Сервере**.

Чтобы просмотреть или изменить параметры соединения с **Сервером**, выберите пункт **Соединение** (см. п. Настройки соединения с Сервером).

Чтобы просмотреть или изменить параметры ведения протокола вирусных событий на вашем компьютере, выберите пункт **Уровень протокола** (см. п. Уровень подробности протокола).

Пункт **Синхронизировать время** доступен в меню **Настройки** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

3.3.1. Настройки соединения с Сервером

Просмотр и редактирование настроек соединения с **Enterprise Сервером** осуществляется при помощи пункта контекстного меню **Настройки** → **Соединение.**

Пункт **Соединение** доступен в меню **Настройки** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

В диалоговом окне настроек соединения с **Enterprise Сервером** (см. рис. 3-1) вы можете изменить настройки подключения к текущему **Серверу** или настроить соединение с новым **Enterprise Сервером**.

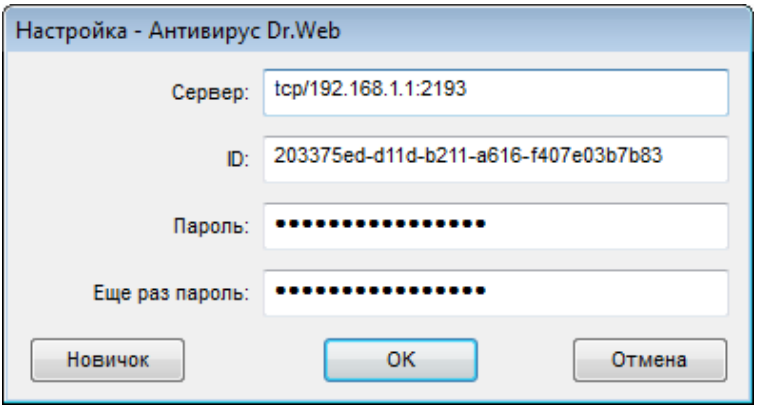

Рисунок 3-1. Настройки соединения с Сервером.

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

Настройки подключения к **Enterprise Серверу** можно менять только согласованно с администратором антивирусной сети, иначе ваш компьютер будет отключен от антивирусной сети.

При необходимости измените параметры:

- **Сервер** - введите имя **Enterprise Сервера** или его IP-адрес.
- **ID** - укажите идентификатор **Dr.Web Агента**, присвоенный вашему компьютеру для регистрации на **Сервере**.
- **Пароль** - укажите пароль **Dr.Web Агента** для подключения к **Enterprise Серверу**. В поле **Еще раз пароль** повторите тот же самый пароль.

Чтобы выйти из окна и сохранить изменения, нажмите **ОК**.

Чтобы выйти из окна, не сохраняя изменений, нажмите **Отмена**.

Чтобы сбросить все настройки соединения с **Сервером**, нажмите кнопку **Новичок**. В этом случае **Агент** потеряет связь с **Enterprise Сервером**, и антивирусный пакет не сможет обеспечивать максимально надежную защиту вашего компьютера. Чтобы потом настроить соединение с **Сервером** заново, вам потребуется ввести в этом диалоговом окне новые данные регистрации на **Сервере**. После подтверждения регистрации администратором антивирусной сети ваш компьютер будет снова подключен к **Enterprise Серверу**.

3.3.2. Уровень подробности протокола

Изменение уровня подробности протокола событий на вашем компьютере осуществляется при помощи пункта контекстного меню **Настройки** → **Уровень протокола**.

Пункт **Уровень протокола** доступен в меню **Настройки** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

В выпадающем списке выберите необходимое значение (**Отладка 3** - максимально детализированное ведение протокола, **Критические ошибки** - наименее детализированный протокол, сохраняются только сообщения об ошибках):

- **Отладка 3** … **Отладка** - отладочные сообщения с разной степенью детализации,
- **Трассировка 3** … **Трассировка** - отслеживание происходящих действий с разной степенью детализации,
- **Информация** - информационные сообщения,
- **Замечания** - важные информационные сообщения,
- **Предупреждения** - предупреждения о возможных ошибках,
- **Ошибки** - сообщения об ошибках функционирования,
- **Критические ошибки** - сообщения о критических ошибках функционирования.

3.4. Режим взаимодействия Агента с Сервером

Изменение параметров взаимодействия **Dr.Web Агента** с **Сервером** осуществляется при помощи команды **Режим** контекстного меню **Агента**.

Пункт **Режим** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

В выпадающем списке **Режим** доступны следующие пункты:

- **Соединяться с Dr.Web Enterprise Server** - для отправления администратору статистики и получения с **Сервера** инструкций и обновлений **Dr.Web**.
- **Принимать задания** - для периодического получения заданий от администратора по проверке вашего компьютера на вирусы.
- **Принимать обновления** - для получения регулярных обновлений компонентов антивируса и вирусных баз.
- **Запоминать события** - для сохранения и отключения отправки статистики о вирусных событиях на вашем компьютере.

  При включенной опции **Агент** продолжает взаимодействие с **Сервером**, но при этом на **Сервер** не будет отсылаться следующая информация:

  - периодическая статистика,
  - информация о вирусах,
  - изменение конфигурации **Агента** и антивирусных компонентов,

- информация о запуске и остановке антивирусных компонентов.

Информация является некритичной и не влияет на работоспособность **Агента**.

При этом данная информация сохраняется, и будет отправлена при следующем соединении с **Сервером** после выключения опции **Запоминать события**.

Данная опция может быть полезна при низкой пропускной способности канала.

3.5. Настройка расписания

В зависимости от настроек на **Сервере** вы можете редактировать и просматривать расписание работы антивирусного **Сканера**:

- задавать и менять локальное расписание проверок;
- просматривать централизованное расписание проверок.

Для этого вам нужно выбрать соответствующий пункт в выпадающем меню команды **Расписание** контекстного меню **Агента**.

3.5.1. Локальное расписание. Список локальных заданий

В зависимости от установок на **Сервере** вы можете создавать свое собственное расписание и добавлять в него различные типы заданий для проверки вашего компьютера.

Пункт **Локальное** доступен в меню **Расписание** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

При выборе пункта **Локальное** из раздела контекстного меню **Расписание** откроется окно вашего собственного расписания.

Если вы хотите назначить задание на сканирование вашего компьютера, нажмите кнопку **Добавить** и в появившемся меню выберите тип задания:

- Ежечасно
- Ежедневно
- Еженедельно
- Ежемесячно
- Каждые X минут
- При старте

Если в дальнейшем необходимо отредактировать какое-либо из назначенных заданий, выберите задание в списке и нажмите кнопку **Редактировать**.

Чтобы удалить задание, выберите его в списке и нажмите кнопку **Удалить**.

Запустить сканирование немедленно можно выбрав команду **Сканер** в контекстном меню значка Dr.Web Агента.

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

3.5.1.1. Ежечасное задание

Данный тип задания будет выполняться через каждый час в указанную минуту часа.

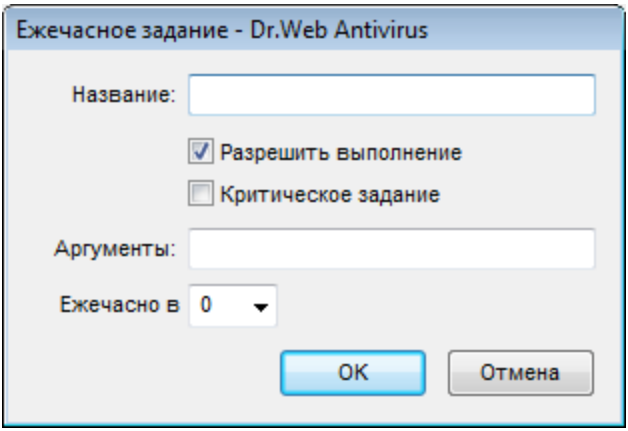

Рисунок 3-2. Диалоговое окно ежечасного задания

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

В диалоговом окне ежечасного задания (см. рис. 3-2) вы можете задать следующие параметры:

- **Название** - введите название задания.
- Установите флаг **Разрешить выполнение** чтобы разрешить выполнение задания.

  Чтобы запретить выполнение задания, уберите флаг. При этом задание останется в списке, но не будет выполняться.

- Установленный флаг **Критическое задание** дает указание выполнить это задание при следующем запуске **Dr.Web Агента**, если выполнение данного задания будет пропущено

(**Dr.Web Агент** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Dr.Web Агента** оно выполняется 1 раз.

- **Аргументы** - укажите при необходимости дополнительные параметры запуска задания. При этом используются параметры командной строки, указанные в Приложении Ключи командной строки для Сканера.
- **Ежечасно в** - укажите минуту выполнения ежечасного задания.

Чтобы выйти из окна и сохранить параметры задания, нажмите **ОК.**

Чтобы выйти из окна, не сохраняя изменений/нового задания, нажмите **Отмена**.

3.5.1.2. Ежедневное задание

Данный тип задания будет выполняться каждый день в указанное время.

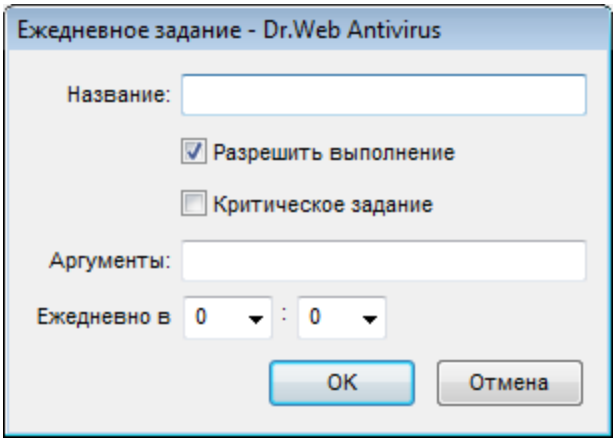

Рисунок 3-3. Диалоговое окно ежедневного задания

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

В диалоговом окне ежедневного задания (см. рис. 3-3) вы можете задать следующие параметры:

- **Название** - введите название задания.
- Установите флаг **Разрешить выполнение** чтобы разрешить выполнение задания.

  Чтобы запретить выполнение задания, уберите флаг. При этом задание останется в списке, но не будет выполняться.

- Установленный флаг **Критическое задание** дает указание выполнить это задание при следующем запуске **Dr.Web Агента**, если выполнение данного задания будет пропущено (**Dr.Web Агент** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Dr.Web Агента** оно выполняется 1 раз.
- **Аргументы** - укажите при необходимости дополнительные параметры запуска задания. При этом используются параметры командной строки, указанные в Приложении Ключи командной строки для Сканера.
- **Ежедневно в** - укажите час и минуту выполнения ежедневного задания.

Чтобы выйти из окна и сохранить параметры задания, нажмите **ОК.**

Чтобы выйти из окна, не сохраняя изменений/нового задания, нажмите **Отмена.**

3.5.1.3. Еженедельное задание

Данный тип задания будет выполняться каждую неделю в указанный день недели в установленное время.

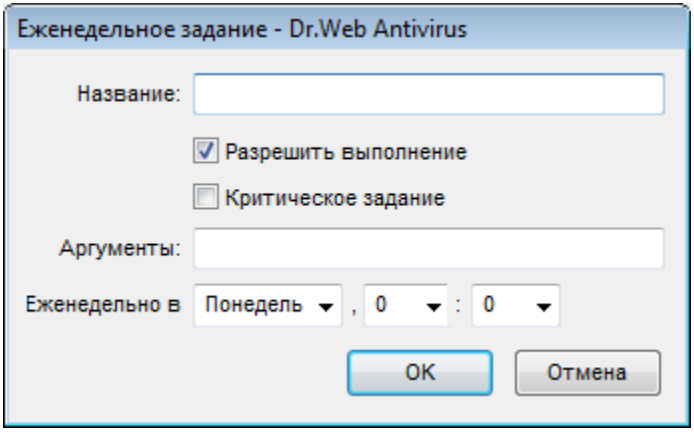

Рисунок 3-4. Диалоговое окно еженедельного задания

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

В диалоговом окне еженедельного задания (см. рис. 3-4) вы можете задать следующие параметры:

- **Название** - введите название задания.
- Установите флаг **Разрешить выполнение** чтобы разрешить выполнение задания.

  Чтобы запретить выполнение задания, уберите флаг. При этом задание останется в списке, но не будет выполняться.

- Установленный флаг **Критическое задание** дает указание выполнить это задание при следующем запуске **Dr.Web Агента**, если выполнение данного задания будет пропущено (**Dr.Web Агент** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Dr.Web Агента** оно выполняется 1 раз.
- **Аргументы** - укажите при необходимости дополнительные параметры запуска задания. При этом используются параметры командной строки, указанные в Приложении

Ключи командной строки для Сканера.

- **Еженедельно в** - укажите день недели, час и минуту выполнения еженедельного задания.

Чтобы выйти из окна и сохранить параметры задания, нажмите **ОК.**

Чтобы выйти из окна, не сохраняя изменений/нового задания, нажмите **Отмена.**

3.5.1.4. Ежемесячное задание

Данный тип задания будет выполняться каждый месяц в указанный день месяца в установленное время.

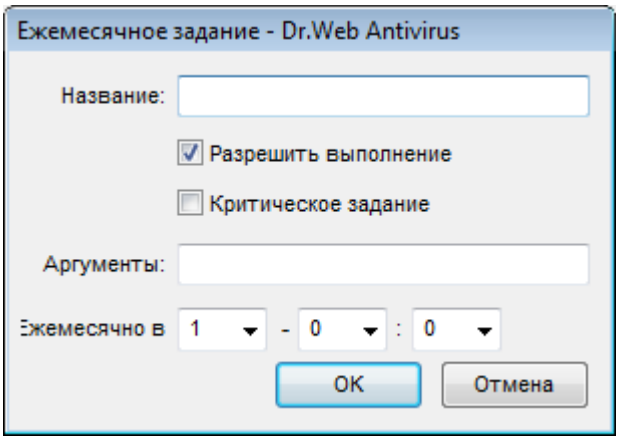

Рисунок 3-5. Диалоговое окно ежемесячного задания

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

В диалоговом окне ежемесячного задания (см. рис. 3-5) вы можете задать следующие параметры:

- **Название** - введите название задания.
- Установите флаг **Разрешить выполнение** чтобы разрешить выполнение задания.

  Чтобы запретить выполнение задания, уберите флаг. При этом задание останется в списке, но не будет выполняться.

- Установленный флаг **Критическое задание** дает указание выполнить это задание при следующем запуске **Dr.Web Агента**, если выполнение данного задания будет пропущено (**Dr.Web Агент** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Dr.Web Агента** оно выполняется 1 раз.
- **Аргументы** - укажите при необходимости дополнительные параметры запуска задания. При этом используются параметры командной строки, указанные в Приложении Ключи командной строки для Сканера.
- **Ежемесячно в** - укажите день месяца, час и минуту выполнения ежемесячного задания.

Чтобы выйти из окна и сохранить параметры задания, нажмите **ОК.**

Чтобы выйти из окна, не сохраняя изменений/нового задания, нажмите **Отмена.**

3.5.1.5. Задание, выполняемое каждые X минут

Данный тип задания будет выполняться через определенный интервал времени, заданный в минутах.

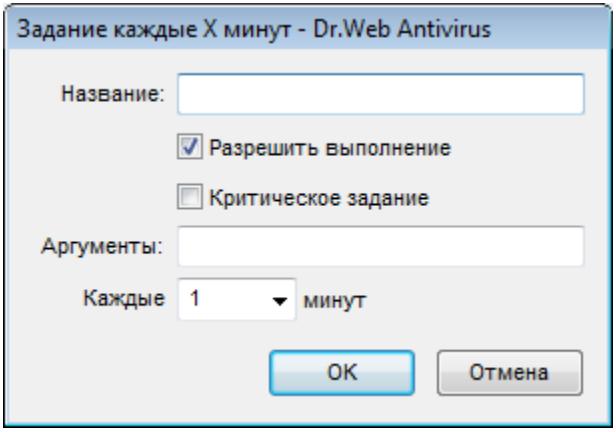

Рисунок 3-6. Диалоговое окно задания

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

В диалоговом окне задания (см. рис. 3-6) вы можете задать следующие параметры:

- **Название** - введите название задания.
- Установите флаг **Разрешить выполнение** чтобы разрешить выполнение задания.

  Чтобы запретить выполнение задания, уберите флаг. При этом задание останется в списке, но не будет выполняться.

- Установленный флаг **Критическое задание** дает указание выполнить это задание при следующем запуске **Dr.Web Агента**, если выполнение данного задания будет пропущено (**Dr.Web Агент** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Dr.Web Агента** оно выполняется 1 раз.
- **Аргументы** - укажите при необходимости дополнительные параметры запуска задания. При этом используются параметры командной строки, указанные в Приложении

Ключи командной строки для Сканера.

- **Каждые <...> минут** - укажите интервал выполнения задания в минутах.

Чтобы выйти из окна и сохранить параметры задания, нажмите **ОК.**

Чтобы выйти из окна, не сохраняя изменений/нового задания, нажмите **Отмена.**

3.5.1.6. Задание, выполняемое при старте

Данный тип задания будет выполняться при включении компьютера (запуске операционной системы).

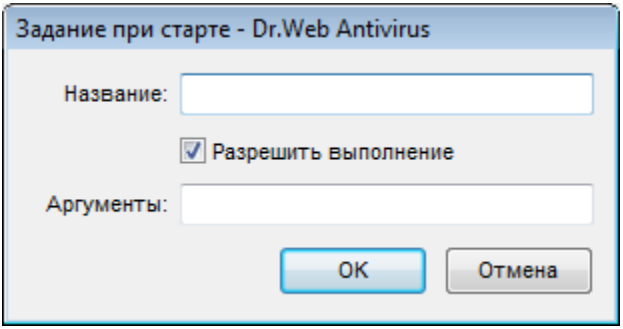

Рисунок 3-7. Диалоговое окно задания

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

В диалоговом окне задания (см. рис. 3-7) вы можете задать следующие параметры:

- **Название** - введите название задания.
- Установите флаг **Разрешить выполнение** чтобы разрешить выполнение задания.

Чтобы запретить выполнение задания, уберите флаг. При этом задание останется в списке, но не будет выполняться.

- **Аргументы** - укажите при необходимости дополнительные параметры запуска задания. При этом используются параметры командной строки, указанные в Приложении Ключи командной строки для Сканера.

Чтобы выйти из окна и сохранить параметры задания, нажмите **ОК.**

Чтобы выйти из окна, не сохраняя изменений/нового задания, нажмите **Отмена.**

3.5.2. Централизованное расписание

В окне централизованного расписания проверок вы можете просмотреть задания на сканирование компьютеров антивирусной сети, назначенные на **Enterprise Сервере**.

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

3.6. Настройки мобильного режима

Если ваш компьютер (или ноутбук) долгое время не будет иметь связи с **Enterprise Сервером**, для своевременного получения обновлений с серверов **BCO Dr.Web** рекомендуется установить мобильный режим работы **Dr.Web Агента**.

Для этого в контекстном меню значка **Агента** выберите пункт **Мобильный режим** → **Разрешен**. Цвет значка **Агента** изменится на желтый.

В мобильном режиме **Агент** пытается подключиться к **Серверу**, делает три попытки, и, если не удалось, выполняет HTTP-апдейт с серверов **ВСО Dr.Web**. Попытки обнаружения **Сервера** идут непрерывно с интервалом около минуты.

Пункт **Мобильный режим** будет доступен в контекстном меню при условии, что на **Сервере** в правах станции разрешен мобильный режим использования **ВСО Dr.Web**.

Чтобы задать настройки мобильного режима работы, выберите **Мобильный режим** → **Настройки**. Откроется окно настроек мобильности **Агента**.

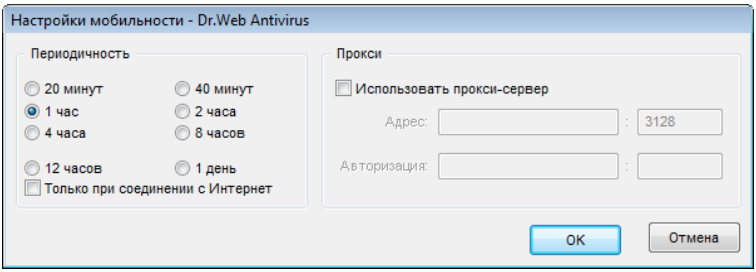

Рисунок 3-8. Диалоговое окно настроек мобильного режима

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

На панели **Периодичность** укажите частоту проверки наличия обновлений на **ВСО**:

- **20 минут** - проверять наличие обновлений каждые 20 минут.
- **40 минут** - проверять наличие обновлений каждые 40 минут.
- **1 час** - проверять наличие обновлений каждый час.

- **2 часа** - проверять наличие обновлений каждые 2 часа.
- **4 часа** - проверять наличие обновлений каждые 4 часа.
- **8 часов** - проверять наличие обновлений каждые 8 часов.
- **12 часов** - проверять наличие обновлений каждые 12 часов.
- **1 день** - проверять наличие обновлений раз в день.

Установите флаг **Только при соединении с Интернет**, если необходимо, чтобы проверка наличия обновлений производилась только при соединении с Интернет.

При использовании прокси-сервера установите флаг **Использовать прокси-сервер**. В этом случае станут активными поля:

- **Адрес** - для указания адреса и порта прокси-сервера.
- **Авторизация** - для указания параметров авторизации на прокси-сервере: логина и пароля.

Чтобы немедленно запустить обновление в мобильном режиме, выберите в контекстном меню **Агента** пункт **Мобильный режим** → **Запустить обновление**.

Во время функционирования **Агента** в мобильном режиме связь **Агента** с **Enterprise Сервером** прерывается. Все изменения, которые задаются на **Сервере** для такой станции, вступят в силу как только мобильный режим работы **Агента** будет выключен и связь **Агента** с **Сервером** возобновится.

В мобильном режиме производится обновление только вирусных баз.

Чтобы отключить мобильный режим, в контекстном меню **Агента** выберите пункт **Мобильный режим** и снимите флаг **Разрешен**. Цвет значка **Агента** изменится с желтого на зеленый, и связь **Агента** с **Сервером** возобновится.

3.7. Просмотр статистики

Для просмотра статистики рабочей станции выберите в контекстном меню **Агента** пункт **Статистика**. Или дважды щелкните левой кнопкой по значку **Агента**. Откроется окно с таблицей, содержащей всю статистику по работе антивирусного ПО.

В первом столбце таблицы перечислены компоненты **Dr.Web**, которые были хоть раз запущены на вашем компьютере за текущий сеанс работы. Если при этом компонент не осуществлял сканирование (нулевое количество просканированных объектов), то он не будет отображен в списке статистики.

В остальных столбцах указано количество объектов, просканированных за текущий сеанс работы.

Объекты разделяются на следующие категории:

- обнаруженные антивирусом инфицированные объекты,
- модификации вирусов,
- подозрительные,
- вирусные активности.

Затем указывается количество объектов, которые были:

- исцелены,
- удалены,
- переименованы,
- перемещены,
- заблокированы.

Далее приведено количество ошибок и скорость при сканировании.

Более подробно об этих категориях статистики вы можете узнать в разделе Вкладка статистика главы Сканер Dr.Web для Windows.

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

3.8. Просмотр состояния антивирусного ПО

Для просмотра состояния антивирусного ПО, установленного на рабочей станции, выберите в контекстном меню **Агента** пункт **Состояние**.

В верхней части открывшегося окна выводится общая информация:

- общее количество записей в вирусной базе,
- дата последнего обновления,
- версия работающего на станции **Агента**,
- активность сканирования (запущен ли в данный момент на станции сканер).

Также окно состояния содержит следующие вкладки:

- **Базы**. Содержит подробную информацию обо всех установленных вирусных базах:
  - название файла, содержащего конкретную вирусную базу,
  - версия вирусной базы,
  - количество записей в вирусной базе,
  - дата создания вирусной базы.
- **Компоненты**. Содержит подробную информацию обо всех установленных на рабочей станции компонентах антивируса **Dr.Web**:
  - название компонента,

- состояние компонента: запущен (работает) или не запущен (выключен).

- **Модули**. Содержит подробную информацию обо всех модулях антивируса **Dr.Web**:
  - файл, определяющий отдельный модуль продукта,
  - полная версия модуля,
  - описание модуля - его функциональное название.

В нижней части окна состояния выводятся:

- Строка состояния антивирусного ПО. Содержит важные оповещения (см. п. Настройки Dr.Web Агента). При нормальной работе **Агента** - выводится сообщение **Вмешательство не требуется**.
- ID (уникальный идентификационный номер) **Агента**.

Во всех диалоговых окнах **Dr.Web Агента**, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

3.9. Информационные сообщения

В качестве системы оповещения пользователя выступают всплывающие окна, располагающиеся непосредственно возле значка **Dr.Web Агента**.

Сообщения во всплывающих окнах могут содержать информацию различного вида:

- Оповещения - подробная информация о производимых или необходимых действиях относительно антивирусного ПО или вашего ПК.
- Сводка **Dr.Web Агента** - сводные данные о работе и состоянии антивирусного ПО.
- Сообщения от администратора.

Оповещения

При помощи информационных сообщений выводятся оповещения о вирусных событиях и действиях антивирусного ПО на вашем ПК (подробнее см. п. Настройки Dr.Web Агента).

Помимо информативных функций, всплывающие сообщения могут нести и управляющие функции. Например, окно о необходимости перезагрузки ПК после обновления антивирусных компонентов (см. рис. 3-9) имеет диалоговый формат и содержит кнопки, позволяющие произвести перезагрузку компьютера или отложить напоминание об ее необходимости на заданное время. Чтобы отложить перезагрузку, выберите в выпадающем списке требуемый промежуток времени и нажмите **Позднее**.

Рисунок 3-9. Оповещение от Dr.Web Агента

Сводка Dr.Web Агента

При наведении курсора мыши на значок **Dr.Web Агента**, выводится всплывающее информационное окно, содержащее сводные данные о:

- статистике вирусных событий (см. также п. Просмотр статистики),

- состоянии компонентов антивирусного ПО,
- дате последнего обновления.

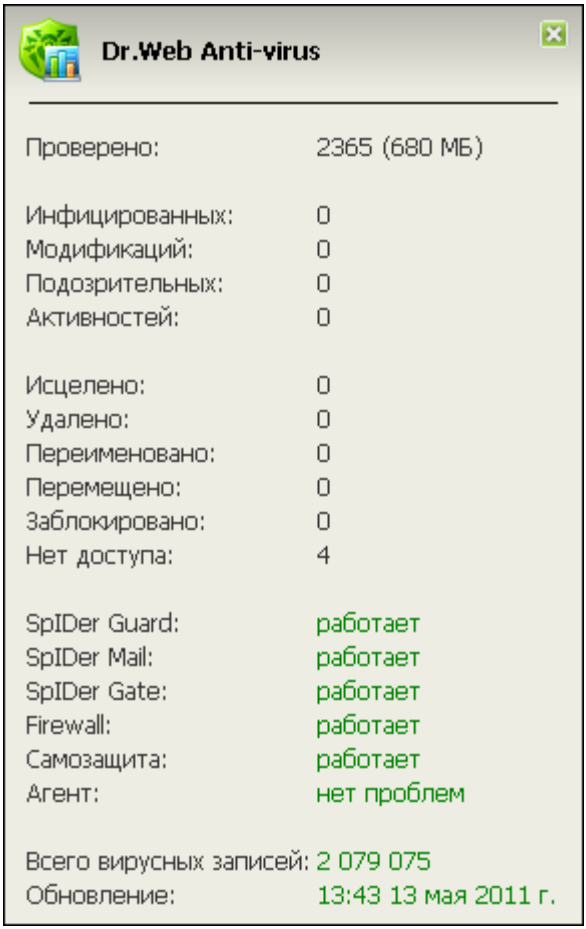

Рисунок 3-10. Информационное окно Dr.Web Агента

Сообщения от администратора

Пользователь может получать от системного администратора антивирусной сети информационные сообщения произвольного содержания, включающие:

- текст сообщения;
- гиперссылки на интернет-ресурсы;
- логотип компании (или любое графическое изображение);
- в заголовке окна также указывается точная дата получения сообщения.

Данные сообщения выводятся в виде всплывающих окон (см. рис. 3-11).

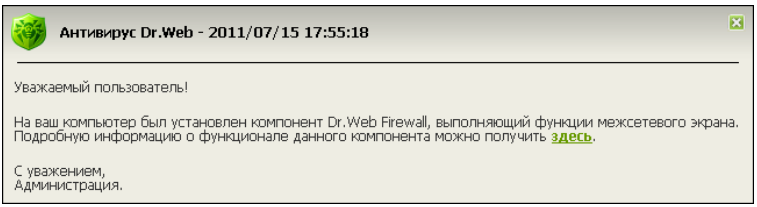

Рисунок 3-11. Окно сообщения от администратора

В отличие от всплывающих окон с оповещениями и сводкой **Dr.Web Агента**, которые будут скрыты при неактивности по истечение некоторого времени, окна с сообщениями от администратора будут отображаться, пока пользователь самостоятельно их не закроет.

Глава 4. Dr.Web Сканер для Windows

При помощи команды **Сканер** из контекстного меню **Агента** вы можете запускать антивирусный **Dr.Web Сканер для Windows** для периодической проверки вашего компьютера на вирусы и вредоносное ПО.

Dr.Web Сканер для Windows предназначен для антивирусного сканирования загрузочных секторов, памяти, а также как отдельных файлов, так и объектов в составе сложных структур (архивы, контейнеры, электронные письма с вложениями).

Установленная версия **Dr.Web Сканера для Windows** различается в зависимости от операционной системы. Существуют две версии **Dr.Web Сканера**:

- Dr.Web Сканер,
- Dr.Web Сканер NT4.

Перед установкой **Сканера** автоматически определяется версия операционной системы и устанавливается соответствующая версия **Dr.Web Сканера** (см. п. Системные требования).

Для перехода на справку **Антивирус Dr.Web для Windows** нажмите клавишу F1 в любом окне **Сканера**.

4.1. Dr.Web Сканер

Описание доступных режимов проверки при помощи **Dr.Web Сканера** приведено в Руководстве **Антивирус Dr.Web для Windows,** раздел **Виды проверки**.

Описание действий **Dr.Web Сканера** при обнаружении зараженных и подозрительных объектов приведено в Руководстве **Антивирус Dr.Web для Windows**, раздел **Действия при обнаружении угроз**.

Описание настройки параметров работы **Dr.Web Сканера** приведено в Руководстве **Антивирус Dr.Web для Windows**, раздел **Настройка Сканера Dr.Web**.

4.2. Dr.Web Сканер NT4

4.2.1. Антивирусная проверка

4.2.1.1. Виды проверки

Dr.Web Сканер NT4 (далее - **Сканер**) поддерживает несколько режимов проверки.

Быстрая проверка

В данном режиме производится сканирование следующих объектов:

- оперативная память;
- загрузочные секторы всех дисков;
- объекты автозапуска;
- корневой каталог загрузочного диска;
- корневой каталог диска установки ОС Windows;
- системный каталог ОС Windows;
- каталог документов пользователя `Мои Документы`;
- временный каталог системы;
- временный каталог пользователя.

Полная проверка

В данном режиме производится полное сканирование оперативной памяти, всех жестких дисков и сменных носителей (включая загрузочные секторы).

Выборочно

Данный режим предоставляет возможность выбрать любые каталоги и файлы для последующего сканирования.

При выборе данного режима в центральной части вкладки **Проверка** будет представлена файловая система в виде иерархического списка (дерева). При необходимости его можно развернуть вплоть до каталогов любого уровня и файлов в них.

Выберите в иерархическом списке объекты, которые будут подвергнуты сканированию. Наряду с выбранными объектами будут проверены загрузочные секторы всех дисков.

На рисунке изображена ситуация, в которой в режиме **Выборочно** выбран для проверки каталог на диске C.

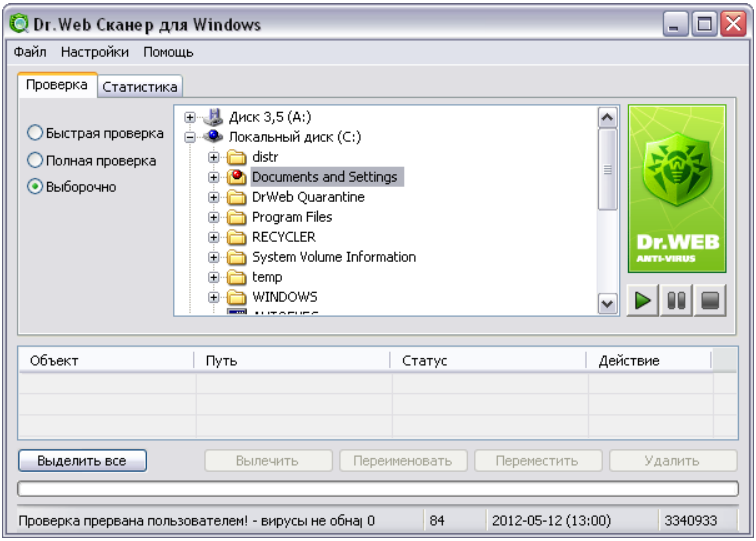

Рисунок 4-1. Главное окно Dr.Web Сканера. Вкладка Проверка.

По умолчанию наряду с выбранными объектами также будут проверяться подкаталоги всех выбранных каталогов и логических дисков, а также загрузочные секторы всех логических дисков, на которых выбран хотя бы один каталог или файл, а также главные загрузочные секторы соответствующих физических дисков.

При быстром и полном типе проверки **Сканер** определит, не был ли изменен HOSTS-файл (текстовый файл, который содержит базу данных доменных имен и используется при их трансляции в сетевые адреса узлов). HOSTS-файл может подвергнуться воздействию вредоносных программ (например, с целью перенаправить пользователя на определённый сайт).

В случае, если HOSTS-файл был изменен, **Сканер** предложит восстановить его исходное состояние. Это позволит устранить несанкционированное изменение файла вредоносным программным обеспечением.

4.2.1.2. Запуск антивирусного сканирования

По умолчанию сканирование осуществляется с использованием всех методов обнаружения вредоносных объектов, при этом:

- распаковываются и проверяются исполняемые файлы, упакованные специальными упаковщиками;
- проверяются файлы в архивах всех распространенных типов (ACE (до версии 2.0), ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP и др.);
- проверяются файлы в составе файловых контейнеров (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM и др.);
- проверяются электронные письма (формат писем должен соответствовать стандарту RFC822), хранящиеся в почтовых ящиках программ обработки электронной почты.

Запуск антивирусного сканирования

1. В контекстном меню значка **Агента** выберите пункт **Сканер**. Откроется главное окно **Сканера**.

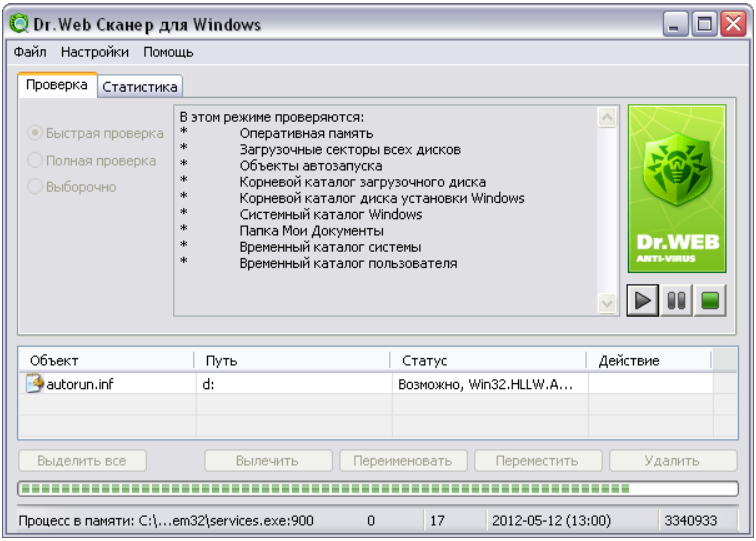

Рисунок 4-2. Главное окно Dr.Web Сканера для Windows.

2. Перед запуском сканирования выберите один из следующих типов проверки на вкладке Проверка:
   - Быстрая проверка;
   - Полная проверка;
   - Выборочно.

   Далее вы также сможете остановить запущенное сканирование и задать другой тип проверки.

3. При необходимости задайте настройки сканирования в разделе Настройки.

   Также при необходимости измените принцип задания действий над обнаруженными угрозами, установленный по умолчанию (подробнее см. п. Действия при обнаружении угроз), в разделе настроек **Действия**.

4. Для управления проверкой используйте следующие кнопки в правой части окна:
   - **Пуск** - чтобы приступить к сканированию;

-  **Пауза** - чтобы приостановить проверку. Чтобы продолжить проверку, повторно нажмите кнопку  **Пуск**;
-  **Стоп** - чтобы остановить проверку.

5. Результаты сканирования отражаются в списке в нижней части вкладки **Проверка** и на вкладке Статистика. Таблица отчета включает следующую информацию:

Колонка	Описание
Объект	Наименования зараженных или подозрительных объектов, загрузочных секторов или процессов в памяти. Если вредоносный или подозрительный объект обнаружен внутри составного объекта (архива, файла электронной почты или файлового контейнера), то в отчете также указывается наименование составного объекта.
Путь	Полный путь к вредоносному объекту (для файлов и загрузочных секторов) или информация о зараженном архиве.
Статус	Для файлов и загрузочных секторов: наименование вредоносной программы или ее модификации (модификацией известного вируса называется код, полученный таким изменением известного вируса, что при этом он опознается, но алгоритмы лечения исходного вируса к нему неприменимы) по внутренней классификации компании **«Доктор Веб»**. Для угроз в составе составного объекта указывается информация о составном объекте. Для подозрительных объектов указывается, что объект *возможно инфицирован* и указывается тип возможной вредоносной программы по классификации эвристического анализатора.
Действие	Информация о действиях, предпринятых **Сканером** для деактивации вредоносной программы. Например, лечение, удаление, переименование, перемещение.

Колонка	Описание
	Если обнаруженный объект используется другим приложением ОС Windows, выбранное вами действие не может быть выполнено немедленно. Для таких объектов в поле отчета **Сканера** в колонке **Действие** появляется запись **Будет излечен после рестарта**, **Будет удален после рестарта** или **Будет переименован после рестарта** в зависимости от выбранного действия. Соответственно только при последующей перезагрузке нужное действие будет фактически выполнено. Поэтому при обнаружении таких объектов рекомендуется провести перезагрузку системы сразу после окончания сканирования.

Кроме кнопок и пунктов меню для доступа к различным окнам, настройкам и функциям предусмотрены клавиши быстрого доступа

F1 – вызвать справку;

F3 – открыть главное окно **Dr.Web Сканера** на вкладке **Проверка**;

F4 – открыть главное окно **Dr.Web Сканера** на вкладке **Статистика**;

F5 – открыть окно задания пути и маски проверки;

F7 – запустить быструю проверку (сканирование оперативной памяти и объектов автозапуска);

F8 – запустить процесс обновления;

F9 – открыть окно настроек **Dr.Web Сканера**;

F10 – перевести фокус на меню текущего окна;

CTRL+F5 – запустить сканирование;

CTRL+F6 – остановить сканирование;

CTRL+F2 – очистить отчет **Dr.Web Сканера**;

ALT+X – завершить работу **Dr.Web Сканера**.

4.2.1.3. Действия при обнаружении угроз

В случае обнаружения известного вируса или при подозрении на зараженность объекта вирусом, возможны следующие варианты задания действия над этим объектом:

1. По умолчанию **Сканер** информирует пользователя об обнаруженных угрозах в специальном поле отчета, расположенном в нижней части вкладки **Проверка**. Инфицированные процессы, обнаруженные в памяти компьютера, автоматически прекращаются, а обнаруженные троянские программы – удаляются. При этом пользователю предоставляется возможность выбрать дальнейшие действия для конкретных обнаруженных объектов (подробнее см. раздел Задание действий над обнаруженными угрозами).
2. Если в настройках **Сканера** на вкладке **Действия** была отключена опция **Запрос подтверждения**, **Сканер** автоматически без запроса пользователя применяет к обнаруженным угрозам реакции, заданные на вкладке **Действия** (подробнее см. раздел Вкладка Действия).

Задание действий над обнаруженными угрозами

При настройках по умолчанию, в случае обнаружения вредоносного объекта **Сканер** предупреждает вас об угрозе (исключение составляют программы-шутки, потенциально опасные программы и программы взлома, которые при обнаружении по умолчанию игнорируются). Отчет о результатах проверки приводится в таблице, где вы можете вручную выбрать необходимое действие для обработки обнаруженного объекта.

В поле отчета в табличной форме представлены сведения о найденных в ходе сканирования зараженных и подозрительных объектах, а также о действиях, произведенных **Сканером**. Если указанные объекты обнаружены в файловых архивах, почтовых файлах или файловых контейнерах, в таблице приводятся как инфицированные объекты, так и содержащие их архивы.

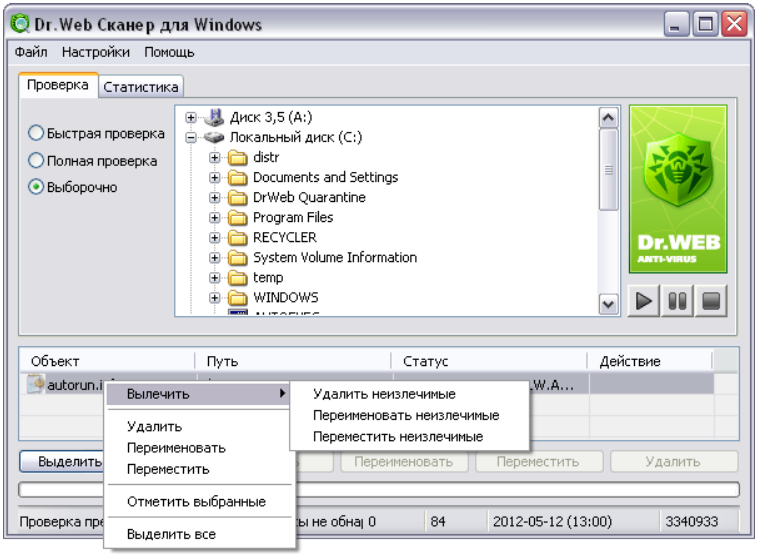

Рисунок 4-3. Главное окно Dr.Web Сканера. Вкладка Проверка.

Возможны следующие действия, применяемые к обнаруженным объектам:

Действие	Описание
Вылечить	Восстановить состояние объекта до заражения. При выборе этого действия открывается дополнительное контекстное меню, в котором необходимо выбрать реакцию **Сканера** в случае невозможности лечения конкретного объекта. Данное действие возможно только при обнаружении объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров). Это единственное действие, доступное для зараженных загрузочных секторов.
Удалить	Удалить объект.

Действие	Описание
	Данное действие неприменимо для загрузочных секторов.
Переименовать	Изменить расширение файла объекта в соответствии с настройками **Сканера**. По умолчанию первый символ расширения заменяется на символ #. Данное действие неприменимо для загрузочных секторов.
Переместить	Переместить объект в специальный каталог **Карантина**, путь к которому задается настройками **Сканера**. Данное действие неприменимо для загрузочных секторов.

Выполнение действий по устранению угроз

1. Выберите объект в таблице отчета. Чтобы выбрать несколько объектов, удерживайте клавишу SHIFT или CTRL. Также вы можете использовать следующие клавиши и комбинации клавиш:
   - INSERT – выделить объект с перемещением курсора на следующую позицию;
   - CTRL+A – выделить все;
   - клавиша * на цифровой клавиатуре – выделить все или полностью снять выделение.
2. Выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши по выделенному объекту и в контекстном меню выберите действие, которое вы хотите применить.
   - Нажмите на кнопку, соответствующую действию, которое вы хотите применить, под полем отчета.

Любые действия для отдельных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров) невозможны. Действие в таких случаях применяется только ко всему объекту целиком. При этом по умолчанию при выборе действия **Удалить** для составного объекта **Сканер** выдает предупреждение о возможной потере данных.

Кроме кнопок и пунктов меню для доступа к различным окнам, настройкам и функциям предусмотрены клавиши быстрого доступа

F1 – вызвать справку;

F3 – открыть главное окно **Dr.Web Сканера** на вкладке **Проверка**;

F4 – открыть главное окно **Dr.Web Сканера** на вкладке **Статистика**;

F5 – открыть окно задания пути и маски проверки;

F7 – запустить быструю проверку (сканирование оперативной памяти и объектов автозапуска);

F8 – запустить процесс обновления;

F9 – открыть окно настроек **Dr.Web Сканера**;

F10 – перевести фокус на меню текущего окна;

CTRL+F5 – запустить сканирование;

CTRL+F6 – остановить сканирование;

CTRL+F2 – очистить отчет **Dr.Web Сканера**;

ALT+X – завершить работу **Dr.Web Сканера**.

4.2.2. Главное окно Dr.Web Сканера

Главное окно **Сканера** состоит из следующих вкладок:

- вкладка Проверка, на которой формируется задание на сканирование;
- вкладка Статистика, на которой предоставляется доступ к итоговым сведениям о работе **Сканера**.

4.2.2.1. Вкладка Проверка

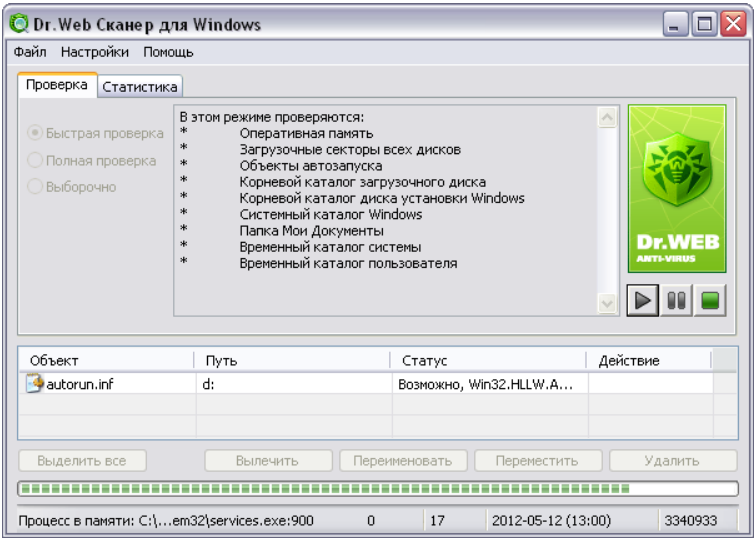

Рисунок 4-4. Главное окно Dr.Web Сканера. Вкладка Проверка. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Проверка** вы можете настраивать, запускать и наблюдать за сканированием объектов операционной системы Windows. По умолчанию **Сканер** использует все методы обнаружения вредоносных объектов.

В центральной части окна в зависимости от выбора режима сканирования отображается список объектов, которые будут подвергнуты проверке, либо иерархический список объектов файловой системы. В нижней части окна располагается таблица для отображения сведений о найденных в ходе сканирования зараженных и подозрительных объектах, а также о произведенных **Сканером** действиях.

Кроме кнопок и пунктов меню для доступа к различным окнам, настройкам и функциям предусмотрены клавиши быстрого доступа

F1 – вызвать справку;

F3 – открыть главное окно **Dr.Web Сканера** на вкладке **Проверка**;

F4 – открыть главное окно **Dr.Web Сканера** на вкладке **Статистика**;

F5 – открыть окно задания пути и маски проверки;

F7 – запустить быструю проверку (сканирование оперативной памяти и объектов автозапуска);

F8 – запустить процесс обновления;

F9 – открыть окно настроек **Dr.Web Сканера**;

F10 – перевести фокус на меню текущего окна;

CTRL+F5 – запустить сканирование;

CTRL+F6 – остановить сканирование;

CTRL+F2 – очистить отчет **Dr.Web Сканера**;

ALT+X – завершить работу **Dr.Web Сканера**.

4.2.2.2. Вкладка Статистика

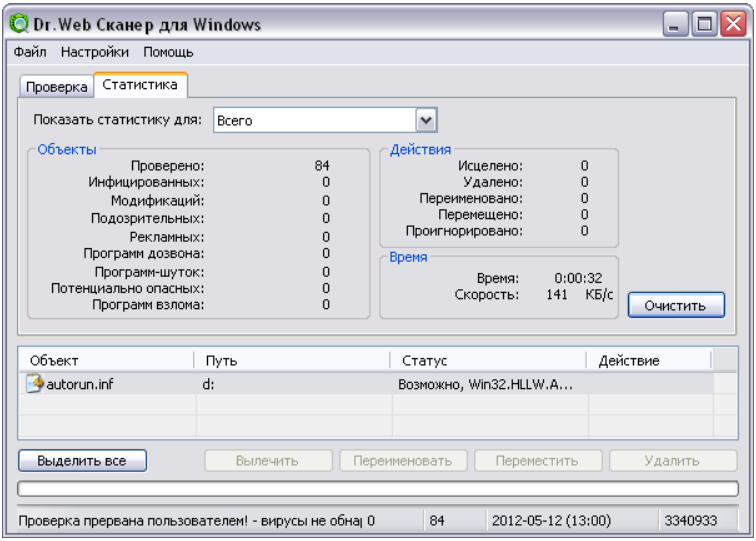

Рисунок 4-5. Главное окно Dr.Web Сканера. Вкладка Статистика

Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Статистика** собраны итоговые сведения о работе **Сканера**, включая общее количество проверенных объектов, количество обнаруженных объектов, инфицированных известными вирусами, модификациями известных вирусов, количество обнаруженных подозрительных объектов, а также сведения о действиях программы над зараженными и подозрительными объектами.

Вы также можете получить эти сведения для любого из логических дисков компьютера. Для этого выберите необходимый диск в выпадающем списке, расположенном в верхней части окна.

Для того чтобы обнулить статистические сведения, нажмите кнопку **Очистить**.

Кроме кнопок и пунктов меню для доступа к различным окнам, настройкам и функциям предусмотрены клавиши быстрого доступа

F1 – вызвать справку;

F3 – открыть главное окно **Dr.Web Сканера** на вкладке **Проверка**;

F4 – открыть главное окно **Dr.Web Сканера** на вкладке **Статистика**;

F5 – открыть окно задания пути и маски проверки;

F7 – запустить быструю проверку (сканирование оперативной памяти и объектов автозапуска);

F8 – запустить процесс обновления;

F9 – открыть окно настроек **Dr.Web Сканера**;

F10 – перевести фокус на меню текущего окна;

CTRL+F5 – запустить сканирование;

CTRL+F6 – остановить сканирование;

CTRL+F2 – очистить отчет **Dr.Web Сканера**;

ALT+X – завершить работу **Dr.Web Сканера**.

4.2.3. Настройка Сканера Dr.Web

Настройки по умолчанию являются оптимальными для большинства применений **Сканера**. Не следует изменять их без необходимости.

Изменение настроек Сканера Dr.Web

1. Если **Сканер** не запущен, запустите его. Для этого в контекстном меню значка **Агента** выберите пункт **Сканер**. Откроется главное окно **Сканера**.
2. Выберите в меню главного окна **Dr.Web Сканера** пункт **Настройки**, после чего в открывшемся подменю выберите пункт **Изменить настройки**. Откроется окно настроек, содержащее следующие вкладки:

- вкладка Проверка, на которой задаются списки каталогов и файлов, исключаемых из сканирования;
- вкладка Типы файлов, на которой задаются дополнительные ограничения на состав файлов, подлежащих проверке;
- вкладка Действия, на которой задается реакция **Сканера** на обнаружение зараженных или подозрительных файлов, вредоносных программ, а также инфицированных архивов;
- вкладка Отчет, задается режим ведения файла отчета **Сканера**;
- вкладка Общие, на которой задаются параметры взаимодействия **Сканера** с операционной системой, а также звуковые реакции на различные события.

3. Внесите необходимые изменения. При необходимости нажимайте кнопку **Применить** перед переходом на другую вкладку.
4. Чтобы получить информацию о настройках, расположенных на открытой вкладке, нажмите кнопку F1.
5. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.
6. Чтобы сохранить указанные настройки для последующих сеансов сканирования (которые будут запущены при следующем открытии **Сканера**), если на вкладке Общие отключен режим **Автосохранение настроек**, выберите в меню **Настройки** главного окна пункт **Сохранить настройки**.

4.2.3.1. Вкладка Проверка

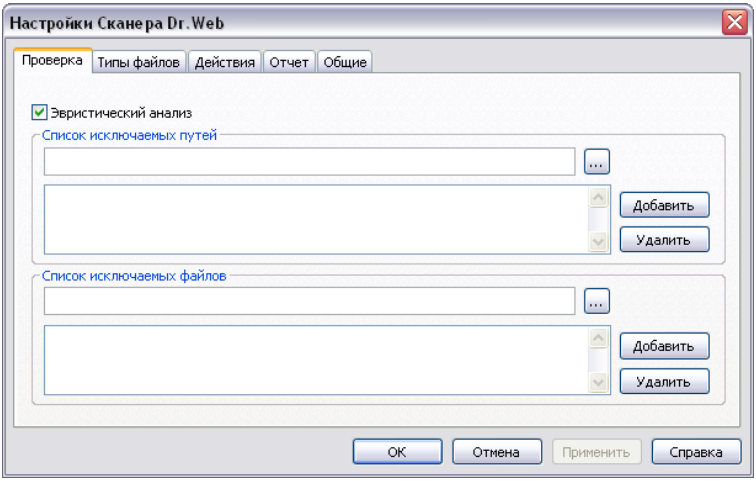

Рисунок 4-6. Окно настроек Dr.Web Сканера. Вкладка Проверка. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Проверка** задаются следующие настройки:

- Возможность использования эвристического анализа (метода, позволяющего выявлять подозрительные объекты, с большой вероятностью зараженные еще неизвестными вирусами).

  По умолчанию данная настройка включена. Рекомендуется сохранить использование эвристического анализа при сканировании и не менять данную настройку.

  Особенностью этого типа поиска вирусов является приблизительный, вероятностный характер обнаружения заражения, что позволяет говорить не о зараженных, а лишь о подозрительных объектах. Целый класс программ (например, мультисистемные загрузчики ПК) ввиду использования сходного с вирусами кода может вызывать ложные срабатывания эвристического анализатора. Кроме

того, данный вид проверки может несколько увеличить время проверки на ПК со слабыми процессорами. Эти обстоятельства могут быть доводами в пользу отмены эвристического анализа. Вместе с тем, сохранение этого типа анализа увеличивает надежность антивирусной защиты.

- Списки каталогов и файлов, исключаемых из сканирования.

Список исключаемых путей

В данной секции задается список каталогов, файлы в которых будут исключены из сканирования. В таком качестве могут выступать каталоги **Карантина** антивируса, рабочие каталоги некоторых программ и т.п.

Чтобы отредактировать список исключаемых путей:

1. Чтобы добавить каталог в список:
   a) Введите путь к каталогу, файлы в котором должны быть исключены из проверки. Вы также можете воспользоваться кнопкой **Обзор**  и выбрать конкретный каталог в браузере по операционной системе.
   b) Нажмите кнопку **Добавить**, расположенную справа. Каталог будет добавлен в список, расположенный ниже.
2. Для того чтобы удалить какой-либо каталог из списка, выберите его в этом списке и нажмите кнопку **Удалить**. Содержимое каталога будет допущено к последующей проверке.

Список исключаемых файлов

В данной секции задается список имен или масок файлов, которые будут исключены из сканирования. Все файлы с именами, совпадающими с именами или масками указанных файлов, будут исключены из проверки. В таком качестве могут выступать временные файлы, файлы подкачки и т.п.

Чтобы отредактировать список исключаемых файлов:

1. Чтобы добавить файл в список:
   a) введите имя файла, который должен быть исключен из проверки. Вы можете воспользоваться кнопкой **Обзор**  и выбрать объект в браузере по операционной системе. Также вы можете использовать маски.

Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в именах файлов, а также специальные обозначения:

- `*` заменяет любую (в том числе пустую) последовательность любых символов;
- `?` заменяет один любой символ в заданной позиции.

Примеры:

- **отчет*.doc** – маска, задающая все документы Microsoft Word, название которых начинается с последовательности символов `отчет`, например, файлы `отчет-февраль.doc`, `отчет121209.doc` и т.д.;
- ***.exe** – маска, задающая все исполняемые файлы с расширением `EXE`, например, `setup.exe`, `iTunes.exe` и т.д.;
- **photo????09.jpg** – маска, задающая все файлы изображений формата `JPG`, название которых начинается с последовательности символов `photo` и заканчивается последовательностью символов `09`, при этом между двумя этими последовательностями в названии файла стоит четыре произвольных символа, например,

```
photo121209.jpg, photomama09.jpg или
photo----09.jpg.
```

b) Нажмите кнопку **Добавить**, расположенную справа. Файл (маска файла) будет добавлен в список, расположенный ниже.

2. Для того чтобы удалить какой-либо объект из списка, выберите его в списке и нажмите кнопку **Удалить**. Файл будет допущен к последующей проверке.

При необходимости исключения из антивирусной проверки определенного файла, внесите полный путь к данному файлу включая его имя в **Список исключаемых путей** (вы можете воспользоваться кнопкой **Обзор**  , чтобы выбрать каталог, где расположен файл, а затем ввести имя файла вручную после выбранного пути).

4.2.3.2. Вкладка Типы файлов

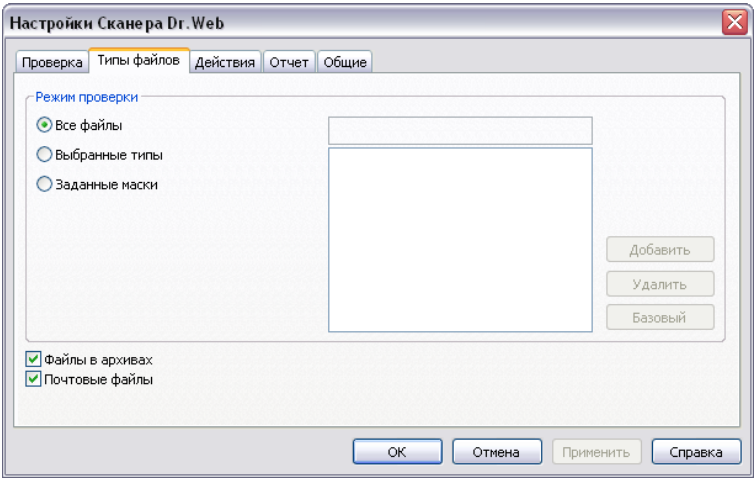

Рисунок 4-7. Окно настроек Dr.Web Сканера. Вкладка Типы файлов.

Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Типы файлов** задаются дополнительные ограничения на состав файлов, подлежащих сканированию в соответствии с заданием на сканирование.

В разделе **Режим проверки** выберите типы файлов, которые будут проверяться **Сканером**:

- Установленный по умолчанию вариант **Все файлы** предписывает проверку всех файлов в соответствии с заданием на сканирование. Данный вариант обеспечивает максимальную защиту.
- Варианты **Выбранные типы** и **Заданные маски** предписывают проверять только файлы, типы или расширения и имена которых соответственно входят в список, задаваемый в правой части вкладки. Данный список активируется при установке переключателя на соответствующем пункте.

По умолчанию список включает расширения основных типов файлов, которые могут быть носителями вирусов, и основных типов файловых архивов. Вы можете отредактировать этот список.

Формирование списка проверяемых файлов

1. Чтобы добавить элемент в список проверяемых файлов:

   а) Выберите один из следующих разделов и задайте соответствующие значения проверяемых элементов:

   - чтобы задать список расширений проверяемых файлов, выберите опцию **Выбранные типы** и укажите расширение файлов в поле ввода над списком;
   - чтобы задать проверяемые файлы определенного вида, выберите опцию **Заданные маски** и укажите маску, определяющую данные файлы, в поле ввода над списком.

   ▸ Подробнее о масках

   Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в именах файлов, а также специальные обозначения:

   - `*` заменяет любую (в том числе пустую) последовательность любых символов;
   - `?` заменяет один любой символ в заданной позиции.

   Примеры:

   - **отчет*.doc** – маска, задающая все документы Microsoft Word, название которых начинается с последовательности символов `отчет`, например, файлы `отчет-февраль.doc`, `отчет121209.doc` и т.д.;
   - ***.exe** – маска, задающая все исполняемые файлы с расширением `EXE`, например, `setup.exe`, `iTunes.exe` и т.д.;
   - **photo????09.jpg** – маска, задающая все файлы изображений формата `JPG`, название которых начинается с последовательности символов `photo` и

заканчивается последовательностью символов `09`, при этом между двумя этими последовательностями в названии файла стоит четыре произвольных символа, например, `photo121209.jpg`, `photomama09.jpg` или `photo----09.jpg`.

b) Нажмите кнопку **Добавить**.

c) При необходимости повторите шаги a) и b) для добавления других типов или масок файлов.

2. Чтобы удалить элемент из списка проверяемых файлов, выберите данный элемент в списке и нажмите кнопку **Удалить**.
3. Для восстановления списка, заданного по умолчанию, нажмите кнопку **Базовый**.

Также на данной вкладке задается режим проверки файловых архивов и почтовых файлов:

- Установите флаг **Файлы в архивах**, чтобы распаковывать архивы и проверять входящие в них файлы.

Включение этой проверки значительно увеличит нагрузку на компьютер.

- Установите флаг **Почтовые файлы**, чтобы проверять файлы почтовых клиентов, хранящих сообщения в текстовом виде. Если вы не пользуетесь такими почтовыми клиентами, снимите этот флаг.

Включение проверки почтовых файлов может сильно увеличить нагрузку на компьютер.

Для предотвращения проникновения вирусов с сообщениями электронной почты используйте почтовый сторож **SpIDer Mail**.

4.2.3.3. Вкладка Действия

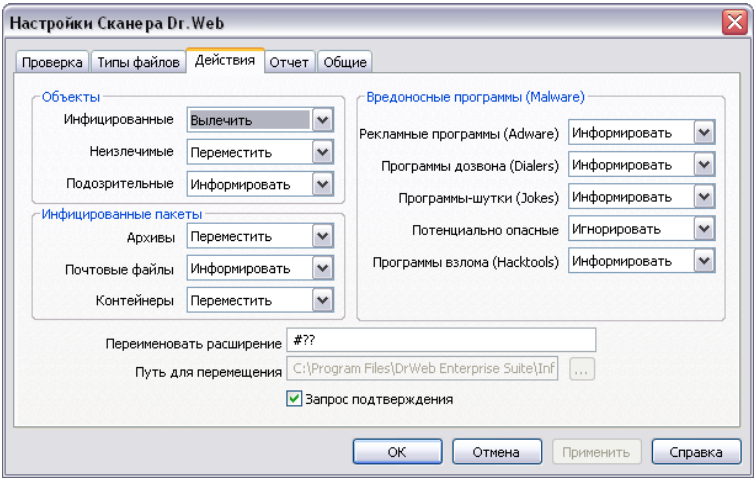

Рисунок 4-8. Окно настроек Dr.Web Сканера. Вкладка Действия. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Действия** задается реакция **Сканера** на обнаружение зараженных или подозрительных файлов, вредоносных программ, а также инфицированных архивов.

Реакция задается отдельно для каждой категории:

- **Объекты**:
  - зараженные известным и (предположительно) излечимым вирусом;
  - зараженные неизлечимым вирусом;
  - предположительно зараженные (подозрительные объекты).
- **Вредоносные программы**.
- **Инфицированные пакеты** (архивы, почтовые файлы, контейнеры).

По умолчанию **Сканер** только информирует пользователя в случае обнаружения известного вируса или при подозрении на зараженность объекта вирусом (см. также раздел Действия при обнаружении угроз). При этом сведения обо всех зараженных и подозрительных объектах выводятся в поле отчета, в котором вы можете в дальнейшем указать необходимые действия вручную.

Доступны следующие реакции над обнаруженными вредоносными объектами:

Действие	Описание
Вылечить	Предписывает **Сканеру** восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, будет применено действие, заданное для неизлечимых вирусов. Данное действие доступно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров). Троянские программы при обнаружении удаляются. Это единственное действие, доступное для зараженных загрузочных секторов.
Удалить	Предписывает **Сканеру** удалить объект. Для загрузочных секторов никаких действий производиться не будет.
Переименовать	Предписывает **Сканеру** изменить расширение файла объекта в соответствии с маской, задаваемой в поле **Переименовать расширение** (по умолчанию `#??`, т.е. заменить первый символ расширения на символ #). Для загрузочных секторов никаких действий производиться не будет.
Переместить	Предписывает **Сканеру** переместить объект в каталог **Карантина**, указанный в поле **Путь для перемещения** (по умолчанию, подкаталог `infected.!!!` каталога установки **Антивируса Dr.Web**).

Действие	Описание
	Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Предписывает **Сканеру** пропустить объект без выполнения каких-либо действий и не выводить информацию в окне отчета. Данное действие возможно только для вредоносных программ таких как: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

При обнаружении инфицированного объекта в архиве применяется реакция, заданная для архивов. Предписанное действие выполняется для всего архива целиком, а не только для инфицированного объекта.

Для успешного завершения лечения некоторых инфицированных файлов требуется перезагрузка операционной системы Windows.

Настройки запроса о перезагрузке задаются на **Сервере** администратором антивирусной сети и могут предписывать автоматическую перезагрузку, запрос пользователя или отказ от перезагрузки компьютера.

4.2.3.4. Вкладка Отчет

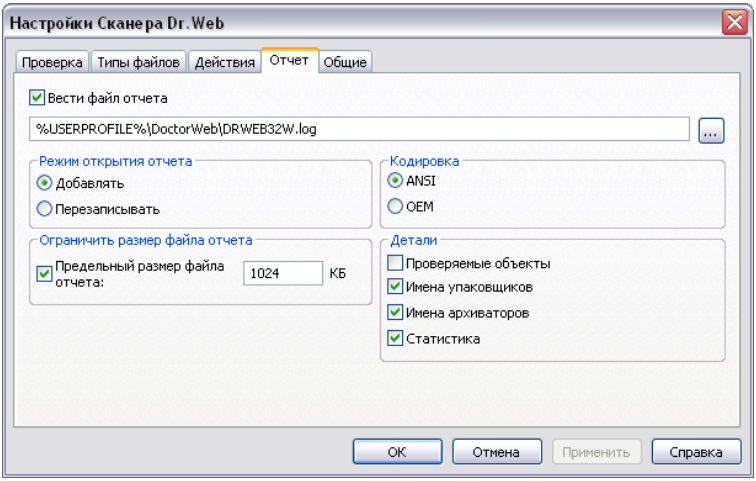

Рисунок 4-9. Окно настроек Dr.Web Сканера. Вкладка Отчет. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Отчет** задаются параметры ведения файла протокола работы **Сканера**.

Установите флаг **Вести файл отчета** для ведения файла отчета.

По умолчанию режим ведения отчета включен и файл отчета `DRWEB32W.log` размещается в каталоге `%USERPROFILE%\DoctorWeb`.

Вы можете настроить следующие параметры ведения файла отчета:

- В разделе **Режим открытия отчета** задается режим записи данных в отчет:
  - **Добавлять** – предписывает **Сканеру** добавлять новые записи в конец файла отчета;

- **Перезаписывать** – предписывает очищать файл отчета при каждом новом запуске **Сканера**.

◆ Установите флаг **Предельный размер файла отчета** для ограничения размера файла отчета. При этом отчет не превысит размера, указанного в поле **КБ**.

При превышении максимального размера файл отчета очищается, и информация в него начинает записываться с начала.

◆ В разделе **Кодировка** осуществляется выбор кодировки файла отчета:

- **ANSI** – использовать для отчета кодировку ANSI (Windows);
- **OEM** – использовать для отчета кодировку OEM (DOS).

◆ Раздел **Детали** позволяет выбрать дополнительную информацию, которая будет заноситься в файл отчета.

При предписанном ведении отчета в файл всегда, даже если больше ни один флаг не установлен, заносятся сообщения об обнаружении зараженных или подозрительных объектов, в том числе наименования вирусов или их модификаций (для подозрительных – классификация подозрительных кодов, принятая в эвристическом анализаторе), а также о предпринятых действиях.

Чтобы вносить в файл отчета расширенную информацию, установите следующие флаги:

- **Проверяемые объекты** - заносить имена всех проверенных объектов, причем для незараженных выводится также пометка **Ok** (этот режим может значительно увеличить файл отчета). Флаг по умолчанию снят.
- **Имена упаковщиков** - заносить сообщения об обнаружении исполняемых файлов, упакованных специальными упаковщиками, и имена этих упаковщиков. Флаг по умолчанию снят.

- **Имена архиваторов** - заносить сообщения о проверенных архивах и создавших их архиваторах, а также о связанных с ними ошибках (например, архив не удалось разархивировать, т.к. он защищен паролем). Флаг по умолчанию снят.
- **Статистика** - выводить статистическую информацию о работе программы во время очередного сканирования и всего сеанса работы **Сканера**.

4.2.3.5. Вкладка Общие

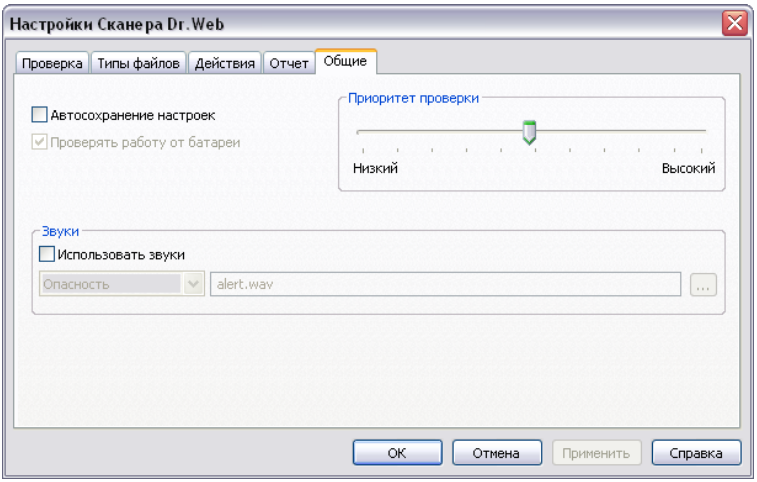

Рисунок 4-10. Окно настроек Dr.Web Сканера. Вкладка Общие. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Общие** задаются параметры взаимодействия программы с операционной системой, а также звуковые реакции программы на различные события.

- Флаг **Автосохранение настроек** предписывает программе сохранять измененные настройки при завершении работы **Сканера**. В противном случае изменения в настройках применяются только для текущего сеанса работы **Сканера** и будут сброшены в предыдущее сохраненное состояние при следующем запуске **Сканера**.

  Вы также можете явно указать необходимость сохранить настройки, выбрав опцию **Сохранить настройки** в меню **Настройки** главного окна **Сканера**.

- Флаг **Проверять работу от батареи** позволяет проверять перед началом сканирования, работает ли ноутбук от батареи. Опция доступна только для портативных компьютеров (ноутбуков).
- Бегунок **Приоритет проверки** позволяет изменить приоритет процесса сканирования в системе.
- В разделе **Звуки** вы можете настроить режим «озвучивания» работы или сопоставить событиям звуковые файлы. По умолчанию режим звуковых реакций на вирусные события выключен.
  - Установите флаг **Использовать звуки**, чтобы включить звуковое сопровождение работы **Сканера**.
  - Если хотите изменить заданное по умолчанию звуковое сопровождение работы **Сканера**, выберите в выпадающем списке необходимое событие и задайте звуковой файл в поле справа.

4.2.4. Сканирование в режиме командной строки

Вы можете запускать **Сканер** в режиме командной строки. Такой способ позволяет задать настройки текущего сеанса сканирования и перечень сканируемых объектов в качестве параметров вызова. Именно в таком режиме возможен автоматический вызов **Сканера** по расписанию.

Синтаксис команды запуска следующий:

```
[<путь_к_программе>]drweb32w [<объекты>] [<ключи>]
```

Список объектов сканирования может быть пуст или содержать несколько элементов, разделенных пробелами.

Наиболее распространены следующие варианты задания объектов сканирования:

- `*` – сканировать все жесткие диски;
- `C:` – сканировать диск `C`;
- `D:\games` – сканировать файлы в каталоге;
- `C:\games\*` – сканировать все файлы и подкаталоги каталога `C:\games`.

Параметры – ключи командной строки, которые задают настройки программы. При их отсутствии сканирование выполняется с ранее сохраненными настройками (или настройками по умолчанию, если вы не меняли их).

Каждый параметр этого типа начинается с символа `/`, ключи разделяются пробелами.

Ниже приведено несколько наиболее часто используемых ключей. Полный их список приведен в Приложении А.

- `/cu` – лечить инфицированные объекты;
- `/icm` – перемещать неизлечимые файлы (в каталог по умолчанию);
- `/icr` – переименовывать (по умолчанию);
- `/qu` – закрыть окно **Сканера** по окончании сеанса;
- `/go` – не выдавать никаких запросов.

Последние два параметра особенно полезны при автоматическом запуске **Сканера** (например, по расписанию).

С такими же параметрами может использоваться **Dr.Web Консольный сканер для Windows DrWebWcl**. В этом случае вместо `drweb32w` необходимо набрать имя команды `drwebwcl`.

Консольный сканер DrWebWcl по умолчанию использует те же настройки, что и GUI-версия **Сканера**. Параметры, заданные средствами графического интерфейса **Сканера** (см. п. Настройка параметров программы), используются также при сканировании в режиме командной строки, если иные значения параметров не были заданы в виде ключей.

4.2.5. Консольный сканер

Также в состав компонентов **Антивируса Dr.Web** входит **Консольный сканер DWScancl**. В отличие от **Консольного сканера DrWebWcl**, он предоставляет пользователю расширенные возможности настройки (большее количество параметров) и рассчитан на многопроцессорные системы.

Файлы, подозрительные на наличие вредоносных объектов, **Консольный сканер DWScancl** помещает не в каталог `infected.!!!`, а в **Карантин**.

Чтобы запустить **Консольный сканер DWScancl**, воспользуйтесь следующей командой:

[*<путь_к_программе>*]`dwscancl` [*<ключи>*] [*<объекты>*]

Ключ начинается с символа `/`, несколько ключей разделяются пробелами. Список объектов сканирования может быть пуст или содержать несколько элементов, разделенных пробелами.

Список ключей **Консольного сканера DWScancl** приведен в Приложении А.

Коды возврата:

0 – сканирование успешно завершено, инфицированные объекты не найдены.

1 – сканирование успешно завершено, найдены инфицированные объекты.

10 – указаны некорректные ключи.

11 – ключевой файл не найден либо не поддерживает **Консольный сканер DWScancl**.

12 – не запущен **Scanning Engine**.

255 – сканирование прервано пользователем.

Глава 5. Карантин

Для просмотра и редактирования содержимого **Карантина** выберите в контекстном меню **Агента** пункт **Карантин**. Откроется окно, содержащее табличные данные о текущем состоянии **Карантина**.

Карантин антивируса **Dr.Web** служит для изоляции файлов, подозрительных на наличие вредоносного ПО.

Каталоги **Карантина** создаются отдельно на каждом логическом диске, где были обнаружены подозрительные файлы. Каталог **Карантина** под названием `DrWeb Quarantine` создается в корне диска и является скрытой. Пользователь не имеет прав доступа к файлам каталога **Карантина**.

При обнаружении зараженных объектов на съемном носителе, если запись на носителе возможна, на нём создается каталог `DrWeb Quarantine` и в неё переносится зараженный объект.

Файлы **Карантина**, размещаемые на жестком диске, хранятся в зашифрованном виде.

Файлы **Карантина**, размещаемые на съемном носителе, хранятся в незашифрованном виде.

Необходимо, чтобы станции с установленным модулем **Карантина** работали под ОС, на которые возможна установка **SpIDer Guard G3** (см. п. Системные требования).

В противном случае **Карантин** не сможет управлять файлами из каталога `Infected.!!!` (расположена в каталоге установки **Антивируса**), и информация о содержимом **Карантина** не будет отправляться на **Сервер**.

Информация о зараженных объектах, перенесенных в каталог **Карантина** на съемном носителе, доступна только в локальном карантине на станции (при условии, что съемный носитель подключен к компьютеру) и не доступна для удаленного управления с **Сервера**.

5.1. Настройка интерфейса

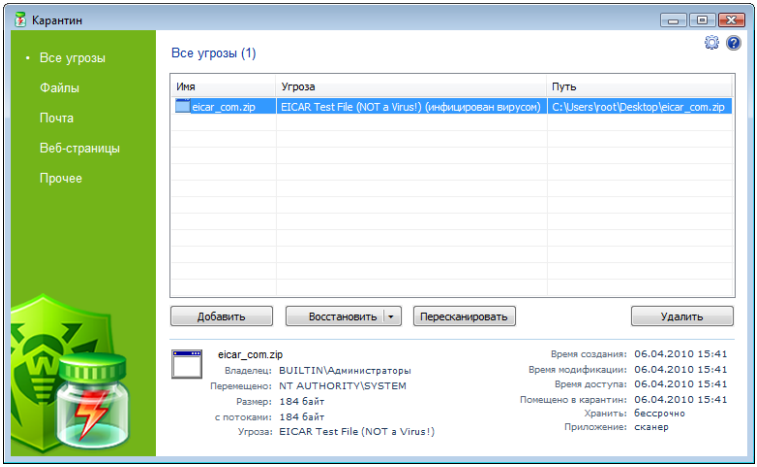

Рисунок 5-1. Окно карантина

В центральной части окна отображается таблица объектов с информацией о состоянии карантина. По умолчанию отображаются следующие столбцы:

- **Имя** – список имен объектов, находящихся в карантине,
- **Угроза** – классификация вредоносной программы, определяемая **Антивирусом** при автоматическом перемещении объекта в карантин,
- **Путь** – полный путь, по которому находился объект до перемещения в **Карантин**.

Также возможно включить отображение столбцов с подробной информацией об объекте, аналогичной данным в нижней части окна **Карантина**.

Чтобы настроить отображение столбцов:

1. Вызовите контекстное меню заголовка таблицы объектов. Для этого нажмите правой кнопки мыши по заголовку.
2. В контекстном меню выберите **Настроить колонки**.
3. В открывшемся окне установите флаги напротив тех пунктов, которые вы хотите включить в таблицу объектов. Для того, чтобы исключить столбцы из таблицы объектов, снимите флаги напротив соответствующих пунктов.
    a) Для установления флагов напротив всех объектов сразу нажмите кнопку **Отметить все**.
    b) Для снятия всех флагов нажмите кнопку **Снять отметки**.
4. Для изменения порядка следования столбцов в таблице выберите соответствующий столбец в списке и нажмите на одну из следующих кнопок:
    a) **Вверх** – для перемещения столбца ближе к началу таблицы (вверх по списку в настройках и левее в таблице объектов).
    b) **Вниз** – для перемещения столбца ближе к концу таблицы (вниз по списку в настройках и правее в таблице объектов).
5. Для сохранения изменений в настройках нажмите кнопку **ОК**, для закрытия окна без сохранения изменений - кнопку **Отменить**.

В нижней части окна **Карантина** отображается подробная информация о выбранных объектах **Карантина**.

5.2. Настройка свойств Карантина

Для настройки свойств Карантина:

1. Нажмите на кнопку  **Настройки** в окне **Карантина**.
2. Откроется окно **Свойства карантина**, в котором вы можете изменять следующие параметры:
   - Раздел **Задать размер карантина** позволяет управлять объемом дискового пространства, занимаемого каталогом **Карантина**. Передвиньте ползунок для изменения максимально допустимого размера **Карантина**, который определяется в процентном соотношении относительно общего размера диска (при наличии нескольких логических дисков, данный размер будет рассчитан отдельно для каждого диска, на котором располагаются каталоги **Карантина**). Значение `100%` означает снятие ограничений для максимального размера каталога **Карантина**.
   - В разделе **Вид** установите флаг **Показывать резервные копии**, чтобы отобразить в таблице объектов резервные копии файлов, находящихся в **Карантине**.
3. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

Резервные копии создаются автоматически при перемещении файлов в **Карантин**. Даже при хранении файлов в **Карантине** **бессрочно**, их резервные копии сохраняются **временно** (см. также раздел Очистка Карантина).

Для отображения справки нажмите на кнопку  .

5.3. Управление содержимым Карантина

Боковая панель слева служит для фильтрации объектов **Карантина**, которые будут отображены. При нажатии на соответствующий пункт, в центральной части окна будут показаны все объекты **Карантина** или только заданные группы объектов: файлы, почтовые объекты, веб-страницы или все остальные объекты, не попадающие в данные категории.

В окне **Карантина** пользователи могут видеть только те файлы, к которым имеют права доступа.

Чтобы отобразить скрытые объекты, запустите под учетной записью с административными правами либо файл **Карантина** `dwqrui.exe`, расположенный в каталоге установки, либо интерфейс **Dr.Web Агента** (см. п. Запуск и останов интерфейса Dr.Web Агента).

В окне **Карантина** доступны следующие кнопки управления:

- **Добавить** – добавить файл в **Карантин**. В открывшемся браузере по операционной системе выберите нужный файл.
- **Восстановить** – переместить файл из **Карантина** и восстановить первоначальное местоположение файла на компьютере (восстановить файл под тем же именем в каталог, в котором он находился до перемещения в **Карантин**).

Используйте данную функцию только если вы уверены, что объект безопасен.

В выпадающем меню доступен вариант **Восстановить в** – переместить файл под заданным именем в каталог, указанный пользователем.

- **Пересканировать** – сканировать файл из **Карантина** повторно. Если при повторном сканировании файла

обнаружится, что он не является зараженным, **Карантин** предложит восстановить данный файл.

- **Удалить** – удалить файл из **Карантина** и из системы.

Для работы одновременно с несколькими объектами выберите необходимые объекты в окне **Карантина**, удерживая клавиши SHIFT или CTRL, затем щелкните правой кнопкой мыши на любой строчке таблицы и в выпадающем меню выберите необходимое действие.

5.4. Очистка Карантина

Автоматическая очистка Карантина

При переполнении диска осуществляется автоматическая очистка Карантина:

1. В первую очередь удаляются резервные копии файлов **Карантина**.
2. При нехватке дискового пространства удаляются файлы **Карантина** с истекшим сроком хранения.

При переполнении **Карантина** и невозможности его автоматической очистки, перемещение файлов в **Карантин** будет завершаться с ошибкой. В этом случае вы можете увеличить размер **Карантина** в разделе **Свойства карантина** → **Задать размер карантина** или удалить файлы **Карантина** вручную.

Полная очистка Карантина

Удаление всего содержимого Карантина возможно следующими способами:

1. Откройте менеджер **Карантина** через контекстное меню **Агента**, пункт **Карантин**. Выделите все файлы в окне **Карантина** и нажмите кнопку **Удалить**.

2. Воспользуйтесь системной функцией **Disk Cleanup** для очистки диска.

   a) Запустить данную функцию можно следующими способами:

   - Для ОС младше Windows Vista:
     - меню **Пуск** → **Программы** → **Стандартные** → **Служебные** → **Очистка диска**.
     - Через файловый браузер по ОС: в контекстном меню диска, на котором вы хотите очистить **Карантин**, выберите **Свойства** → **Очистка диска**.
   - Для ОС Windows Vista и Windows 7: меню **Пуск** → **Программы** → **Стандартные** → **Служебные** → **Очистка диска**.
   - Для ОС Windows 8: меню **Приложения** (открывается через пункт Все приложения на панели приложений стартового экрана) → раздел **Администрирование** → пункт **Очистка диска**.

     При наличии нескольких логических дисков выберите диск, на котором вы хотите очистить **Карантин**.

   b) В открывшемся окне **Очистка Диска** в списке **Удалить следующие файлы** установите флаг напротив пункта **Карантин Dr.Web** и нажмите **ОК**. Содержимое **Карантина** будет удалено.

Глава 6. Dr.Web Firewall

Сетевой экран **Dr.Web Firewall** предназначен для защиты вашего компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети. Этот компонент позволяет вам контролировать подключение и передачу данных по сети Интернет и блокировать подозрительные соединения на уровне пакетов и приложений.

После установки **Dr.Web Firewall** некоторое время в процессе вашей работы за компьютером производится обучение программы. Описание процесса обучения Сетевого экрана приведено в Руководстве **Антивирус Dr.Web для Windows**, в разделе **Обучение Dr.Web Firewall**.

Для перехода на Справку **Антивирус Dr.Web для Windows** нажмите клавишу F1 в любом окне Сетевого экрана.

При помощи контекстного меню **Агента** вы можете:

1. Вызывать Настройки Dr.Web Firewall.
2. Просматривать Журнал Dr.Web Firewall.

6.1. Настройки Dr.Web Firewall

Для просмотра и изменения параметров Сетевого экрана **Dr.Web Firewall** выберите в контекстном меню **Агента** пункт **Настройки Firewall**.

Пункт **Настройки Firewall** доступен в контекстном меню **Агента** только при наличии у пользователя прав администратора на данном компьютере.

Откроется окно настроек **Dr.Web Firewall**. Подробное описание управления компонентом **Dr.Web Firewall** приведено в Руководстве **Антивирус Dr.Web для Windows**, в разделе

Настройки Брандмауэра.

Для перехода на Справку **Антивирус Dr.Web для Windows** нажмите клавишу F1 в любом окне **Сетевого экрана**.

6.2. Журнал Dr.Web Firewall

Для просмотра журнала Сетевого экрана **Dr.Web Firewall** выберите в контекстном меню **Агента** пункт **Журнал Firewall**.

Пункт **Журнал Firewall** доступен в контекстном меню **Агента** только при наличии у пользователя прав администратора на данном компьютере.

Откроется окно журнала **Dr.Web Firewall**. Подробное описание журнала **Dr.Web Firewall** приведено в Руководстве **Антивирус Dr.Web для Windows**, в разделе **Регистрация событий**.

Для перехода на Справку **Антивирус Dr.Web для Windows** нажмите клавишу F1 в любом окне Сетевого экрана.

Глава 7. Офисный Контроль

Модуль **Офисного контроля Dr.Web** обеспечивает ограничение доступа пользователей к определенным локальным ресурсам и веб-сайтам. Это позволяет не только контролировать целостность важных файлов и защищать их от заражения вирусами, но также сохранить необходимую конфиденциальность данных на вашем компьютере.

Существует возможность защиты как отдельных файлов, так и папок полностью, расположенных как на локальных дисках, так и на внешних носителях информации (пока они подключены к данному компьютеру). Также можно наложить полный запрет на просмотр информации со всех внешних носителей.

Контроль доступа к интернет-ресурсам позволяет как оградить пользователя от просмотров нежелательных веб-сайтов (сайтов, посвященных насилию, азартным играм и т.п.), так и разрешить пользователю доступ только к тем сайтам, которые определены настройками модуля **Офисного контроля**.

По умолчанию монитор блокирует доступ к каталогам антивируса **Dr.Web**. Чтобы задать параметры работы модуля, воспользуйтесь настройками параметров модуля.

В зависимости от установок на **Сервере** вы можете настраивать модуль **Офисного контроля**.

При возможности самостоятельного ограничения доступа к ресурсам со стороны пользователя, сохраняется возможность задания настроек на **Сервере** администратором. Настройки, указанные на **Сервере**, будут автоматически обновляться на стороне пользователя.

Для того чтобы изменить настройки модуля:

1. Выберите в контекстном меню **Агента** пункт **Настройки Офисного контроля**.

Пункт **Настройки Офисного контроля** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

2. Введите пароль доступа к модулю **Офисного контроля**.

Защита от редактирования списка ресурсов осуществляется с помощью пароля, который задается при первичной настройке модуля **Офисного контроля.** Вы можете изменить пароль в окне настроек модуля или обратиться для этого к администратору.

Для того чтобы изменить пароль, нажмите кнопку **Сменить пароль**, расположенную в окне настроек.

3. Для того чтобы получить информацию о настройках, расположенных на вкладке, нажмите кнопку  **(Справка).**
4. Внесите необходимые изменения на вкладках настроек:
   - **Фильтр URL** (подробное описание приведено в Справке **Антивирус Dr.Web для Windows**, **Раздел Фильтр URL**).
   - **Локальный доступ** (подробное описание приведено в Справке **Антивирус Dr.Web для Windows**, **Раздел Локальный доступ**).

   Для перехода на Справку **Антивирус Dr.Web для Windows** нажмите клавишу F1 в любом окне **Офисного Контроля**.
5. Нажмите кнопку **Применить** для сохранения внесенных изменений без закрытия окна настроек.

6. По окончанию редактирования настроек нажмите кнопку **ОК** для сохранения всех внесенных изменений или кнопку **Отмена** - для отказа от них с последующим закрытием окна настроек.

Глава 8. SpIDer Gate

HTTP-монитор **SpIDer Gate** помогает защитить ваш компьютер от вредоносных программ, которые могут распространяться при сетевом взаимодействии по протоколу HTTP. Через HTTP работают веб-браузеры (интернет-браузеры), различные менеджеры загрузки и многие другие программы, получающие данные из сети Интернет. Такие программы также называются HTTP-клиентами.

SpIDer Gate по умолчанию включается в состав устанавливаемых компонентов, постоянно находится в памяти и автоматически перезапускается при загрузке ОС Windows.

С помощью изменения настроек **SpIDer Gate** вы можете отключить проверку исходящего или входящего трафика, а также сформировать список тех приложений, HTTP-трафик (информация, передаваемая по протоколу HTTP) которых будет проверяться в любом случае и в полном объеме. Также существует возможность исключения из проверки трафика отдельных приложений.

Изменение параметров проверки HTTP-монитора **SpIDer Gate** может быть разрешено или заблокировано администратором **Dr.Web Enterprise Security Suite**. Для просмотра и изменения параметров монитора **SpIDer Gate** выберите в контекстном меню **Агента** пункт **Настройки SpIDer Gate**.

Пункт **Настройки SpIDer Gate** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

По умолчанию монитор проверяет весь HTTP-трафик. Чтобы задать параметры проверки, воспользуйтесь настройками параметров модуля.

Подробное описание управления сторожем **SpIDer Gate** приведено в Руководстве **Антивирус Dr.Web для Windows**, в разделе **Настройка SpIDer Gate**.

Для перехода на Справку **Антивирус Dr.Web для Windows** нажмите клавишу F1 в любом окне сторожа.

Глава 9. SpIDer Guard

SpIDer Guard – антивирусный сторож (называемый также файловым монитором). Программа постоянно находится в оперативной памяти, осуществляя проверку файлов "на лету", а также обнаруживает проявления вирусной активности.

SpIDer Guard запускается автоматически при каждой загрузке операционной системы, при этом запущенный сторож не может быть выгружен в течение текущего сеанса работы операционной системы. При необходимости (например, в случае выполнения критически чувствительного к загрузке процессора задания в реальном масштабе времени) вы можете временно отключить сканирование файлов "на лету".

При настройках по умолчанию сторож **SpIDer Guard** "на лету" проверяет все создаваемые или изменяемые файлы и загрузочные секторы, а на сменных носителях и сетевых дисках – также все открываемые файлы. Сканирование проводится аналогично тому, как работает **Сканер Dr.Web**, однако с более "мягкими" условиями проверки. Кроме того, сторож **SpIDer Guard** постоянно отслеживает действия запущенных процессов, характерные для вирусов, и при обнаружении угроз безопасности – блокирует соответствующие процессы.

При обнаружении зараженных объектов сторож **SpIDer Guard** применяет к ним действия согласно установленным настройкам. Соответствующими настройками вы можете изменить автоматическую реакцию сторожа на вирусные события.

Настройка сторожа

Раздел настроек сторожа **SpIDer Guard** различается в зависимости от установленной версии сторожа. Существуют две версии сторожа **SpIDer Guard**:

- SpIDer Guard G3,
- SpIDer Guard NT4.

Перед установкой сторожа автоматически определяется версия операционной системы и устанавливается соответствующая версия **SpIDer Guard** (см. п. Системные требования).

9.1. Настройки SpIDer Guard G3

Настройки программы по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.

При необходимости настройки файлового монитора SpIDer Guard:

1. В контекстном меню **Агента** выберите пункт **Настройки SpIDer Guard**.

Пункт **Настройки SpIDer Guard** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

2. Откроется окно настроек, содержащее следующие разделы:
   - раздел Общие, в котором задается режим проверки файлов и процессов защищаемого компьютера;
   - раздел Действия, в котором задается реакция сторожа **SpIDer Guard** на обнаружение зараженных или подозрительных файлов и вредоносных программ;
   - раздел Исключения, в котором задается список каталогов и файлов, исключаемых из проверки сторожем **SpIDer Guard**;
   - раздел Отчет, в котором задается режим ведения файла отчета сторожа **SpIDer Guard**.
3. Внесите необходимые изменения.

4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от изменений.

Для получения справки об активном окне настроек **SpIDer Guard** нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

9.1.1. Раздел Общие

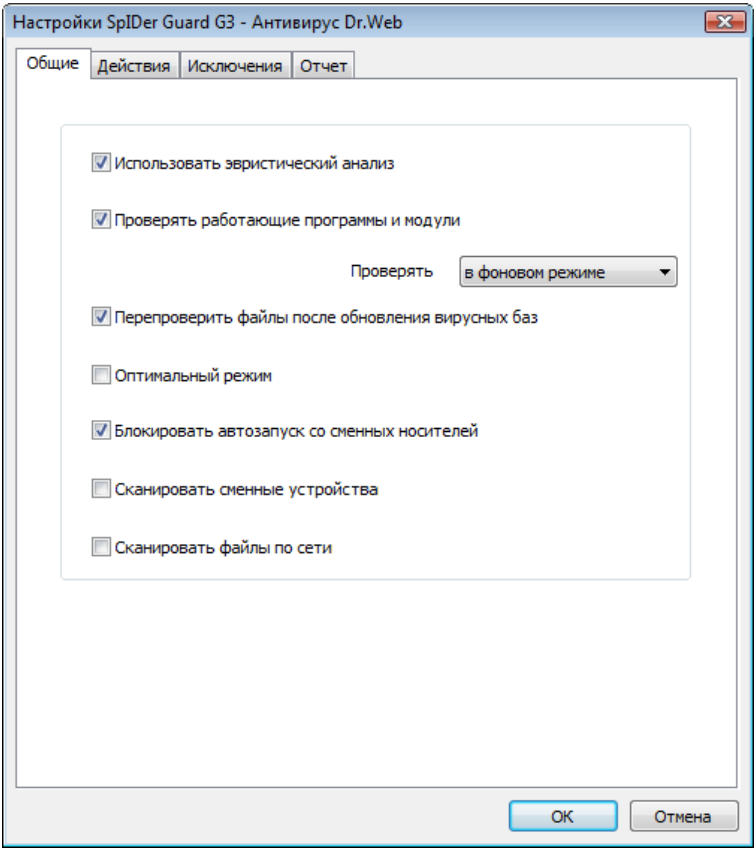

Рисунок 9-1. Окно настроек SpIDer Guard. Вкладка Общие. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Общие** задается режим проверки файлов и процессов защищаемого компьютера:

- Установите флаг **Использовать эвристический анализ**, чтобы использовать при проверке эвристический анализатор.

  Снимите этот флаг, чтобы проводить проверку только по сигнатурам известных вирусов (см. также раздел Методы обнаружения вирусов).

- Опция **Проверять работающие программы и модули** предписывает проверять файлы программ, работающих в данный период времени. Для задания режима проверки файлов запускаемых процессов в выпадающем списке выберите один из следующих вариантов:
  - **в фоновом режиме** - предписывает проверку модулей в фоновом режиме, т.е. после их запуска, в процессе выполнения.
  - **при запуске программы** - предписывает проверку модулей перед их запуском.
- При установке флага **Перепроверить файлы после обновления вирусных баз** осуществляется повторная проверку всех активных загруженных в данный момент модулей и инфицированных файлов сразу после обновления вирусных баз. Если данный флаг снят, то после обновления вирусных баз будут перепроверены только инфицированные файлы.
- Флаг **Оптимальный режим** задает режим проверки, определяющий при каких действиях с объектом должна производиться его проверка сторожем **SpIDer Guard**:
  - Если флаг **Оптимальный** установлен, сканирование файлов на жестких дисках производится только при некоторых обращениях к этим файлам: при запуске на исполнение, при создании, при записи (попытке записи) в существующие файлы или загрузочные сектора.

- Если флаг **Оптимальный** не установлен, сканирование файлов на жестких дисках производится при любом обращении к этим файлам: при запуске на исполнение, при создании, при записи (попытке записи) в существующие файлы или загрузочные сектора, а также при любом открытии файлов, в том числе только для чтения.

Отключение **Оптимального** режима обеспечивает максимальный уровень защиты, но значительно увеличивает нагрузку на компьютер.

Режимы проверки файлов на сменных носителях и на сетевых дисках настраиваются отдельно при помощи флагов **Сканировать сменные устройства** и **Сканировать файлы по сети**.

▸ Уточнения и рекомендации

Установку **Оптимального** режима рекомендуется производить после тщательной проверки всех жестких дисков при помощи **Сканера Dr.Web**. При этом будет исключено проникновение на компьютер новых вирусов или других вредоносных программ через сменные устройства, но при этом не будет проводиться повторного сканирования уже проверенных, «чистых», объектов.

Реакция сторожа **SpIDer Guard** на обнаружение вредоносных объектов задается в разделе Действия.

Некоторые внешние накопители (в частности, мобильные жесткие диски с интерфейсом USB) могут представляться в системе как жесткие диски. Поэтому такие устройства следует использовать с особой осторожностью и проверять на вирусы при подключении к компьютеру с помощью **Сканера Dr.Web**.

◆ Флаг **Блокировать автозапуск со сменных носителей** запрещает автоматический запуск программ с внешних носителей информации. Это позволит оградить ваш компьютер от запуска вредоносных программ, которые могут

находиться на внешних носителях информации.

- Установите флаг **Сканировать сменные устройства**, чтобы сканировать файлы на сменных носителях информации (CD/DVD диски, магнитные диски (FDD), flash-накопители и прочие носители информации, подключаемые через USB-порт и т.п.) при любом обращении к ним, в том числе при открытии файлов только для чтения.

  Если флаг **Сканировать сменные устройства** снят, то сканирование файлов на сменных носителях будет производиться только при запуске этих файлов на исполнение.

- Установите флаг **Сканировать файлы по сети**, чтобы проверять объекты на сетевых дисках при запуске этих файлов на исполнение на вашем компьютере и при любом открытии файлов, в том числе файлов только для чтения.

  Если флаг **Сканировать файлы по сети** снят, то сканирование файлов на сетевых дисках будет производиться только при запуске этих файлов на исполнение на вашем компьютере.

9.1.2. Раздел Действия

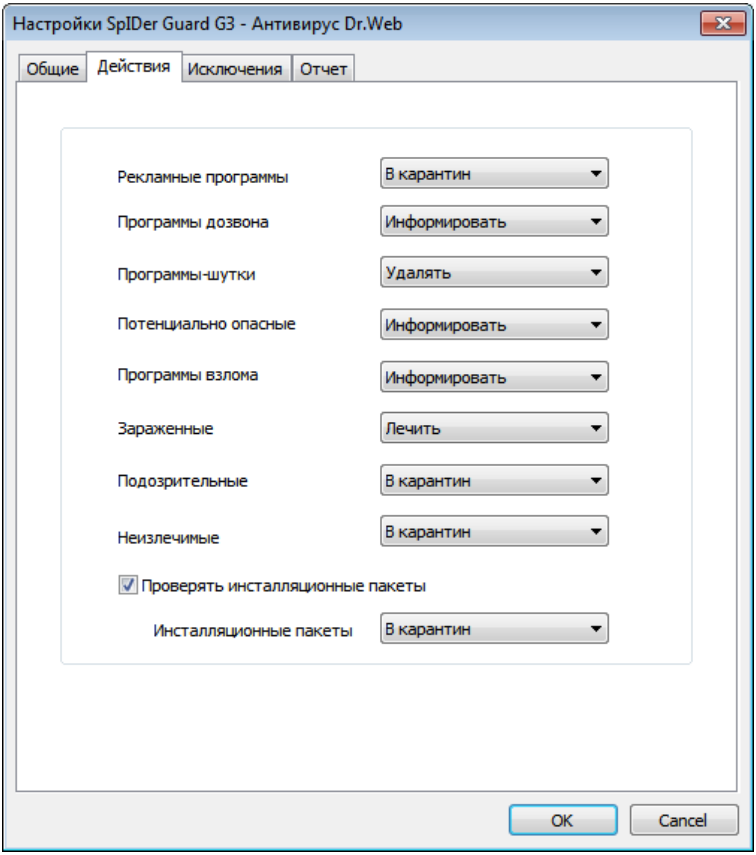

Рисунок 9-2. Окно настроек SpIDer Guard. Вкладка Действия. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Действия** задается реакция сторожа **SpIDer Guard** на обнаружение зараженных или подозрительных файлов и вредоносных программ. Состав доступных реакций при этом зависит от типа вирусного события.

Предусмотрены следующие действия над обнаруженными объектами:

- **Лечить** - восстановить состояние инфицированного объекта до заражения. При невозможности лечения применяется настройка, заданная для неизлечимых объектов.

  Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).

- **Удалять** - удалить зараженные объекты.
- **В карантин** - переместить зараженные объекты в каталог Карантина.
- **Информировать** - ограничиться оповещением об обнаружении вируса (о настройке режима оповещений см. ниже).
- **Игнорировать** - пропустить объект без выполнения каких-либо действий и не выводить оповещения.

При задании действия **Игнорировать** не будет произведено никаких действий: пользователю не будет выдано предупреждение, как в случае включенной опции **Информировать** при обнаружении вредоносного объекта.

Таблица 3. Действия SpIDer Guard над обнаруженными вредоносными объектами

Объект	Действие				
	Лечить	Удалять	В карантин	Информировать	Игнорировать
Рекламные программы		+	+/*	+	+
Программы дозвона		+	+	+/*	+
Программы-шутки		+/*	+	+	+

Объект	Действие				
	Лечить	Удалять	В карантин	Информи-ровать	Игнори-ровать
Потенциально опасные		+	+	+/*	+
Программы взлома		+	+	+/*	+
Зараженные	+/*	+	+		
Подозри-тельные		+	+/*	+	+
Неизлечимые		+	+/*		
Инсталляци-онные пакеты		+	+/*	+	+

Условные обозначения

+	действие разрешено для данного типов объектов
+/*	действие установлено как реакция по умолчанию для данного типов объектов

Для задания действий над обнаруженными вредоносными объектами служат следующие настройки:

- Выпадающий список **Рекламные программы** задает реакцию **SpIDer Guard** на обнаружение данной разновидности нежелательного ПО.
- Аналогично действиям над рекламными программами, настраивается реакция **SpIDer Guard** при обнаружении прочего нежелательного ПО, такого как:
  - программы дозвона;
  - программы-шутки;
  - потенциально опасные;
  - программы взлома.
- Выпадающий список **Зараженные** задает реакцию **SpIDer Guard** на обнаружение файла, зараженного известным вирусом.
- Выпадающий список **Подозрительные** задает реакцию

SpIDer Guard на обнаружение файла, предположительно зараженного вирусом (срабатывание эвристического анализатора).

- Выпадающий список **Неизлечимые** задает реакцию **SpIDer Guard** на обнаружение файла, зараженного известным неизлечимым вирусом (а также когда предпринятая попытка излечения не принесла успеха).
- Опция **Проверять инсталляционные пакеты** задает проверку «на лету» установочных файлов.

  При задании данной опции, в выпадающем списке **Инсталляционные пакеты** выберите действие, которое будет выполняться при обнаружении вредоносных объектов в инсталляционных пакетах.

Настройка уведомлений

После выполнения предписанного действия сторож **SpIDer Guard** по умолчанию выводит соответствующее оповещение в область уведомлений ОС Windows. Вы можете запретить или разрешить вывод уведомлений.

Для настройки уведомлений сторожа **SpIDer Guard**, в контекстном меню значка **Агента** в выпадающем списке **Настройки** установите или снимите флаг **Оповещения о вирусах** для получения или отказа от вывода сообщений соответственно.

9.1.3. Раздел Исключения

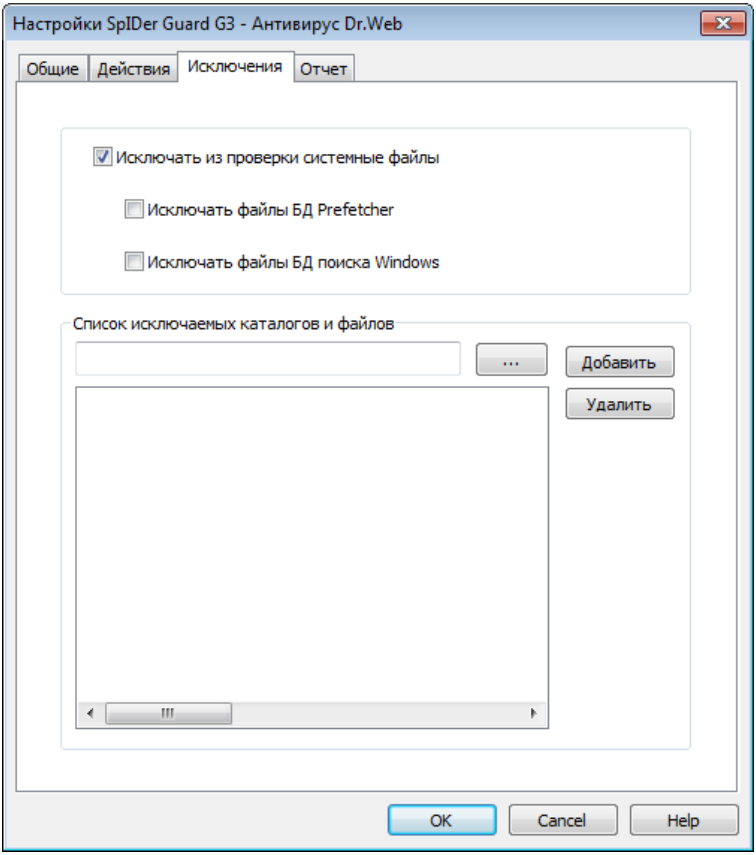

Рисунок 9-3. Окно настроек SpIDer Guard. Вкладка Исключения. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Исключения** задается список каталогов и файлов, исключаемых из проверки сторожем **SpIDer Guard**.

Флаг **Исключать из проверки системные файлы** предписывает исключать из проверки системные файлы, входящие во внутренний список компонента **SpIDer Guard**. Данный список составляется для каждой версии ОС Windows на основе рекомендаций от компании Microsoft® по использованию антивирусных программ.

При установке флага **Исключать из проверки системные файлы** станут доступны следующие настройки:

- Флаг **Исключать файлы БД Prefetcher** предписывает исключение из проверки файлов базы данных системного компонента Prefetcher (компонент операционной системы Microsoft Windows, ускоряющий процесс ее начальной загрузки, а также сокращающий время запуска программ за счет сохранения информации, используемой при запуске).
- Флаг **Исключать файлы БД windows поиска** предписывает исключение из проверки файлов базы данных службы поиска ОС Windows.

В разделе **Список исключаемых каталогов и файлов** приводится список каталогов и файлов, которые не проверяются сторожем **SpIDer Guard**. В таком качестве могут выступать каталоги **Карантина** антивируса, рабочие каталоги некоторых программ, временные файлы (файлы подкачки) и т.п.

По умолчанию список пуст. Вы можете добавить к исключениям конкретные каталоги и файлы или использовать маски, чтобы запретить проверку определенной группы объектов.

Формирование списков исключений

1. Чтобы добавить каталог или файл к списку исключений, выполните одно из следующих действий:
   - чтобы указать конкретный существующий каталог или файл, нажмите кнопку  и выберите каталог или файл в стандартном браузере по операционной системе. Вы также можете вручную ввести полный путь к файлу или каталогу в поле ввода;

- чтобы исключить из проверки все файлы или каталоги с определенным именем, введите это имя в поле ввода. Указывать путь к каталогу или файлу при этом не требуется;
- чтобы исключить из проверки файлы или каталоги определенного вида, введите определяющую их маску в поле ввода.

▸ Подробнее о масках

Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в именах файлов, а также специальные обозначения:

- `*` заменяет любую (в том числе пустую) последовательность любых символов;
- `?` заменяет один любой символ в заданной позиции.

Примеры:

- **отчет*.doc** – маска, задающая все документы Microsoft Word, название которых начинается с последовательности символов `отчет`, например, файлы `отчет-февраль.doc`, `отчет121209.doc` и т.д.;
- ***.exe** – маска, задающая все исполняемые файлы с расширением `EXE`, например, `setup.exe`, `iTunes.exe` и т.д.;
- **photo????09.jpg** – маска, задающая все файлы изображений формата `JPG`, название которых начинается с последовательности символов `photo` и заканчивается последовательностью символов `09`, при этом между двумя этими последовательностями в названии файла стоит четыре произвольных символа, например, `photo121209.jpg`, `photomama09.jpg` или `photo----09.jpg`.

2. Нажмите кнопку **Добавить**.
3. При необходимости повторите шаги 1 и 2 для добавления других файлов или каталогов.
4. Чтобы удалить файл или каталог из списка исключений, выберите соответствующий элемент в списке и нажмите кнопку **Удалить**.

9.1.4. Раздел Отчет

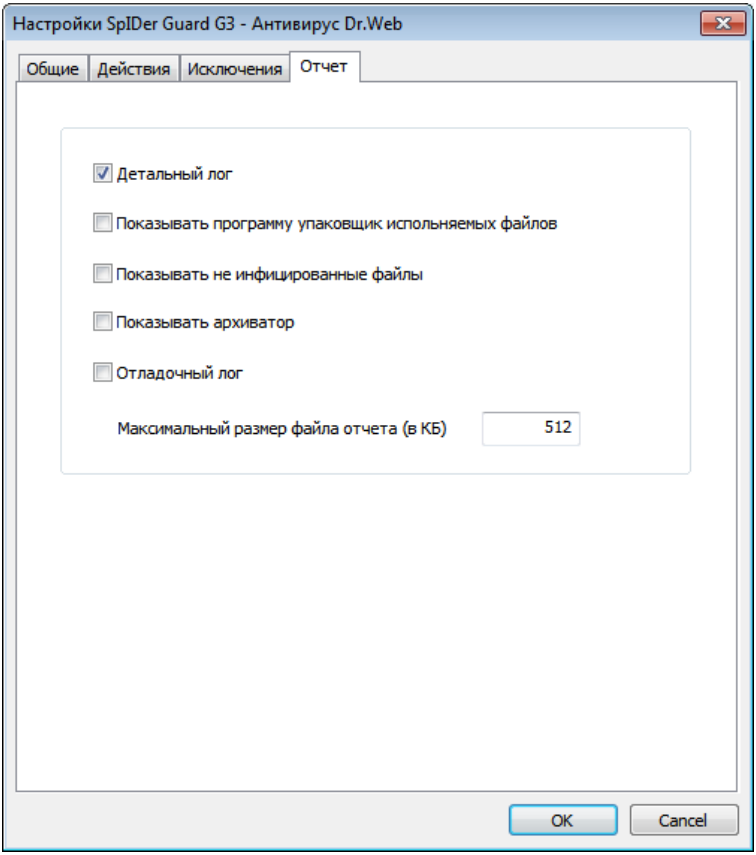

Рисунок 9-4. Окно настроек SpIDer Guard. Вкладка Отчет. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Отчет** задается режим ведения файла отчета и указывается информация, которая будет заноситься в файл отчета.

Отчет сторожа **SpIDer Guard** хранится в файле `spiderg3.log`, расположенном в каталоге установки **Enterprise Security Suite**.

Рекомендуется периодически анализировать файл отчета.

Для детализации отчета установите флаги режимов ведения отчета и типов информации, заносимой в отчет.

Для задания режимов ведения отчета служат следующие флаги:

- **Детальный лог** – в данном режиме в отчете помимо общих событий фиксируются подробные данные о проверяемых объектах. Рекомендуется использовать этот режим для определения объектов, которые сторож **SpIDer Guard** проверяет наиболее часто. При необходимости вы можете добавить такие объекты в список исключений, что может снизить нагрузку на компьютер;
- **Отладочный лог** – в данном режиме в отчете фиксируется максимальное количество информации о работе сторожа **SpIDer Guard**, что может привести к значительному увеличению файла отчета. Рекомендуется использовать этот режим только при возникновении проблем в работе сторожа **SpIDer Guard** или по просьбе технической поддержки компании **Dr.Web**.

Для задания типов информации, заносимой в отчет, служат следующие флаги:

- **Показывать программу упаковщик исполняемых файлов** - предписывает заносить сообщения об обнаружении исполняемых файлов, упакованных специальными упаковщиками, и имена этих упаковщиков. Флаг по умолчанию не установлен.
- **Показывать не инфицированные файлы** - предписывает заносить имена всех проверенных объектов, в том числе незараженных, для которых выводится пометка `Ok` (этот режим может значительно увеличить файл отчета). Флаг по умолчанию не установлен.

- **Показывать архиватор** - предписывает заносить сообщения о проверенных архивах и создавших их архиваторах, а также о связанных с ними ошибках (например, архив не удалось разархивировать, т.к. он защищен паролем). Флаг по умолчанию не установлен.

Поле **Максимальный размер файла отчета (в КБ)** позволяет ограничить размер файла отчета, задавая максимально допустимую величину в Кб.

9.2. Настройки SpIDer Guard NT4

Настройки программы по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.

При необходимости настройки файлового монитора SpIDer Guard NT4:

Пункт **Настройки SpIDer Guard** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

1. Чтобы просмотреть или изменить параметры сканирования, выберите в контекстном меню **Агента** пункт **Настройки SpIDer Guard** → **Настройки сканирования**. Подробное описание настроек приведено в Настройки сканирования.
2. Чтобы просмотреть или изменить параметры запуска сторожа, настройки его работы и оповещения о событиях, выберите в контекстном меню **Агента** пункт **Настройки SpIDer Guard** → **Управление**. Подробное описание управлением приведено в разделе Управление.

3. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от изменений.

Во всех диалоговых окнах, чтобы получить справку об активном окне, нажмите F1. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

9.2.1. Настройки сканирования

Настройки программы по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.

При необходимости настройки файлового монитора SpIDer Guard:

1. В контекстном меню **Агента** выберите пункт **Настройки SpIDer Guard** → **Настройки сканирования**.

Пункт **Настройки SpIDer Guard** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

2. Откроется окно настроек, содержащее следующие разделы:
   - раздел Проверка, в котором задается режим проверки файлов и процессов защищаемого компьютера;
   - раздел Типы файлов, в котором задается состав файлов, которые будут проверяться сторожем в соответствии с условиями, заданными на вкладке Проверка;

- раздел Действия, в котором задается реакция сторожа **SpIDer Guard** на обнаружение зараженных или подозрительных файлов и вредоносных программ;
- раздел Отчет, в котором задается режим ведения файла отчета сторожа **SpIDer Guard**;
- раздел Исключения, в котором задается список каталогов и файлов, исключаемых из проверки сторожем **SpIDer Guard**.

3. Внесите необходимые изменения.
4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от изменений.

9.2.1.1. Вкладка Проверка

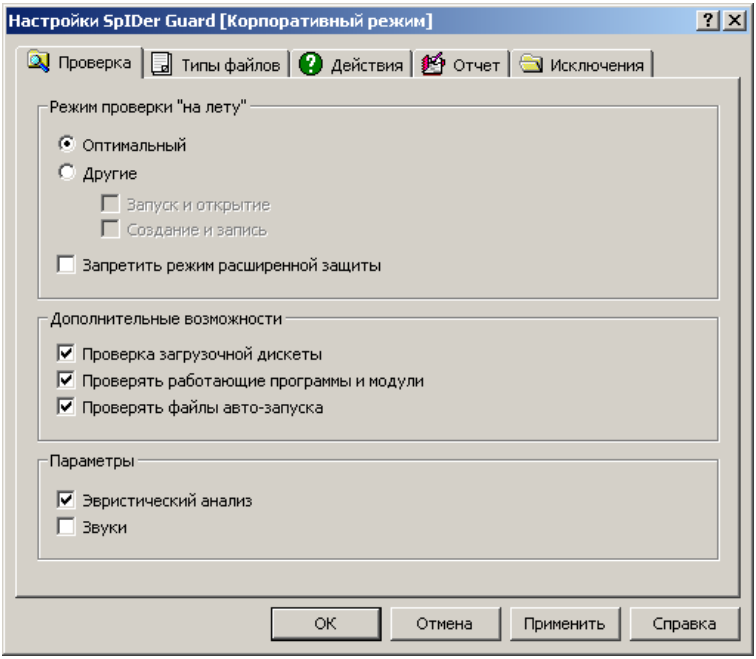

Рисунок 9-5. Окно настроек SpIDer Guard. Вкладка Проверка. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Проверка** задается режим проверки файлов и процессов защищаемого компьютера.

Режим проверки "на лету"

В разделе **Режим проверки "на лету"** задается режим проверки, определяющий при каких действиях с объектом должна производиться его проверка сторожем **SpIDer Guard**:

- Если выбран режим **Оптимальный**, то сканирование файлов и загрузочных секторов на жестких дисках производится только при некоторых обращениях к этим файлам: при запуске на исполнение, при создании, при записи (попытке записи) в существующие файлы или загрузочные сектора.

  Но сканирование файлов на сменных носителях и на сетевых дисках производится при любом обращении к этим файлам: при запуске на исполнение, при создании, при записи (попытке записи) в существующие файлы, а также при любом открытии файлов, в том числе только для чтения.

- При выборе варианта **Другие**, доступны следующие режимы:
  - **Запуск и открытие** - предписывает проверять все файлы при запуске на исполнение, а также при любом открытии файлов, в том числе только для чтения.
  - **Создание и запись** - предписывает проверять все файлы при создании или записи (попытке записи) в существующие файлы или загрузочные сектора.

  С помощью этих флагов вы можете самостоятельно установить уровень защиты компьютера.

Одновременная установка флагов **Запуск и открытие** и **Создание и запись** обеспечивает максимальный уровень защиты, но значительно увеличивает нагрузку на компьютер.

▸ Уточнения и рекомендации

Установку **Оптимального** режима рекомендуется производить после тщательной проверки всех жестких дисков при помощи **Сканера Dr.Web**. При этом будет исключено проникновение на компьютер новых вирусов или других вредоносных программ через сменные устройства, но при этом не будет проводиться повторного сканирования уже проверенных, «чистых», объектов.

Реакция сторожа **SpIDer Guard** на обнаружение вредоносных объектов задается в разделе Действия.

Некоторые внешние накопители (в частности, мобильные жесткие диски с интерфейсом USB) могут представляться в системе как жесткие диски. Поэтому такие устройства следует использовать с особой осторожностью и проверять на вирусы при подключении к компьютеру с помощью **Сканера Dr.Web**.

- Флаг **Запретить режим расширенной защиты** позволяет отключить режим расширенной защиты. По умолчанию данный режим включен. В этом режиме сторож проверяет все файлы, проверка которых предусмотрена настройками программы, немедленно, а остальные открывающиеся файлы помещает в очередь отложенной проверки (файлы, открывающиеся на чтение при режимах **Оптимальный** и **Создание и запись**). При наличии свободных ресурсов ПК эти файлы также будут проверены сторожем.

Дополнительные возможности

- флаг **Проверка загрузочной дискеты** задает проверку наличия дискеты в дисководе и, в случае наличия, проверку дискеты на вирусы (в случае зараженности дискеты при последующей загрузке ПК возможно его заражение).
- Флаг **Проверять работающие программы и модули** предписывает проверять файлы программ, работающих в данный период времени.
- Флаг **Проверять файлы авто-запуска** предписывает проверку всех файлов из автозагрузки (по каталогу `Автозагрузка`, системным `ini`-файлам, реестру ОС Windows).

Параметры

- Установите флаг **Эвристический анализ**, чтобы использовать при проверке эвристический анализатор.

Снимите этот флаг, чтобы проводить проверку только по сигнатурам известных вирусов (см. также раздел Методы обнаружения вирусов).

- Флаг **Звуки** задет использование звуковых реакций сторожа. По умолчанию звуки отключены.

9.2.1.2. Вкладка Типы файлов

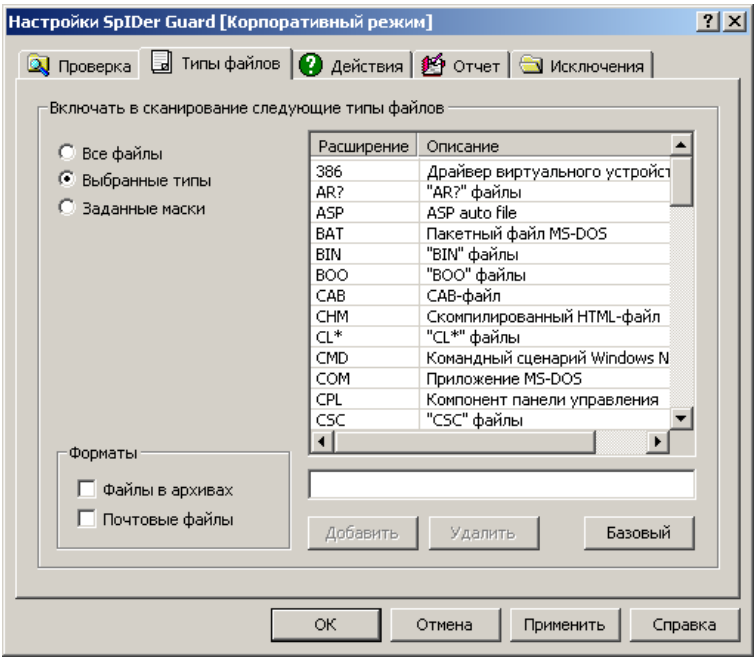

Рисунок 9-6. Окно настроек SpIDer Guard. Вкладка Типы файлов. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Типы файлов** задается дополнительное ограничение на состав файлов, которые должны проверяться в соответствии с условиями, заданными на вкладке Проверка.

В разделе **Включать в сканирование следующие типы файлов** выберите типы файлов, которые будут проверяться сторожем:

- Установленный по умолчанию вариант **Все файлы** предписывает проверку всех файлов согласно условиями, заданными на вкладке Проверка. Данный вариант обеспечивает максимальную защиту.
- Варианты **Выбранные типы** и **Заданные маски** предписывают проверять только файлы, типы или расширения и имена которых соответственно входят в список, задаваемый в правой части вкладки. Данный список активируется при установке переключателя на соответствующем пункте.

  По умолчанию список включает расширения основных типов файлов, которые могут быть носителями вирусов, и основных типов файловых архивов. Вы можете отредактировать этот список.

  Чтобы восстановить первоначальный список, нажмите кнопку **Базовый**.

Формирование списка проверяемых файлов

1. Чтобы добавить элемент в список проверяемых файлов:

   а) Выберите один из следующих разделов и задайте соответствующие значения проверяемых элементов:

   - чтобы задать список расширений проверяемых файлов, выберите опцию **Выбранные типы** и введите расширение файлов в поле ввода под списком;
   - чтобы задать проверяемые файлы определенного вида, выберите опцию **Заданные маски** и введите маску, определяющую данные файлы, в поле ввода под списком.

   ▸ Подробнее о масках

   Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в именах файлов, а также специальные обозначения:

- * заменяет любую (в том числе пустую) последовательность любых символов;
- ? заменяет один любой символ в заданной позиции.

Примеры:

- **отчет*.doc** – маска, задающая все документы Microsoft Word, название которых начинается с последовательности символов `отчет`, например, файлы `отчет-февраль.doc`, `отчет121209.doc` и т.д.;
- ***.exe** – маска, задающая все исполняемые файлы с расширением `EXE`, например, `setup.exe`, `iTunes.exe` и т.д.;
- **photo????09.jpg** – маска, задающая все файлы изображений формата `JPG`, название которых начинается с последовательности символов `photo` и заканчивается последовательностью символов `09`, при этом между двумя этими последовательностями в названии файла стоит четыре произвольных символа, например, `photo121209.jpg`, `photomama09.jpg` или `photo----09.jpg`.

b) Нажмите кнопку **Добавить**.

c) При необходимости повторите шаги a) и b) для добавления других типов или масок файлов.

2. Чтобы удалить элемент из списка проверяемых файлов, выберите данный элемент в списке и нажмите кнопку **Удалить**.
3. Для восстановления списка, заданного по умолчанию, нажмите кнопку **Базовый**.

Также на данной вкладке в разделе **Форматы** задается режим проверки файловых архивов и почтовых файлов:

- Установите флаг **Файлы в архивах** для проверки упакованных файлов. Файлы внутри архивов по умолчанию не проверяются, даже если тип или маска файла соответствующие архиву указаны в списке проверяемых типов или масок файлов (если какой-либо файл в архиве инфицирован, вирус будет обнаружен сторожем при извлечении файла из архива до появления возможности заражения ПК).

Включение этой проверки значительно увеличит нагрузку на компьютер.

- Установите флаг **Почтовые файлы** для проверки файлов электронной почты. Почтовые ящики по умолчанию не проверяются (если какой-либо файл в почтовом вложении инфицирован, вирус будет обнаружен сторожем при извлечении файла до появления возможности заражения ПК).

Включение проверки почтовых файлов может сильно увеличить нагрузку на процессор.

Для предотвращения проникновения вирусов с сообщениями электронной почты используйте почтовый сторож **SpIDer Mail**.

9.2.1.3. Вкладка Действия

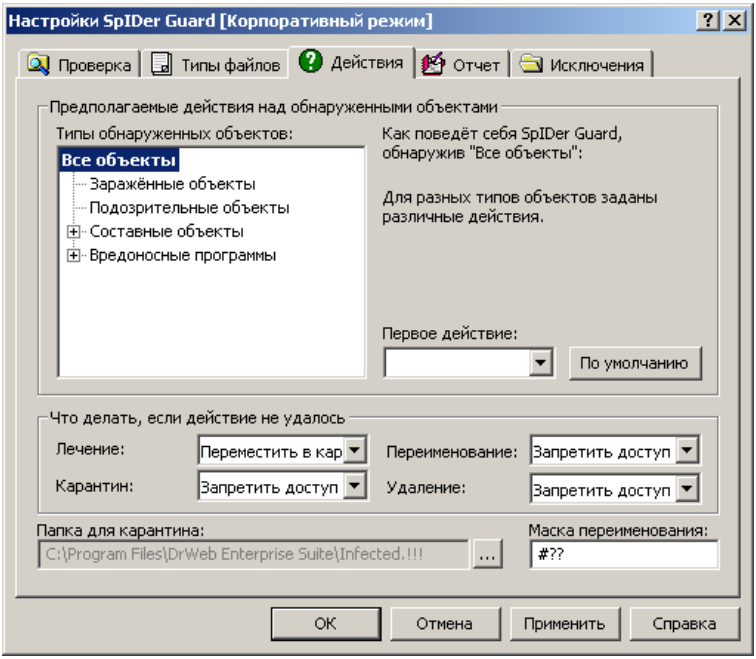

Рисунок 9-7. Окно настроек SpIDer Guard. Вкладка Действия. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Действия** задается реакция сторожа **SpIDer Guard** на обнаружение зараженных или подозрительных файлов и вредоносных программ. Состав доступных реакций при этом зависит от типа вирусного события.

Настройка действий

Все виды вредоносных объектов представлены в иерархическом списке в левой части окна. При выборе объекта из списка реакция программы по умолчанию на его обнаружение отображается в

правой части окна. Указывается действие, предписанное текущими настройками, а также последовательность действий в случае неудачи предыдущего.

Вы можете изменить реакции программы на обнаружение каждого типа объектов в отдельности.

Для задания действий над обнаруженными вредоносными объектами:

1. Чтобы изменить настройки первого действия, укажите в выпадающем списке **Первое действие** первичную реакцию программы.
2. В секции **Что делать, если действие не удалось** задаются те действия, которые выполняются в случае неудачного срабатывания следующих основных действий: лечение, перемещение в **Карантин**, переименование, удаление.

Возможные действия

Предусмотрены следующие действия над обнаруженными объектами:

- **Вылечить** – восстановить состояние инфицированного объекта до заражения.

  Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).

- **Удалить** – удалить зараженные или подозрительные объекты (для загрузочных секторов никаких действий производиться не будет).

По умолчанию программа не проверяет и не позволяет удалять файловые архивы. Если проверка файловых архивов включена (включение этой проверки значительно увеличит нагрузку на компьютер), вы можете разрешить выбор действия **Удалить** для архива. Для этого откройте в текстовом редакторе конфигурационный файл программы (файл `drweb32.ini` в каталоге установки программы), в секции `[SpIDerGuardNT]` добавьте строку `EnableDeleteArchiveAction=Yes` (или, если такая строка есть, исправьте значение `No` на `Yes`) и сохраните файл.

Для файлов внутри архивов никакие действия невозможны. При выборе действия **Удалить** архив будет удален целиком.

- **Переместить в карантин** – переместить зараженные объекты в каталог Карантина, задаваемый в поле **Папка для карантина** (по умолчанию подкаталог `infected.!!!` в каталоге установки программы).
- **Информировать** – ограничиться оповещением об обнаружении вируса (в окне Запрос пользователю).
- **Запретить доступ** – предписывает запретить доступ к файлу, проверка которого вызвала реакцию сторожа. Блокировка доступа к файлу снимается после перезагрузки компьютера, а также при временном отключении мониторинга.
- **Игнорировать** – пропустить объект без выполнения каких-либо действий и не выводить оповещения.

При задании действия **Игнорировать** не будет произведено никаких действий: пользователю не будет выдано предупреждение, как в случае включенной опции **Информировать** при обнаружении вредоносного объекта.

- **Переименовать** предписывает переименовать расширение имени зараженного или подозрительного объекта в соответствии с маской, задаваемой в поле **Маска переименования** (по умолчанию `#??`, т.е. заменить первый символ расширения на символ `#`).

Таблица 4. Действия SpIDer Guard над зараженными и подозрительными объектами

Действие	Объект	
	Зараженные	Подозрительные
Вылечить	+/*	
Удалить	+	+
Переместить в карантин	+	+/*
Информировать	+	+
Запретить доступ	+	+
Игнорировать		+
Переименовать	+	+

Таблица 5. Действия SpIDer Guard над составными объектами

Действие	Составной объект		
	Архивы	Почтовые файлы	Контейнеры
Переместить в карантин	+/*	+	+/*
Информировать	+	+/*	+
Запретить доступ	+	+	+
Игнорировать	+	+	+
Переименовать	+	+	+

Таблица 6. Действия SpIDer Guard над вредоносным ПО

Действие	Вредоносный объект				
	Реклама	Программы дозвона	Шутки	Потенциально опасные	Программы взлома
Удалить	+	+	+	+	+
Переместить в карантин	+	+	+	+	+
Информировать	+/*	+/*	+/*	+	+/*
Запретить доступ	+	+	+	+	+
Игнорировать	+	+	+	+/*	+
Переименовать	+	+	+	+	+

Условные обозначения

+	действие разрешено для данного типов объектов
+/*	действие установлено как первая реакция по умолчанию для данного типов объектов

При обнаружении объектов, содержащих **Рекламные программы** и **Программы дозвона**, для сторожа в пакете **Dr.Web для серверов** по умолчанию предусмотрена реакция **Переместить в карантин**, для сторожа в пакете **Dr.Web для рабочих станций** – **Информировать**.

Реакция при обнаружении

При обнаружении зараженного или подозрительного объекта возможны следующие реакции в зависимости от версии сторожа:

- **SpIDer Guard** в пакете **Dr.Web для рабочих станций** по умолчанию запрашивает действия пользователя. При этом сторож выводит окно Запрос пользователю, в котором вы можете в дальнейшем задать программе необходимые действия вручную.
- **SpIDer Guard** в пакете **Dr.Web для серверов** по умолчанию предпринимает автоматические действия по предотвращению вирусной угрозы.

9.2.1.4. Вкладка Отчет

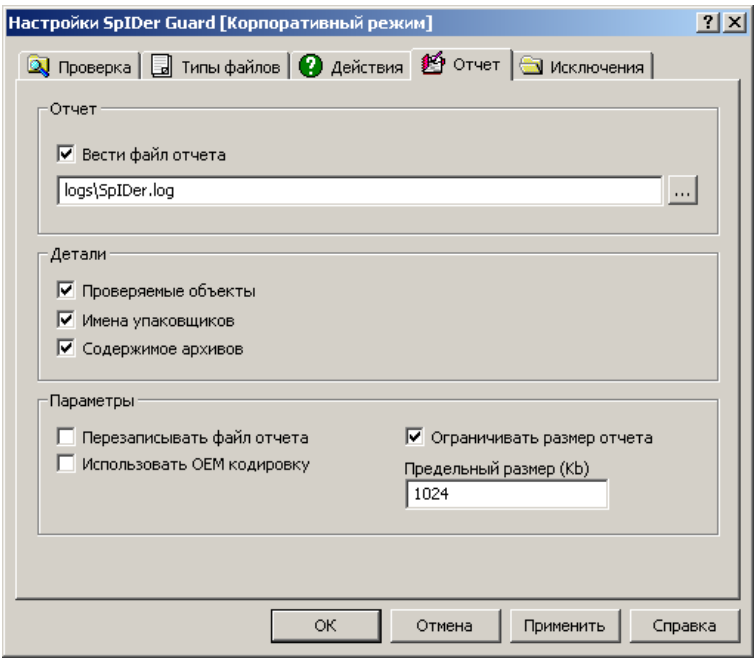

Рисунок 9-8. Окно настроек SpIDer Guard. Вкладка Отчет. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Отчет** задается режим ведения отчета и указывается информация, которая будет заноситься в файл отчета.

Рекомендуется вести файл отчета и периодически анализировать его.

Отчет

В секции **Отчет** устанавливаются общие параметры файла отчета.

Установите флаг **Вести файл отчета** для занесения данных о работе сторожа **SpIDer Guard** в файл отчета.

Также вы можете задать имя и расположение файла отчета в соответствующем поле. По умолчанию отчет сторожа **SpIDer Guard** записывается в `logs/SpIDer.log`, расположенном в каталоге установки **Enterprise Security Suite**.

Детали

В секции **Детали** указывается дополнительная информация, которая будет заноситься в отчет.

Для детализации отчета служат следующие флаги:

- **Проверяемые объекты** - предписывает заносить имена всех проверенных объектов, в том числе незараженных, для которых выводится пометка `Ok` (этот режим может значительно увеличить размер файла отчета). Флаг по умолчанию не установлен.
- **Имена упаковщиков** - предписывает заносить сообщения об обнаружении исполняемых файлов, упакованных специальными упаковщиками, и имена этих упаковщиков.

- **Содержимое архивов** - предписывает заносить сообщения о проверенных архивах и создавших их архиваторах, а также о связанных с ними ошибках (например, архив не удалось разархивировать, т.к. он защищен паролем).

Параметры

В разделе **Параметры** задаются дополнительные параметры записи файла отчета:

- Установите флаг **Перезаписывать файл отчета** для удаления старого файла отчета и записи нового в начале каждого сеанса. Если данный флаг снят, то данные отчета будут записываться в конец существующего файла.
- Установите флаг **Использовать OEM кодировку** для записи отчета в DOS-кодировке.
- Если вы хотите ограничить размер файла отчета, установите флаг **Ограничивать размер отчета** и введите максимально допустимый размер файла в килобайтах в поле **Предельный размер (Kb)**. При превышении максимального размера файл отчета очищается и информация в него начинает записываться с начала.

9.2.1.5. Вкладка Исключения

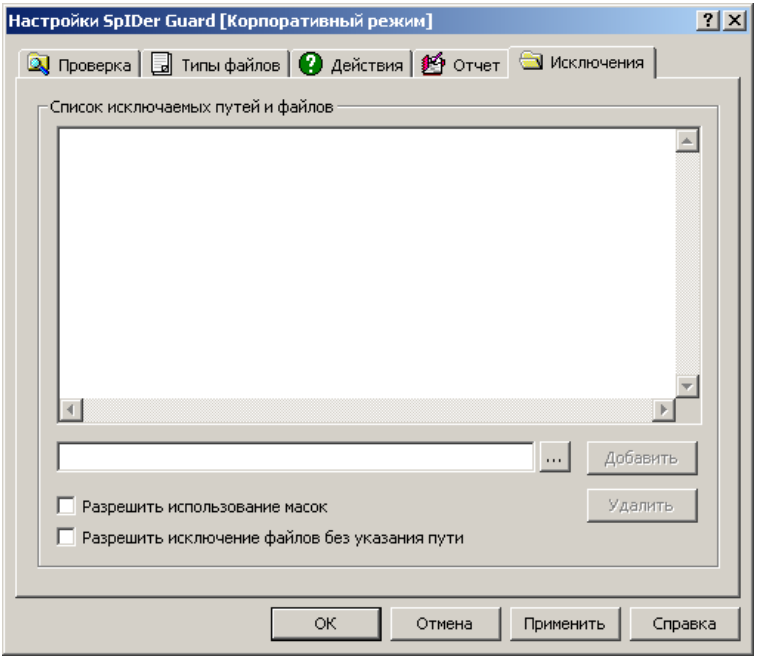

Рисунок 9-9. Окно настроек SpIDer Guard. Вкладка Исключения. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Исключения** задается список каталогов и файлов, исключаемых из проверки сторожем **SpIDer Guard**.

В разделе **Список исключаемых путей и файлов** приводится список каталогов и файлов, которые не проверяются сторожем **SpIDer Guard**. В таком качестве могут выступать каталоги карантина антивируса, рабочие каталоги некоторых программ, временные файлы (файлы подкачки) и т.п.

По умолчанию список пуст. Вы можете добавить к исключениям конкретные каталоги и файлы или использовать маски, чтобы запретить проверку определенной группы объектов.

Формирование списка исключений

1. Чтобы добавить каталог или файл к списку исключений, выполните одно из следующих действий:
   - чтобы указать конкретный существующий каталог или файл, нажмите кнопку  и выберите каталог или файл в стандартном браузере по операционной системе. Вы также можете вручную ввести полный путь к файлу или каталогу в поле ввода;
   - чтобы исключить из проверки все файлы или каталоги с определенным именем без указания конкретного пути, установите флаг **Разрешить исключение файлов без указания пути**, после чего введите требуемое имя в поле ввода;
   - чтобы исключить из проверки файлы или каталоги определенного вида, установите флаг **Разрешить использование масок**, после чего введите маску в поле ввода.

   ▸ Подробнее о масках

   Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в именах файлов, а также специальные обозначения:

   - `*` заменяет любую (в том числе пустую) последовательность любых символов;
   - `?` заменяет один любой символ в заданной позиции.

   Примеры:

   - **отчет*.doc** – маска, задающая все документы Microsoft Word, название которых начинается с последовательности символов `отчет`, например, файлы `отчет-февраль.doc`, `отчет121209.doc` и т.д.;
   - ***.exe** – маска, задающая все исполняемые файлы с расширением `EXE`, например, `setup.exe`, `iTunes.exe` и т.д.;

- **photo????09.jpg** – маска, задающая все файлы изображений формата JPG, название которых начинается с последовательности символов photo и заканчивается последовательностью символов 09, при этом между двумя этими последовательностями в названии файла стоит четыре произвольных символа, например, photo121209.jpg, photomama09.jpg или photo----09.jpg.

2. Нажмите кнопку **Добавить**.
3. При необходимости повторите шаги 1 и 2 для добавления других файлов или каталогов.
4. Чтобы удалить файл или каталог из списка исключений, выберите соответствующий элемент в списке и нажмите кнопку **Удалить**.

9.2.2. Управление

Настройки программы по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.

При необходимости настройки файлового монитора SpIDer Guard:

1. В контекстном меню **Агента** выберите пункт **Настройки SpIDer Guard** → **Управление** либо воспользуйтесь элементом **SpIDer Guard**, расположенным на **Панели управления** ОС Windows.

Пункт **Настройки SpIDer Guard** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

2. Откроется окно настроек, содержащее следующие разделы:
   - Управление;
   - Параметры;
   - Уведомления;
   - Напоминания.
3. Внесите необходимые изменения.
4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от изменений.

9.2.2.1. Вкладка Управление

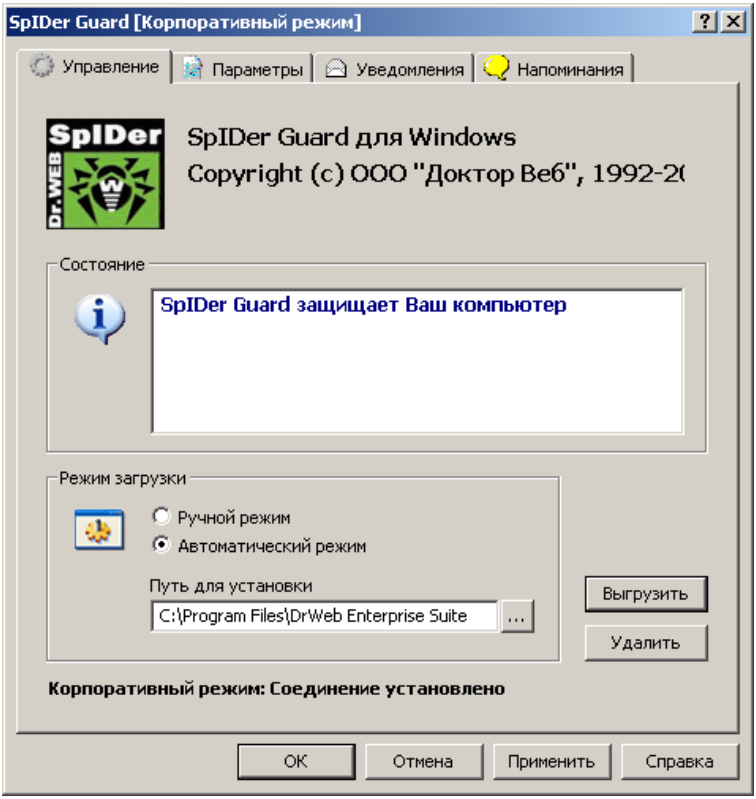

Рисунок 9-10. Окно управления SpIDer Guard. Вкладка Управление.

Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Управление** задается режим загрузки **SpIDer Guard**, а также производится (либо отменяется) регистрация компонента в операционной системе.

Раздел **Режим загрузки** позволяет выбрать способ запуска программы:

- Если выбран **Ручной режим**, для запуска сторожа нажмите на кнопку **Загрузить**. Запущенный таким образом сторож можно остановить, нажав на кнопку **Выгрузить**.
- Если выбран вариант **Автоматический режим**, сторож запускается автоматически при каждой загрузке ОС Windows.

Для того чтобы зарегистрировать сторож в операционной системе, нажмите на кнопку **Установить**, для того чтобы отменить такую регистрацию – на кнопку **Удалить**.

После установки **Антивируса**, согласно стандартным настройкам, загрузка сторожа производится автоматически сразу после запуска операционной системы. Однако вы можете изменить режим загрузки **SpIDer Guard**, отменив автоматический режим.

Для того чтобы отменить режим автоматического запуска SpIDer Guard:

1. Перейдите на вкладку Управление окна элемента Панели управления **SpIDer Guard**.

Пункт **Настройки SpIDer Guard** → **Управление** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

2. В группе кнопок выбора **Режим загрузки** загрузки выберите **Ручной режим**.
3. Нажмите на кнопку **ОК**.

При последующих запусках ОС Windows программа не будет запускаться автоматически. При необходимости ее можно будет запустить вручную, для чего следует нажать в

вышеописанном окне на кнопку **Загрузить**. Сторож, запущенный вручную, можно остановить нажатием на кнопку **Выгрузить**.

9.2.2.2. Вкладка Параметры

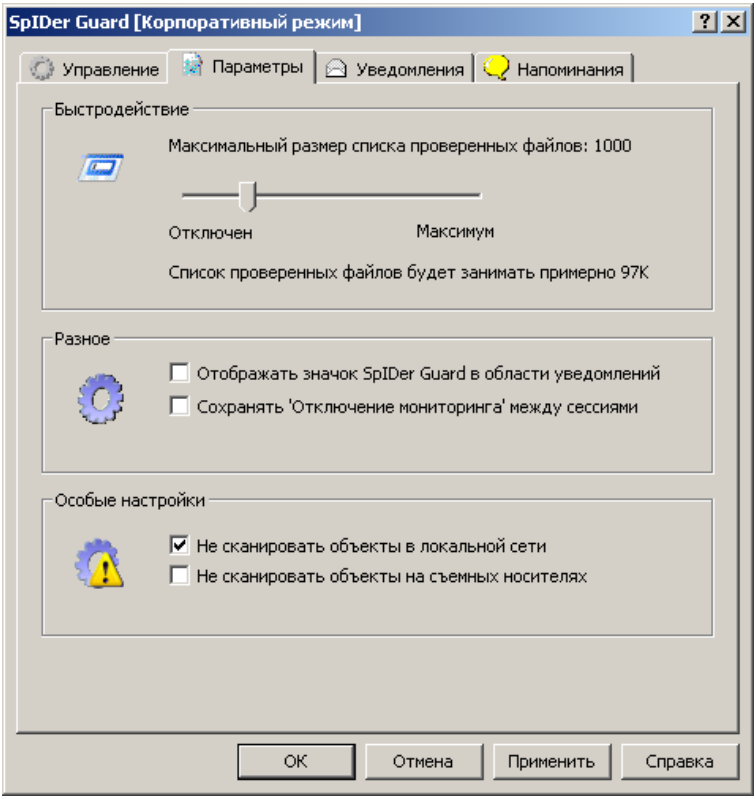

Рисунок 9-11. Окно управления SpIDer Guard. Вкладка Параметры.

Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На этой вкладке элемента Панели управления **SpIDer Guard** задаются отдельные настройки сторожа.

Быстродействие

В разделе **Быстродействие** задается размер списка путей проверенных файлов, хранимого в сверхоперативной памяти.

Передвигая бегунок, установите размер данного списка.

Файлы из этого списка исключаются из повторных проверок, если в них не производятся изменения. По умолчанию значение данного параметра принимается равным 100, что соответствует в среднем 9 КБ используемой памяти на каждый логический диск. Если система располагает достаточным ресурсом свободной памяти, то имеет смысл увеличить этот параметр до 500–1000. Параметр актуален только для режима проверки **Запуск и открытие** и при проверке файлов на сетевых дисках и сменных носителях в режиме **Оптимальный**.

Разное

В разделе **Разное** вы можете задать следующие настройки:

- Установите флаг **Отображать значок SpIDer Guard в области уведомлений**, если хотите отображать значок сторожа в области уведомления Панели задач (элемент рабочего стола Microsoft Windows, отображающий значки активных приложений и располагающийся в правой части Панели задач, которая по умолчанию находится внизу рабочего стола) ОС Windows.
- При установке флага **Сохранять 'Отключение мониторинга' между сессиями SpIDer Guard** будет сохранять режим паузы после перезагрузки, в том случае, если в текущем сеансе работы мониторинг был отключен.

Особые настройки

В разделе **Особые настройки** вы можете задать следующие настройки:

- Установите флаг **Не сканировать объекты на съемных носителях**, чтобы сканирование файлов на сменных носителях осуществлялось только при запуске этих файлов на исполнение.

  Если флаг **Не сканировать объекты на съемных носителях** снят, то сканирование файлов на сменных носителях информации (CD/DVD диски, магнитные диски (FDD), flash-накопители и прочие носители информации, подключаемые через USB-порт и т.п.) будет производиться при любом обращении к ним, в том числе при открытии файлов только для чтения.

- Установите флаг **Не сканировать объекты в локальной сети**, чтобы сканирование файлов на сетевых дисках осуществлялось только при запуске этих файлов на исполнение на вашем компьютере.

  Если флаг **Не сканировать объекты в локальной сети** снят, то проверка объектов на сетевых дисках будет производиться при запуске этих файлов на исполнение на вашем компьютере, а также при любом открытии файлов, в том числе файлов только для чтения.

Некоторые внешние накопители (в частности, мобильные винчестеры с интерфейсом USB) могут представляться в системе как жесткие диски. Поэтому такие устройства следует использовать с особой осторожностью, проверяя на вирусы при подключении к компьютеру с помощью антивирусного сканера.

9.2.2.3. Вкладка Уведомления

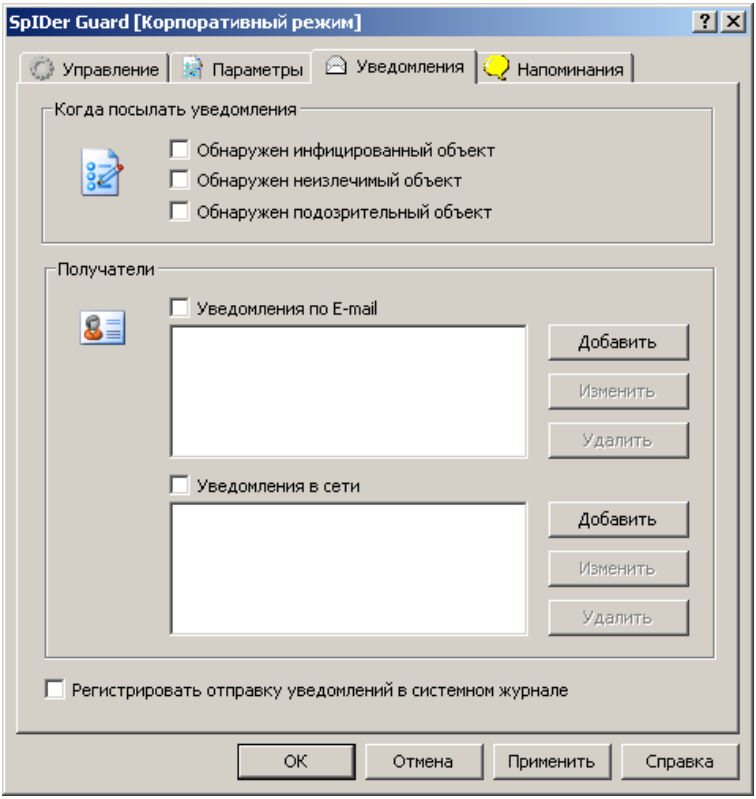

Рисунок 9-12. Окно управления SpIDer Guard. Вкладка Уведомления.

Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Уведомления** задаются настройки уведомления о выявленных вирусных событиях: перечень событий, вызывающих отправку уведомления, способ его отправки и перечни адресатов.

В разделе **Когда посылать уведомления** установите флаги для тех типов событий, о которых следует посылать оповещения.

В разделе **Получатели** задается способ отправки уведомлений:

- Установите флаг **Уведомления по E-mail**, если хотите посылать уведомления о выбранных событиях по электронной почте.
- Установите флаг **Уведомления в сети**, если хотите посылать уведомления о выбранных событиях в локальной сети.

Флаги **Уведомления по E-mail** и **Уведомления в сети** независимы и могут устанавливаться одновременно.

После этого следует создать (отредактировать) списки адресатов уведомлений для выбранных способов:

1. Чтобы добавить новый элемент в список получателей по электронной почте, нажмите на кнопку **Добавить** рядом со списком e-mail адресов. Откроется окно настройки E-mail адреса.
2. Чтобы добавить новый элемент в список адресатов сообщений в локальной сети, нажмите на кнопку **Добавить** рядом со списком сетевых адресов. Откроется окно настройки сетевого адреса.
3. Для того чтобы удалить элемент из какого-либо списка, выберите его в одном из списков и нажмите на кнопку **Удалить**.
4. Для того чтобы отредактировать элемент какого-либо списка, выберите его в одном из списков и нажмите на кнопку **Изменить**. Откроется окно настройки E-mail адреса или окно настройки сетевого адреса соответственно.

9.2.2.4. Вкладка Напоминания

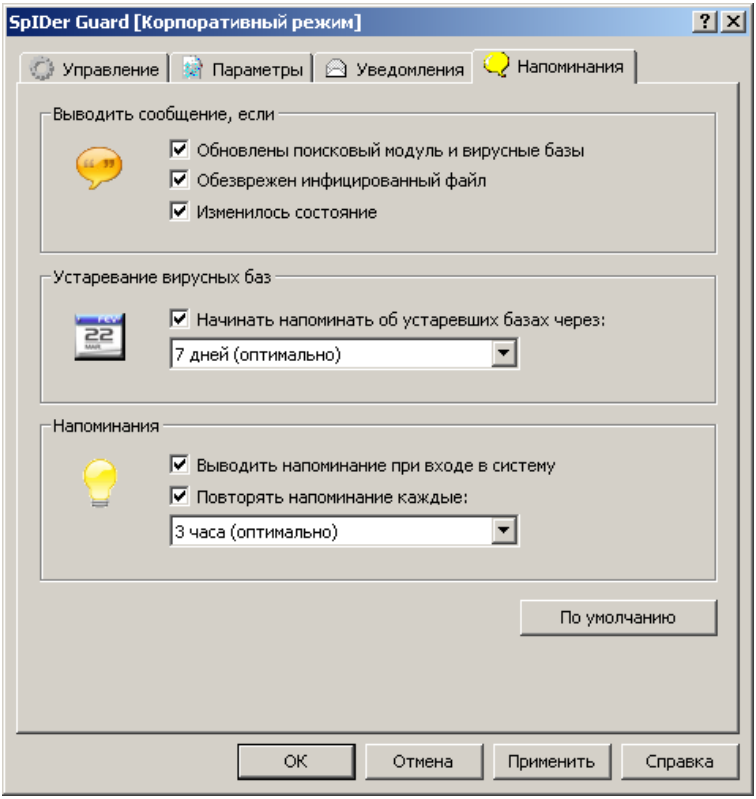

Рисунок 9-13. Окно управления SpIDer Guard. Вкладка Напоминания.

Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На вкладке **Напоминания** задаются настройки появления подсказок-напоминаний. Данные подсказки появляются в виде всплывающего уведомления над значком **SpIDer Guard** в области уведомлений ОС Windows, в том случае, если установлен режим отображения значка сторожа.

В разделе **Выводить сообщение, если** задается перечень событий, при возникновении которых появляется всплывающее уведомление:

- **Обновлены поисковый модуль и вирусные базы** - оповещать при обновлении антивирусного ядра и вирусных баз.
- **Обезврежен инфицированный файл** - оповещать при обнаружении и обезвреживании зараженного объекта.
- **Изменилось состояние** - оповещать при изменениях в работе сторожа **SpIDer Guard** (остановка, запуск).

Флаг **Начинать напоминать об устаревших базах после** указывает сторожу выводить напоминание, если обновление вирусных баз не производилось в истечение срока, указанного в выпадающем списке.

В группе **Напоминания** задается режим появления подсказок о заданных событиях:

- **Выводить напоминание при входе в систему** - отображать подсказки при каждой загрузке операционной системы.
- **Повторять напоминание каждые** - включить повтор напоминаний через каждый промежуток времени, указанный в выпадающем списке.

Нажмите на кнопку **По умолчанию** чтобы восстановить первоначальные, рекомендованные программой, настройки.

9.2.3. Дополнительные пользовательские диалоги

9.2.3.1. Запрос пользователю в случае обнаружения зараженного объекта

Данное окно открывается при обнаружении сторожем зараженного или подозрительного объекта, если в настройках реакции программы задано информирование.

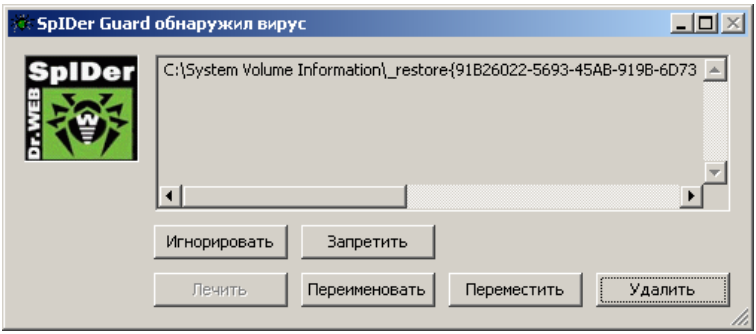

Рисунок 9-14. Окно запроса действий сторожа в случае обнаружения зараженного объекта

Состав доступных кнопок зависит от типа вирусного события и типа зараженного объекта (для архивов, почтовых файлов и файловых контейнеров часть реакций недоступна).

- Кнопка **Игнорировать** предписывает не предпринимать каких-либо действий при обнаружении подозрительного объекта.
- Кнопка **Запретить** предписывает запретить доступ к файлу, проверка которого вызвала реакцию сторожа. Блокировка доступа к файлу снимается после перезагрузки компьютера, а также при временном отключении мониторинга.
- Кнопка **Лечить** (доступна только при обнаружении предположительно излечимого вируса, недоступна для архивов любого типа) предписывает сторожу пытаться

вылечить объект, зараженный известным вирусом. Если вирус неизлечим или попытка лечения не была успешной, окно откроется снова в виде, предусмотренном для обнаружения неизлечимых вирусов.

- Кнопка **Переименовать** предписывает переименовать расширение имени зараженного или подозрительного файла в соответствии с настройками по умолчанию.
- Кнопка **Переместить** предписывает переместить зараженный или подозрительный файл в каталог карантина, заданный по умолчанию.
- Кнопка **Удалить** предписывает удалить зараженный или подозрительный файл (для загрузочных секторов никаких действий производиться не будет). При настройках по умолчанию недоступна для архивов любого типа.

9.2.3.2. Окно настроки E-mail адреса

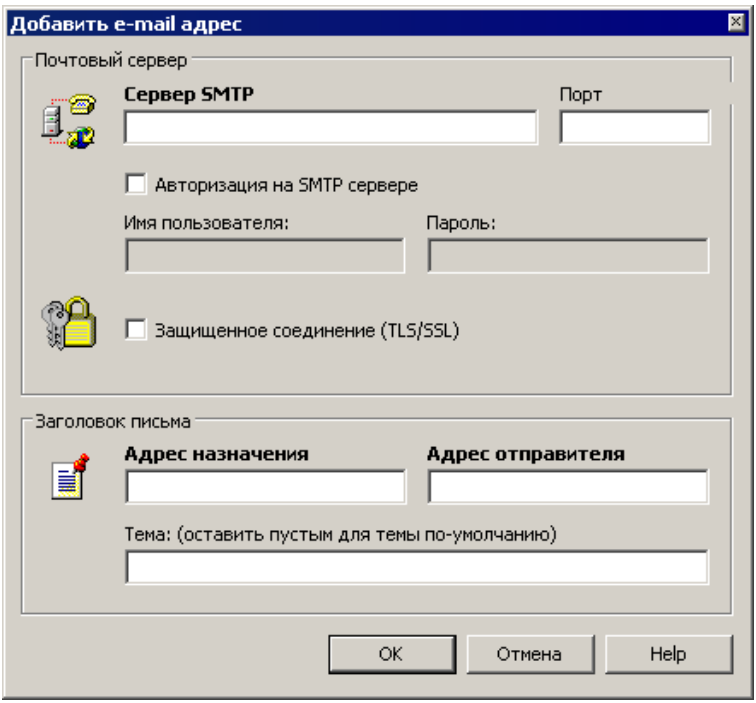

Рисунок 9-15. Окно задания почтового адреса

В этом окне задаются адрес и почтовые настройки ящика электронной почты, по которому будут направляться уведомления о вирусных событиях.

Почтовый сервер

В разделе **Почтовый сервер** задаются настройки SMTP-сервера для отправки электронной почты.

Обязательными являются параметры:

- **Сервер SMTP** - IP адрес или доменное имя сервера для отправляемой почты.
- **Порт** - номер порта, используемого сервером SMTP.

Если на сервере SMTP требуется авторизация, установите флаг **Авторизация на SMTP сервере** и заполните поля **Имя пользователя** и **Пароль** для доступа к серверу отправляемой почты.

При необходимости использования защищенного соединения на основе протоколов TLS и SSL установите флаг **Защищенное соединение (TLS/SSL)**.

Заголовок письма

В разделе **Заголовок письма** задаются атрибуты почтового сообщения.

Укажите следующие e-mail адреса:

- В поле **Адрес назначения** задайте адрес электронной почты, на который будут отправляться уведомления о вирусных событиях.
- В поле **Адрес отправителя** задайте адрес электронной почты, который будет указан как адрес отправителя в сообщении о вирусной обстановке.

Вы также можете указать тему почтового сообщения в поле **Тема**. Если данное поле не заполнено, то в письме будет указана тема, заданная по умолчанию.

9.2.3.3. Окно настройки сетевого адреса

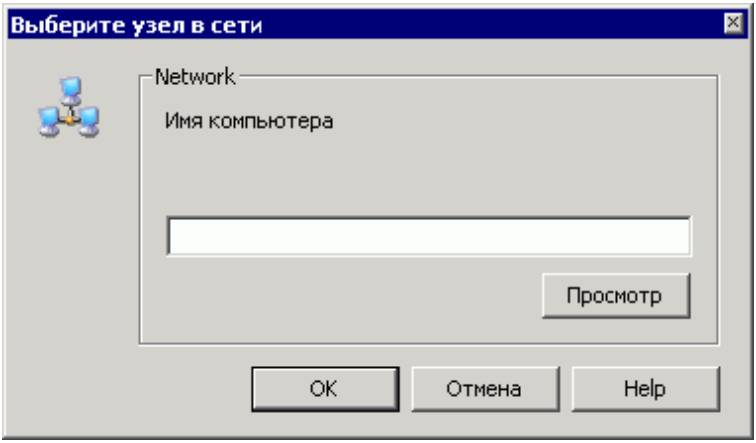

Рисунок 9-16. Окно задания адресата в локальной сети

В данном окне вводится адрес компьютера в сети Microsoft для включения компьютера в список, по которому будут направляться уведомления.

Введите в поле **Имя компьютера** сетевое имя компьютера, или нажмите на кнопку **Просмотр**, чтобы найти компьютер в каталоге Обозревателя сети.

Глава 10. SpIDer Mail

Почтовый сторож **SpIDer Mail** по умолчанию включается в состав устанавливаемых компонентов, постоянно находится в памяти и автоматически запускается при загрузке операционной системы.

Если антивирус работает с лицензией на программный пакет «Антивирус+Антиспам» (и соответствующим ключевым файлом), то почтовый сторож также может осуществлять проверку корреспонденции на спам с помощью **Антиспама Dr.Web**.

Настройки **SpIDer Mail** по умолчанию являются оптимальными для начинающего пользователя, обеспечивая максимальный уровень защиты при наименьшем вмешательстве пользователя. При этом, однако, блокируется ряд возможностей почтовых программ (например, направление письма по многим адресам может быть воспринято как массовая рассылка, полученный спам не распознается), а также теряется возможность получения полезной информации из автоматически уничтоженных писем (из незараженной текстовой части). Более опытные пользователи могут изменить параметры проверки почты и настройки реакции почтового сторожа **SpIDer Mail** на различные события.

Обработка писем

По умолчанию почтовый сторож **SpIDer Mail** автоматически перехватывает все обращения к почтовым серверам, выполняемые по стандартным для протоколов портам любыми почтовыми программами вашего компьютера. Стандартными являются следующие порты:

- для протокола POP3 - порт 110;
- для протокола SMTP - порт 25;
- для протокола IMAP4 - порт 143;
- для протокола NNTP - порт 119.

В ряде случаев автоматический перехват POP3-, SMTP-, IMAP4- и NNTP-соединений невозможен. В таком случае вы можете настроить перехват соединений вручную.

Почтовый сторож **SpIDer Mail** получает все входящие письма вместо почтового клиента и подвергает их антивирусному сканированию с максимальной степенью подробности. При отсутствии вирусов или подозрительных объектов оно передается почтовой программе «прозрачным» образом – так, как если бы оно поступило непосредственно с сервера. Аналогично исходящие письма проверяются до отправки на сервер.

Антиспам Dr.Web

Функция проверки писем на спам доступна только в том случае, если **Dr.Web Agent** работает с лицензией «Антивирус+антиспам».

Технологии антиспам-фильтра **Dr.Web** состоят из нескольких тысяч правил, которые условно можно разбить на несколько групп:

- **эвристический анализ** – чрезвычайно сложная, высокоинтеллектуальная технология эмпирического разбора всех частей письма: поля заголовка, тела, содержания вложения;
- **фильтрация противодействия** – состоит в распознавании уловок, используемых спамерами для обхода антиспам-фильтров;
- **анализ на основе HTML-сигнатур** – сообщения, в состав которых входит HTML-код, сравниваются с образцами библиотеки HTML-сигнатур антиспама;
- **семантический анализ** – сравнение слов и выражений сообщения со словами и идиомами, типичными для спама, производится по специальному словарю. Анализу подвергаются как видимые, так и визуально скрытые специальными техническими уловками слова, выражения и символы;

- **анти-скамминг технология** – к числу скамминг- и фарминг-сообщений относятся т.н. «нигерийские письма», сообщения о выигрышах в лотерею, казино, поддельные письма банков. Для их фильтрации применяется специальный модуль;
- **фильтрация технического спама** – так называемые bounce-сообщения возникают как реакция на вирусы, или как проявление вирусной активности. Специальный модуль антиспама определяет такие сообщения как нежелательные.

Реакции SpIDer Mail

Реакция почтового сторожа **SpIDer Mail** на обнаружение инфицированных и подозрительных входящих писем, а также писем, не прошедших проверки (например, писем с чрезмерно сложной структурой), по умолчанию следующая:

- из зараженных писем удаляется вредоносная информация (это действие называется *лечением* письма), затем они доставляются обычным образом;
- письма с подозрительными объектами перемещаются в виде отдельных файлов в Карантин, почтовой программе посылается сообщение об этом (это действие называется *перемещением* письма);
- незараженные письма и письма, не прошедшие проверку, передаются без изменений (*пропускаются*);
- все удаленные или перемещенные письма также удаляются с POP3- или IMAP4-сервера.

Инфицированные или подозрительные исходящие письма не передаются на сервер, пользователь извещается об отказе в отправке сообщения (как правило, почтовая программа при этом сохраняет письмо).

При наличии на компьютере неизвестного вируса, распространяющегося через электронную почту, почтовый сторож **SpIDer Mail** может определять признаки типичного для таких вирусов «поведения» (массовые рассылки). По умолчанию эта возможность включена.

Почтовый сторож **SpIDer Mail** предоставляет возможность проверки входящих писем на спам с помощью Антиспама Dr.Web. По умолчанию эта возможность включена.

Проверка писем другими средствами

Сторож **SpIDer Guard** и **Сканер Dr.Web** также может обнаруживать вирусы в почтовых ящиках некоторых форматов, однако почтовый сторож **SpIDer Mail** имеет перед ним ряд преимуществ:

- далеко не все форматы почтовых ящиков популярных программ поддерживаются сторожем **SpIDer Guard** и **Сканером Dr.Web**; при использовании почтового сторожа **SpIDer Mail** зараженные письма даже не попадают в почтовые ящики;
- **SpIDer Guard** по умолчанию не проверяет почтовые ящики, при включении этой возможности производительность системы значительно снижается;
- **Сканер Dr.Web** проверяет почтовые ящики, но только по запросу пользователя или по расписанию, а не в момент получения почты, причем данное действие является трудоемким и занимает значительное время.

Таким образом, при настройках всех компонентов **Enterprise Security Suite** по умолчанию почтовый сторож **SpIDer Mail** первым обнаруживает и не допускает на компьютер вирусы и подозрительные объекты, распространяющиеся по электронной почте. Его работа является весьма экономичной с точки зрения расхода вычислительных ресурсов; остальные компоненты могут не использоваться для проверки почтовых файлов.

Настройка сторожа

Раздел настроек сторожа **SpIDer Mail** различается в зависимости от установленной версии сторожа. Существуют две версии сторожа **SpIDer Mail**:

- SpIDer Mail,

- SpIDer Mail NT4.

Перед установкой сторожа автоматически определяется версия операционной системы и устанавливается соответствующая версия **SpIDer Mail** (см. п. Системные требования).

При необходимости (например, в случае выполнения критически чувствительного к загрузке процессора задания в реальном масштабе времени) вы можете временно отключить работу сторожа.

10.1. Настройка SpIDer Mail

Настройки программы по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.

При необходимости настройки почтового монитора SpIDer Mail:

1. В контекстном меню **Агента** выберите пункт **Настройки SpIDer Mail**.

Пункт **Настройки SpIDer Mail** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

2. Откроется окно настроек, содержащее следующие разделы:
   - Раздел **Действия**, в котором задается режим проверки электронной почты (подробное описание приведено в Справке **Антивирус Dr.Web для Windows**, **Раздел Проверка**).

- Раздел **Антиспам**, в котором задается режим проверки электронной почты на спам с помощью **Антиспама Dr.Web** (подробное описание приведено в Справке **Антивирус Dr.Web для Windows**, **Раздел Антиспам**).
- Раздел **Исключения**, в котором задается список приложений, почтовый трафик которых исключается из проверки почтовым сторожем **SpIDer Mail** (подробное описание приведено в Справке **Антивирус Dr.Web для Windows**, **Раздел Исключения**).
- Раздел **Перехват**, в котором задаются параметры перехвата соединений с почтовыми серверами (подробное описание приведено в Справке **Антивирус Dr.Web для Windows**, **Раздел Перехват**).
- Раздел **Отчет**, в котором задается режим ведения файла отчета почтового сторожа **SpIDer Mail** (подробное описание приведено в Справке **Антивирус Dr.Web для Windows**, **Раздел Отчет**).

Во всех диалоговых окнах, чтобы получить справку об активном окне, нажмите F1.

3. Внесите необходимые изменения.
4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от изменений.

10.2. Настройка SpIDer Mail NT4

Настройки программы по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.

При необходимости настройки почтового монитора SpIDer Mail NT4:

1. В контекстном меню **Агента** выберите пункт **Настройки SpIDer Mail**.

Пункт **Настройки SpIDer Mail** доступен в контекстном меню **Агента** только при наличии у пользователя:

1. Прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.
2. Прав администратора на данном компьютере.

2. Откроется окно настроек, содержащее следующие разделы:
   - раздел Проверка, в котором задается режим проверки электронной почты;
   - раздел Действия, в котором задается реакция сторожа **SpIDer Mail** на обнаружение зараженных или подозрительных файлов в электронной почте;
   - раздел Ядро, в котором задаются параметры работы антивирусного ядра;
   - раздел Отчет, в котором задается режим ведения файла отчета сторожа **SpIDer Mail**;
   - раздел Перехват, в котором задаются параметры перехвата соединений с POP3/SMTP/IMAP4/NNTP-серверами;
   - раздел Исключаемые приложения, в котором задается список каталогов и файлов, исключаемых из проверки сторожем **SpIDer Mail**.
3. Внесите необходимые изменения.
4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от изменений.

10.2.1. Вкладка Проверка

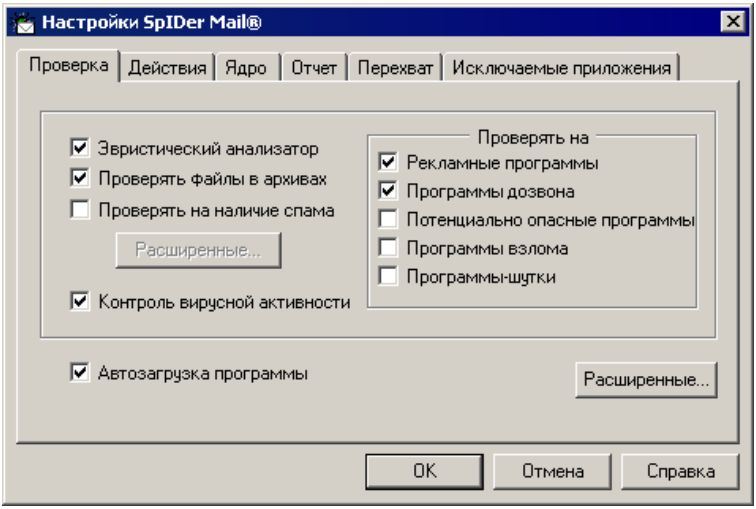

Рисунок 10-1. Окно настроек SpIDer Mail. Вкладка Проверка. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На данной вкладке задается режим проверки электронной почты.

Следующая группа настроек задает параметры проверки электронной почты. По умолчанию установлены следующие важные настройки, изменять которые не рекомендуется:

- Установленный по умолчанию флаг **Эвристический анализатор** предписывается почтовому сторожу использование эвристического анализа при проверке электронной почты. В данном режиме используются специальные механизмы, позволяющие выявить в электронной почте подозрительные объекты, с большой вероятностью зараженные еще неизвестными вирусами.
- Установленный по умолчанию флаг **Проверять файлы в архивах** предписывает проверять содержимое архивов, передаваемых по электронной почте. Для ускорения работы

почтового сторожа **SpIDer Mail** снимите флаг **Проверять файлы в архивах**, чтобы отключить эту настройку.

Отказ от проверки содержимого архивов в условиях постоянной работы сторожа **SpIDer Guard** не ведет к проникновению вирусов на компьютер, а лишь откладывает момент их обнаружения. При распаковке зараженного архива операционная система производит попытку записать инфицированный объект на диск, при этом вредоносный объект будет обнаружен сторожем **SpIDer Guard**.

- Флаг **Контроль вирусной активности** по умолчанию установлен. Данный режим предписывает программе обнаруживать характерные признаки вирусных массовых рассылок, которые являются частым следствием заражения компьютера вирусами. В данном режиме почтовый стороже **SpIDer Mail** может блокировать отправку вами почты по нескольким адресам. При возникновении трудностей с отправкой сообщений нескольким адресатам одновременно, рекомендуется снять данный флаг.

Также на данной вкладке вы можете задать проверку вашей электронной почты на наличие нежелательной корреспонденции:

- Флаг **Проверять на наличие спама** предписывает почтовому сторожу осуществлять проверку входящих писем спам-фильтром.

Функция проверки писем на спам доступна только в том случае, если **Dr.Web Агент** работает с лицензией на программный пакет "Антивирус+антиспам".

Для того чтобы изменить настройки спам-фильтра, нажмите на кнопку **Расширенные**, расположенную ниже. Откроется окно Настройки проверки писем на наличие спама.

Почтовый сторож может обнаруживать наряду с письмами, содержащими инфицированные файлы, письма, содержащие другие разновидности нежелательных программ:

- **Рекламные программы**,
- **Программы дозвона**,
- **Потенциально опасные программы**,
- **Программы взлома**,
- **Программы-шутки**.

Для того чтобы изменить состав обнаруживаемых нежелательных программ, установите флаги у наименований типов нежелательных программ, которые необходимо обнаруживать и снимите флаги у наименований типов программ, которые не надо обнаруживать.

По умолчанию почтовому сторожу предписано обнаруживать из предложенного списка только **Рекламные программы** и **Программы дозвона**.

Реакция почтового сторожа на обнаружение нежелательных программ совпадает с реакцией на обнаружение инфицированных писем, задаваемой на вкладке Действия.

Флаг **Автозагрузка программы** по умолчанию установлен. При этом **SpIDer Mail** автоматически запускается при загрузке ОС Windows. Вы можете снять данный флаг; в этом случае запуск программы необходимо осуществлять вручную.

Для настройки дополнительных параметров проверки электронной почты нажмите кнопку Расширенные в правом нижнем углу окна.

10.2.1.1. Настройки антиспам-фильтра

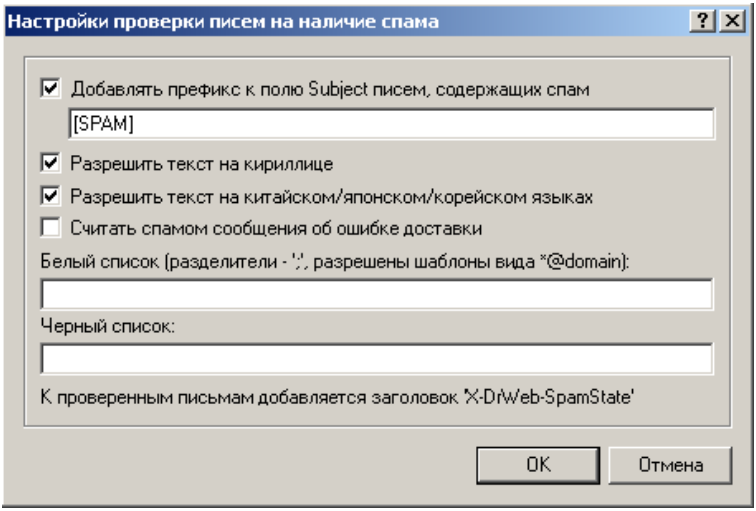

Рисунок 10-2. Окно настроек SpIDer Mail.

Если для получения почтовых сообщений вы используете протоколы IMAP/NNTP – настройте вашу почтовую программу таким образом, чтобы письма загружались с почтового сервера сразу целиком, без предварительного просмотра заголовков. Это необходимо для корректной работы спам-фильтра.

Установка флага **Добавлять префикс к полю Subject писем, содержащих спам** указывает сторожу **SpIDer Mail** добавлять специальный префикс к темам писем, распознаваемых как спам. Этот префикс задается в поле, расположенном ниже. Добавление префикса поможет вам создать правила для фильтрации почтовых сообщений, помеченных как спам, в тех почтовых клиентах (например MS Outlook Express), в которых невозможно настроить фильтры по заголовкам писем.

Флаг **Разрешать текст на кириллице** указывает антиспам-фильтру не причислять письма, написанные с установленной кириллической кодировкой, к спаму без предварительного анализа. Если флаг снят, то такие письма с большой вероятностью будут оценены фильтром как спам.

Установка и снятие флага **Разрешать текст на китайском/японском/корейском языках** работает аналогично.

Поля **Белый список** и **Черный список** содержат "черные" и "белые" списки адресов отправителей почтовых сообщений.

- Если адрес отправителя добавлен в "белый" список, письмо не подвергается анализу на содержание спама. Однако, если доменное имя адресов получателя и отправителя письма совпадают, и это доменное имя занесено в белый список с использованием знака "*", то письмо подвергается проверке на спам.

  ▸ Методы заполнения списка

  - чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, `mail@example.net`). Все письма, полученные с этого адреса, будут доставляться без проверки на спам;
  - разные почтовые адреса разделяются с помощью знака ";"
  - чтобы добавить в список отправителей адреса определенного вида, введите маску, определяющую данные адреса. Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в почтовых адресах, а также специальный символ *, который заменяет любую (в том числе пустую) последовательность любых символов.

    Например, допускаются следующие варианты:

    - `mailbox@domain.com`
    - `*box@domain.com`
    - `mailbox@dom*`
    - `*box@dom*`

Знак * может ставиться только в начале или в конце адреса.

Символ @ обязателен.

- чтобы гарантированно получать письма с почтовых адресов в конкретном домене, используйте символ * вместо имени пользователя. Например, чтобы получать все письма от адресатов из домена example.net, введите *@example.net.
- чтобы гарантированно получать письма с почтовых адресов с конкретным именем пользователя с любого домена, используйте символ * вместо имени домена. Например, чтобы получать все письма от адресатов с названием почтового ящика ivanov, введите ivanov@*.

- Если адрес отправителя добавлен в "черный" список, то письму без дополнительного анализа присваивается статус спам.

  ▸ Методы заполнения списка

  - чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, spam@spam.ru). Все письма, полученные с этого адреса, будут автоматически распознаваться как спам;
  - разные почтовые адреса разделяются с помощью знака ";"
  - чтобы добавить в список отправителей адреса определенного вида, введите маску, определяющую данные адреса. Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в почтовых адресах, а также специальный символ *, который заменяет любую (в том числе пустую) последовательность любых символов.

    Например, допускаются следующие варианты:

    - mailbox@domain.com
    - *box@domain.com

- `mailbox@dom*`
- `*box@dom*`

Знак * может ставиться только в начале или в конце адреса.

Символ @ обязателен.

- чтобы гарантированно помечать как спам письма с почтовых адресов в конкретном домене, используйте символ * вместо имени пользователя. Например, чтобы помечать как спам все письма от адресатов из домена `spam.ru`, введите `*@spam.ru`;
- чтобы гарантированно помечать как спам письма с почтовых адресов с конкретным именем пользователя с любого домена, используйте символ * вместо имени домена. Например, чтобы помечать как спам все письма от адресатов с названием почтового ящика `ivanov`, введите `ivanov@*`.
- адреса из домена получателя не обрабатываются. Например, если почтовый ящик получателя (ваш почтовый ящик) находится в домене `mail.ru`, то адреса отправителей с домена `mail.ru` обрабатываться спам-фильтром не будут.

Ко всем проверенным письмам будет добавляться заголовки:

- **X-DrWeb-SpamState: Yes/No**. Значение **Yes** показывает, что письму присвоен статус спам, **No** – письмо по мнению **SpIDer Mail** спамом не является.
- **X-DrWeb-SpamVersion: version**. **version** – версия библиотеки антиспам-фильтра **Vade Retro**.

Если какие-либо письма неправильно распознаются спам-фильтром, следует пересылать их на специальные почтовые адреса, для анализа и повышения качества работы фильтра. Письма, ошибочно оцененные как спам, отправляйте на адрес vrnonspam@drweb.com, а спам, не распознанный системой - на адрес vrspam@drweb.com. Все сообщения следует пересылать только в виде вложения (а не в теле письма).

10.2.1.2. Дополнительные настройки режима проверки

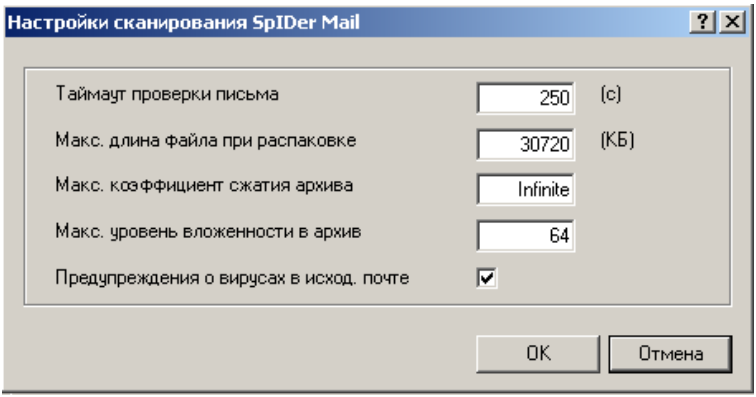

Рисунок 10-3. Окно настроек SpIDer Mail.

В данном окне задаются дополнительные настройки режима проверки электронной почты.

Следующая группа настроек задает условия, при выполнении которых сложно-составные письма, проверка которых является чрезмерно трудоемкой, признаются непроверенными:

- **Таймаут проверки письма** – максимальное время, в течение которого письмо проверяется. По истечении указанного времени проверка письма будет прекращаться;
- **Макс. длина файла при распаковке** – если почтовый

сторож определяет, что после распаковки архив будет больше указанной длины, проверка и распаковка производиться не будет;

- **Макс. коэффициент сжатия архива** – если почтовый сторож определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка производиться не будет;
- **Макс. уровень вложенности в архив** – если уровень вложенности в архив превышает указанный, проверка будет производиться только до указанного уровня вложенности.

Флаг **Предупреждения о вирусах в исход. почте** по умолчанию установлен. При этом будет показано информационное окно, сообщающее об отказе доставить на SMTP-сервер зараженное письмо. Как правило, аналогичное сообщение формируется также почтовой программой; в этом случае флаг можно снять.

10.2.2. Вкладка Действия

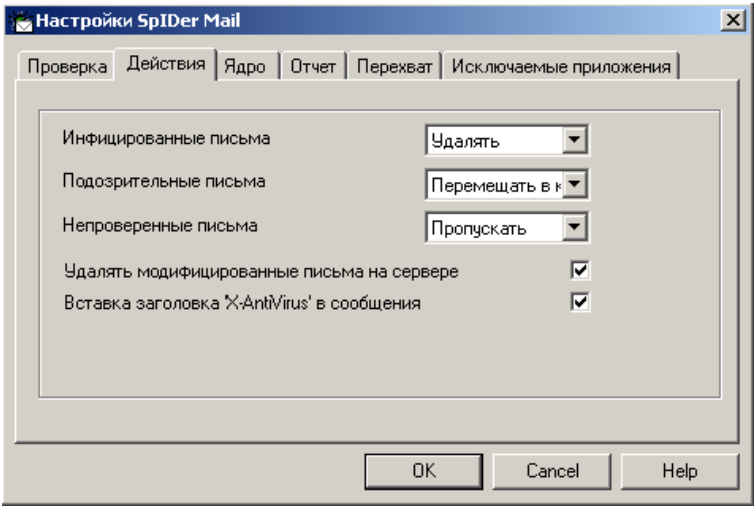

Рисунок 10-4. Окно настроек SpIDer Mail. Вкладка Действия. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На данной вкладке задаются реакции сторожа **SpIDer Mail** на обнаружение зараженных или подозрительных файлов в электронной почте.

Настройка действий

Для задания действий над обнаруженными вредоносными объектами служат следующие настройки:

- Выпадающий список **Инфицированные письма** задает реакцию **SpIDer Mail** на обнаружение письма, содержащего вредоносный объект.
- Выпадающий список **Подозрительные письма** задает реакцию **SpIDer Mail** на обнаружение письма,

предположительно содержащего вирус (срабатывание эвристического анализатора).

- Выпадающий список **Непроверенные письма** задает реакцию **SpIDer Mail** на обнаружение писем, проверка которых не могла быть завершена.

Флаг **Удалять модифицированые письма на сервере** по умолчанию установлен. В этом случае входящие письма, для которых была применена реакция **Удалять** или **В карантин**, удаляются с POP3/IMAP4-сервера, независимо от настроек почтовой программы.

При установке флага **Вставка заголовка 'X-AntiVirus' в сообщения** ко всем проверенным письмам будет добавляться заголовки:

- **X-DrWeb-SpamState: Yes/No**. Значение **Yes** показывает, что письму присвоен статус спам, **No** – письмо по мнению **SpIDer Mail** спамом не является.
- **X-DrWeb-SpamVersion: version**. **version** – версия библиотеки антиспам-фильтра **Vade Retro**.

Возможные реакции

Предусмотрены следующие действия над обнаруженными объектами:

- **Удалять** – в этом случае почтовый сторож не передает письмо почтовому клиенту. Вместо удаленного письма почтовой программе передается сообщение о совершенной операции.
- **В карантин** – в этом случае письмо также не передается почтовой программе, а перемещается в каталог Карантина. Вместо перемещенного письма почтовой программе передается сообщение о совершенной операции.
- **Пропускать –** передавать письма почтовой программе как обычно.

Для исходящих писем любая настройка, кроме **Пропускать**, приводит к отказу в передаче письма на SMTP-сервер.

Таблица 7. Действия SpIDer Mail при проверке электронной почты

Объект	Действие		
	Удалять	В карантин	Пропускать
Инфицированные письма	+	+/*	
Подозрительные письма	+	+/*	+
Непроверенные письма	+	+	+/*

Условные обозначения

+	действие разрешено для данного типов объектов
+/*	действие установлено как реакция по умолчанию для данного типов объектов

10.2.3. Вкладка Ядро

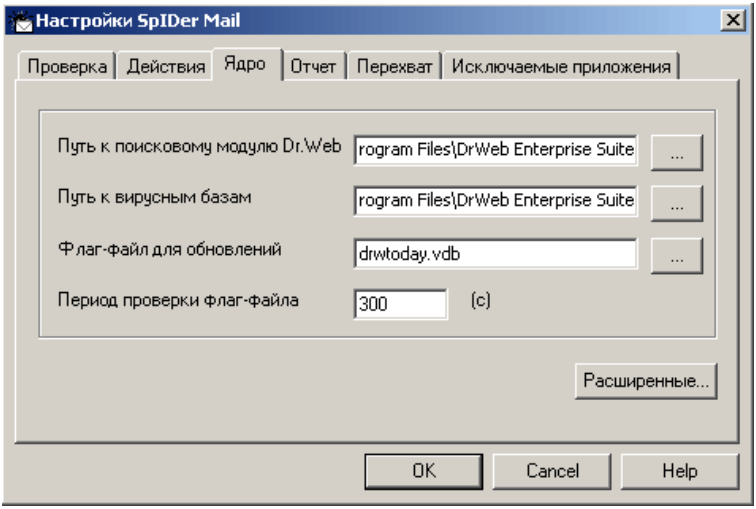

Рисунок 10-5. Окно настроек SpIDer Mail. Вкладка Ядро. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На данной вкладке задаются параметры работы антивирусного ядра.

При необходимости вы можете задать нестандартное расположение антивирусного ядра (поискового модуля) и вирусных баз.

Если во время сеанса работы сторожа произошло обновление вирусных баз при помощи **Модуля обновления**, сторож немедленно загружает обновленные базы. Если обновление баз произошло другим путем (например, прямым копированием баз в каталог установки), сторож также может загрузить обновленные базы без перезагрузки программы. Для этого служит механизм периодической проверки флаг-файла (по умолчанию "горячего обновления" базы). Изменение флаг-файла свидетельствует о необходимости перезагрузки баз. Вы можете задать имя и

расположение флаг-файла, а также период между очередными проверками (по умолчанию 300 секунд).

Нажмите на кнопку **Расширенные**, чтобы задать дополнительные настройки антивирусного ядра.

10.2.3.1. Дополнительные настройки поисковых модулей

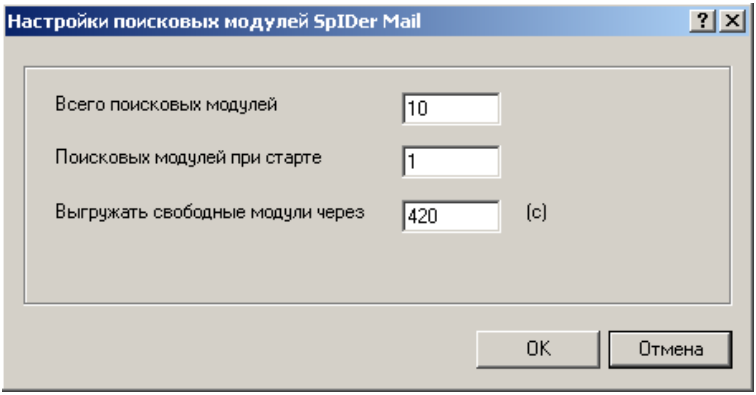

Рисунок 10-6. Окно настроек SpIDer Mail.

В данном окне задаются дополнительные настройки поисковых модулей:

- В поле **Всего поисковых модулей** задается максимальное количество одновременно загружаемых поисковых модулей.
- В поле **Поисковых модулей при старте** задается количество поисковых модулей, загружаемых при старте **SpIDer Mail**.
- В поле **Выгружать свободные модуле через** задается время в секундах, по истечении которого выгружается неиспользуемый поисковый модуль.

10.2.4. Вкладка Отчет

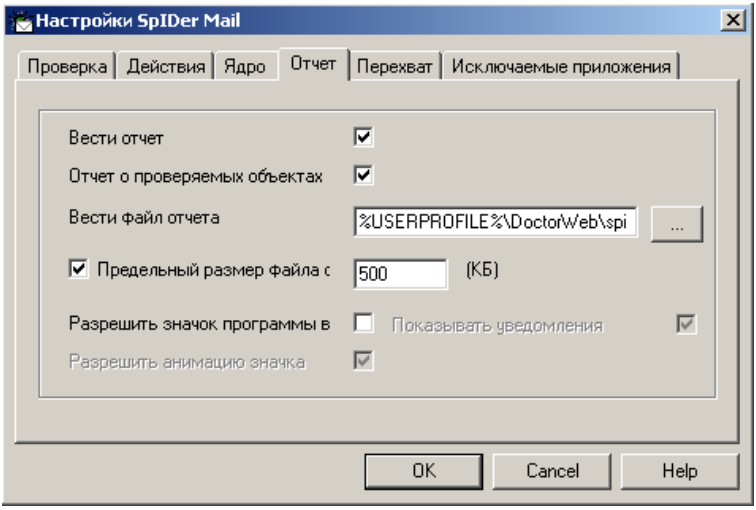

Рисунок 10-7. Окно настроек SpIDer Mail. Вкладка Отчет. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На данной вкладке задаются параметры ведения файла отчета по работе **SpIDer Mail**.

Флаг **Вести отчет** предписывает сторожу **SpIDer Mail** вести файла отчета. По умолчанию флаг установлен.

Вы можете настроить следующие параметры файла отчета:

- Установите флаг **Отчет о проверяемых объектах**, чтобы включать в отчет сведения обо всех проверенных объектах, включая незараженные.
- В поле **Вести файл отчета** вы можете задать имя и путь к файлу отчета. Нажмите кнопку ..., чтобы указать объект в файловом браузере по операционной системе.

- Установите флаг **Предельный размер файла отчета**, чтобы ограничить максимальный размер отчета и укажите предельно допустимый размер в килобайтах.

Также вы можете задать дополнительные параметры:

- Установите флаг **Разрешить значок программы**, чтобы отображать иконку **SpIDer Mail** в области уведомления Панели задач.
- Установите флаг **Разрешить анимацию значка** для того, чтобы разрешить анимацию иконки **SpIDer Mail** в области уведомленияПанели задач.
- Установите флаг **Показывать уведомления**, чтобы разрешить отображение над значком **SpIDer Mail** всплывающей подсказки-уведомления, содержащей информацию о версии программы, количестве вирусных записей и т.д. Подсказка-уведомление появляется сразу после запуска программы.

10.2.5. Вкладка Перехват

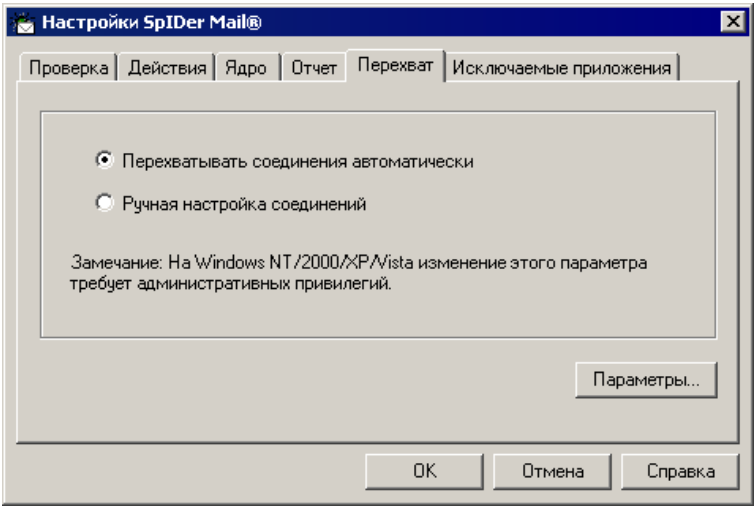

Рисунок 10-8. Окно настроек SpIDer Mail. Вкладка Перехват. Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На данной вкладке задаются параметры перехвата соединений с POP3/SMTP/IMAP4/NNTP-серверами.

Выберите режим перехвата:

- автоматический режим является наиболее удобным;
- ручной режим следует использовать в тех случаях, если автоматический режим невозможен для всех или некоторых перехватываемых адресов серверов (для всех адресов должен применяться один и тот же режим).

После выбора режима нажмите на кнопку **Параметры**. Откроется окно настройки перехвата в выбранном режиме.

10.2.5.1. Автоматический перехват

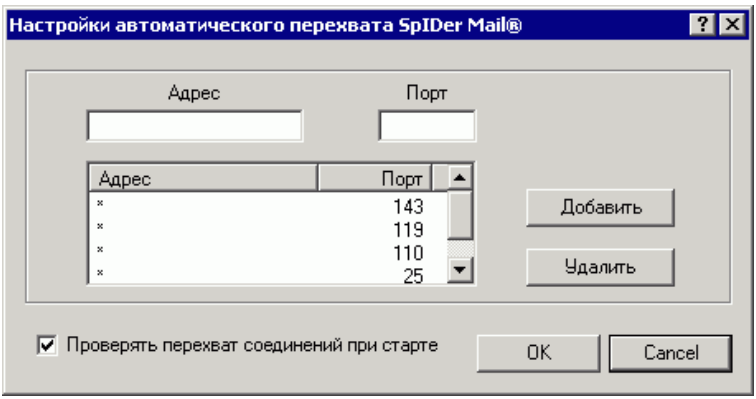

Рисунок 10-9. Окно настройки автоматического перехвата SpIDer Mail.

В данном окне задаются настройки перехвата в автоматическом режиме.

Список перехватываемых адресов почтовых серверов содержит по умолчанию четыре элемента:

- любые адреса с портом 143 – стандартные IMAP4-сервера,
- любые адреса с портом 119 – стандартные NNTP-сервера,
- любые адреса с портом 110 – стандартные POP3-сервера,
- любые адреса с портом 25 – стандартные SMTP-сервера.

Вы можете редактировать этот список:

1. Для добавления элемента в список, введите соответствующие данные в поля **Адрес** и **Порт** и нажмите кнопку **Добавить**.
2. Для удаления элемента из списка, выделите нужный элемент в списке и нажмите кнопку **Удалить**.

Установленный по умолчанию флаг **Проверять перехват соединений при старте** предписывает программе тестирование

работы автоматического перехвата. Если будет обнаружена неработоспособность автоматического перехвата хотя бы для одного соединения, перейдите в ручной режим перехвата.

10.2.5.2. Ручной перехват

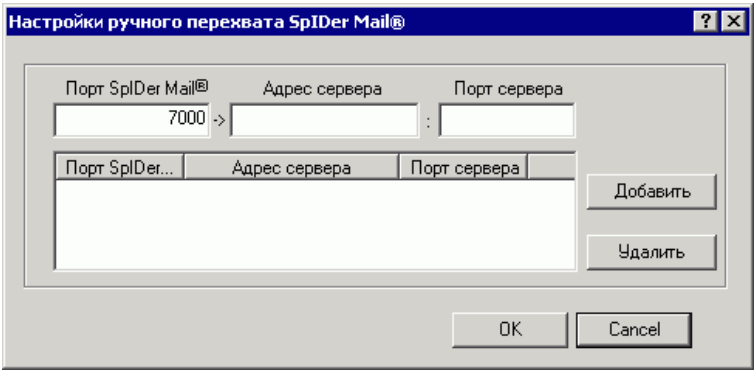

Рисунок 10-10. Окно настройки ручного перехвата SpIDer Mail.

В данном окне задаются настройки ручного перехвата подключений к почтовым серверам. В данном режиме почтовый сторож **SpIDer Mail** выступает в роли прокси-сервера между почтовыми программами и почтовыми серверами и отслеживает только те соединения, которые указаны в настройках в явном виде. Использование данного типа перехвата требует изменения настроек подключения почтовых программ.

Список перехватываемых адресов состоит из записей, каждая из которых устанавливает соответствие между настройками почтового сторожа **SpIDer Mail** и почтового сервера.

По умолчанию список перехвата пуст. Вы можете добавить в него необходимые записи.

Настройка перехвата соединений вручную

1. Составьте список почтовых серверов, обращения к которым вы хотите перехватывать, и задайте номера портов для этих серверов в возрастающем порядке без пропусков. Рекомендуется начинать нумерацию с числа 7000. Эти номера далее будут именоваться *портами SpIDer Mail*.

Почтовый сторож **SpIDer Mail** поддерживает почтовые сервера, работающие по протоколам POP3, SMTP, IMAP4 или NNTP.

2. В настройках почтового сторожа **SpIDer Mail** выберите раздел **Перехват**.
3. Выберите ручной режим перехвата и нажмите соответствующую кнопку **Настройки соединения**.
4. В открывшемся диалоговом окне введите следующую информацию:
   - в поле **Порт SpIDer Mail** – *порт SpIDer Mail*, выбранный для почтового сервера;
   - в поле **Адрес сервера** – доменное имя или IP-адрес почтового сервера;
   - в поле **Порт сервера** – номер порта, который использует почтовый сервер.
5. Нажмите кнопку **Добавить**.
6. При необходимости повторите шаги 4 и 5 для других серверов. Чтобы прекратить перехватывать подключения к серверу, выберите соответствующий элемент в списке и нажмите кнопку **Удалить**.
7. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.
8. Настройте почтовый клиент на работу с почтовым сторожем **SpIDer Mail** при перехвате соединений вручную.

Настройка почтового клиента

Если **SpIDer Mail** использует для перехвата соединений ручные настройки, измените настройки вашего почтового клиента соответствующим образом:

- в качестве адреса сервера входящей и исходящей почты укажите `localhost`;
- в качестве порта почтового сервера укажите *порт SpIDer Mail*, назначенный вами для соответствующего почтового сервера.

Как правило, для этого необходимо в настройках адреса почтового сервера указать:

`localhost`:**<***порт_SpIDer_Mail***>**

где <*порт_SpIDer_Mail*> – порт, назначенный вами соответствующему почтовому серверу.

Например.

Если почтовому серверу с адресом `pop.mail.ru` и портом `110` назначен *порт SpIDer Mail* `7000`, то в настройках почтового клиента необходимо указать `localhost` в качестве севера входящей почты и `7000` в качестве порта.

10.2.6. Вкладка Исключаемые приложения

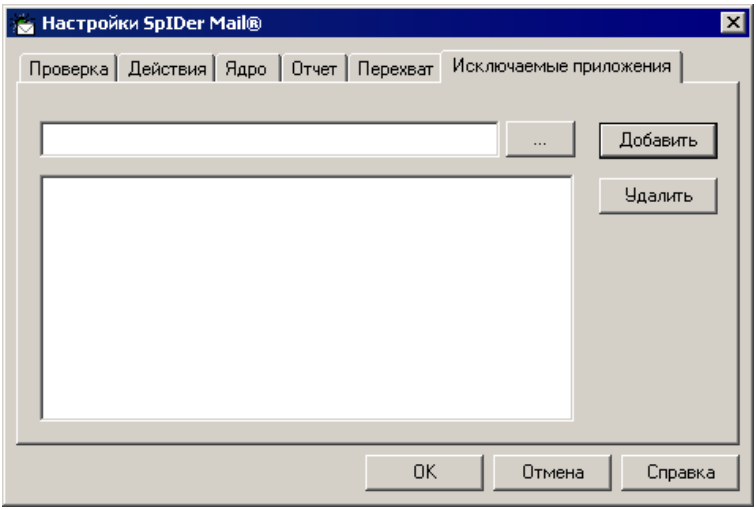

Рисунок 10-11. Окно настроек SpIDer Mail. Вкладка Исключаемые приложения.

Чтобы получить справку о параметрах на другой вкладке, щелкните по названию этой вкладки на рисунке

На данной вкладке задается список приложений, почтовый трафик которых не будет перехватываться и, соответственно, анализироваться почтовым сторожем.

Для того чтобы настроить список приложений:

1. Введите путь к исполняемому файлу приложения. Вы также можете воспользоваться кнопкой ... и выбрать объект в файловом браузере по операционной системе.
2. Нажмите на кнопку **Добавить**. Приложение будет добавлено в список, расположенный ниже.

3. Для того чтобы удалить какое-либо приложение из списка, выберите его исполняемый файл в этом списке и нажмите на кнопку **Удалить**.

Глава 11. Dr.Web для Outlook

Основные функции компонента

Подключаемый модуль **Dr.Web для Outlook** выполняет следующие функции:

- антивирусная проверка вложенных файлов почтовых сообщений;
- проверка почты, поступающей по зашифрованному соединению SSL;
- проверка почтовых сообщений на спам;
- обнаружение и нейтрализацию вредоносного программного обеспечения;
- использование эвристического анализатора для дополнительной защиты от неизвестных вирусов.

Включение/Выключение

Включение и выключение модуля **Dr.Web для Outlook** осуществляется при помощи контекстного меню **Агента**.

Настройка модуля Dr.Web для Outlook

Настройка параметров и просмотр статистики работы программы осуществляется в почтовом приложении Microsoft Outlook в разделе **Сервис** → **Параметры** → вкладка **Антивирус Dr.Web**.

Вкладка **Dr.Web Anti-Virus** в настройках приложения Microsoft Outlook доступна только при наличии у пользователя прав, позволяющих изменять данные настройки. Права устанавливаются на **Сервере** администратором антивирусной сети.

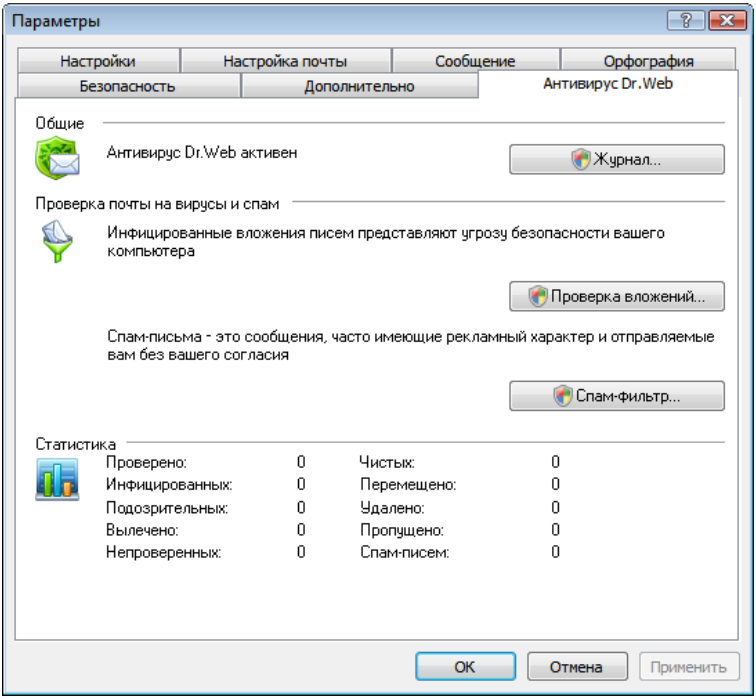

Рисунок 11-1. Окно настроек Microsoft Outlook. Вкладка Антивирус Dr.Web.

На вкладке **Антивирус Dr.Web** отображается текущее состояние защиты (включена/выключена) и предоставляется доступ к следующим функциям программы:

- Журнал - позволяет настроить регистрацию событий программы;
- Проверка вложений - позволяет настроить проверку электронной почты и определить действия программы для обнаруженных вредоносных объектов;
- Спам-фильтр - позволяет определить действия программы для спам-сообщений, а также создать белый и черный списки электронных адресов;

- Статистика - показывает данные об объектах, проверенных и обработанных программой.

11.1. Проверка на вирусы

Dr.Web для Outlook использует различные методы обнаружения вирусов. К найденным вредоносным объектам применяются определяемые пользователем действия: программа может лечить инфицированные объекты, удалять их или перемещать в Карантин для их изоляции и безопасного хранения.

11.1.1. Вредоносные объекты

Программа **Dr.Web для Outlook** обнаруживает следующие вредоносные объекты:

- инфицированные архивы;
- файлы-бомбы или архивы-бомбы;
- рекламные программы;
- программы взлома;
- программы дозвона;
- программы-шутки;
- потенциально опасные программы.

11.1.2. Действия

Dr.Web для Outlook позволяет задать реакцию программы на обнаружение зараженных или подозрительных файлов и вредоносных программ при проверке вложений электронной почты.

Чтобы настроить проверку вложений и определить действия программы для обнаруженных вредоносных объектов, в почтовом приложении Microsoft Outlook в разделе **Сервис** → **Параметры** →

вкладка **Антивирус Dr.Web** нажмите кнопку **Проверка вложений**.

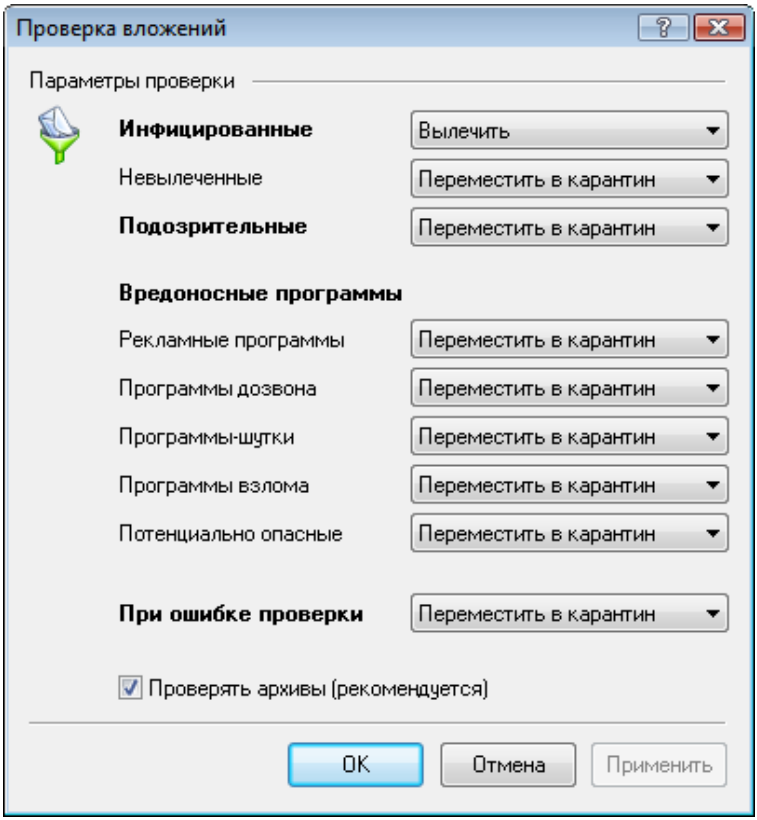

Рисунок 11-2. Окно настроек проверки вложений.

Окно **Проверка вложений** доступно только при наличии у пользователя прав администратора системы.

Для ОС Windows Vista и старше при нажатии кнопки **Проверка вложений**:

- При включенном UAC: администратору будет выдан запрос на подтверждение действий программы, пользователю без административных

прав будет выдан запрос на ввод учетных данных администратора системы.

- При выключенном UAC: администратор сможет изменять настройки программы, пользователь не сможет получить доступ к изменению настроек.

В окне **Проверка вложений** вы можете задать действия программы для различных категорий проверяемых объектов, а также для случая, когда при проверке возникли ошибки. Кроме того, вы можете настроить проверку архивов.

Для задания действий над обнаруженными вредоносными объектами служат следующие настройки:

- Выпадающий список **Инфицированные** задает реакцию на обнаружение объектов, зараженных известными и (предположительно) излечимыми вирусами.
- Выпадающий список **Невылеченные** задает реакцию на обнаружение объектов, зараженных известным неизлечимым вирусом, а также когда предпринятая попытка излечения не принесла успеха.
- Выпадающий список **Подозрительные** задает реакцию на обнаружение объектов, предположительно зараженных вирусом (срабатывание эвристического анализатора).
- Раздел **Вредоносные программы** задает реакцию на обнаружение следующего нежелательного ПО:
  - рекламные программы;
  - программы дозвона;
  - программы шутки;
  - программы взлома;
  - потенциально опасные.
- Выпадающий список **При ошибке проверки** позволяет настроить действия программы в случае, если проверка вложения не возможна, например, если оно представляет собой поврежденный или защищенный паролем файл.

- Флаг **Проверка архивов** позволяет включить или отключить проверку вложенных файлов, представляющих собой архивы. Установите данный флаг для включения проверки, снимите - для отключения.

Состав доступных реакций зависит от типа вирусного события.

Предусмотрены следующие действия над обнаруженными объектами:

- **Вылечить** - означает, что программа предпримет попытку вылечить инфицированный объект;
- **Как для невылеченных** - означает, что к инфицированному вложению будет применено действие, выбранное для невылеченных объектов;
- **Удалить** - удалить объект из системы;
- **Переместить в карантин** - изолировать объект в каталоге Карантина;
- **Пропустить** - пропустить объект без изменений.

Таблица 8. Действия над обнаруженными вредоносными объектами

Объект	Действие				
	Вылечить	Как для невылеченных	Удалить	Переместить в карантин	Пропустить
Инфицированные	+/*	+			
Невылеченные			+	+/*	
Подозрительные			+	+/*	+
Рекламные программы			+	+/*	+
Программы дозвона			+	+/*	+
Программы-шутки			+	+/*	+

Объект	Действие				
	Вылечить	Как для невылеченных	Удалить	Переместить в карантин	Пропустить
Программы взлома			+	+/*	+
Потенциально опасные			+	+/*	+
При ошибке проверки			+	+/*	+

Условные обозначения

+	действие разрешено для данного типов объектов
+/*	действие установлено как реакция по умолчанию для данного типов объектов

11.2. Проверка на спам

Dr.Web для Outlook проверяет на спам все почтовые сообщения с помощью спам-фильтра **Vade Retro** и осуществляет фильтрацию сообщений в соответствии с настройками, задаваемыми пользователем.

Чтобы настроить проверку сообщений на спам, в почтовом приложении Microsoft Outlook в разделе **Сервис** → **Параметры** → вкладка **Антивирус Dr.Web** нажмите кнопку **Спам-фильтр**. Откроется окно настроек Спам фильтра.

Раздел **Спам-фильтр** доступен только в том случае, если **Dr.Web Agent** работает с лицензией «Антивирус +антиспам».

Если лицензия не поддерживает использование спам-фильтра, настройки проверки на спам будут недоступны, и сама проверка сообщений на спам осуществляться не будет.

Окно **Спам-фильтр** доступно только при наличии у пользователя прав администратора системы.

Для ОС Windows Vista и старше при нажатии кнопки **Спам-фильтр**:

- При включенном UAC: администратору будет выдан запрос на подтверждение действий программы, пользователю без административных прав будет выдан запрос на ввод учетных данных администратора системы.
- При выключенном UAC: администратор сможет изменять настройки программы, пользователь не сможет получить доступ к изменению настроек.

11.2.1. Настройка спам-фильтра

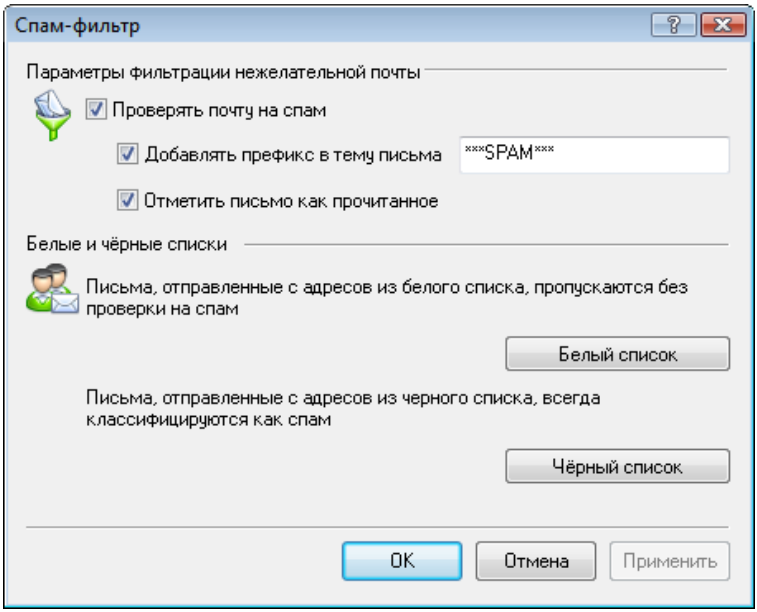

Рисунок 11-3. Окно настроек спам фильтра.

Для настройки параметров спам-фильтра:

- Установите флаг **Проверять почту на спам** для активации спам-фильтра.
- Если вы хотите добавлять специальный текст в заголовок сообщения, распознанного как спам, установить флаг **Добавлять префикс в тему письма**. Добавляемый текст можно ввести в текстовом поле справа от флага. По умолчанию добавляется префикс ***SPAM***.
- Проверенные сообщения могут отмечаться как прочитанные в свойствах письма. Для этого необходимо установить флаг **Отметить письмо как прочитанное**. По умолчанию флаг **Отметить как прочитанное** установлен.
- Также вы можете настроить белые и черные списки для фильтрации писем.

Если некоторые письма были неправильно распознаны, следует отправить их на специальные почтовые адреса для анализа и повышения качества работы фильтра.

▸ Подробнее

- Письма, ошибочно принятые за спам, следует отправлять на адрес vrnonspam@drweb.com;
- Нераспознанные и пропущенные спам-сообщения следует отправлять на адрес vrspam@drweb.com.

Все сообщения необходимо высылать только в виде вложения (а не в теле письма).

11.2.2. Черный и белый списки

Черный и белый списки электронных адресов служат для фильтрации сообщений.

Для просмотра и редактирования черного или белого списка, в настройках спам-фильтра, нажмите кнопку **Черный список** или **Белый список** соответственно.

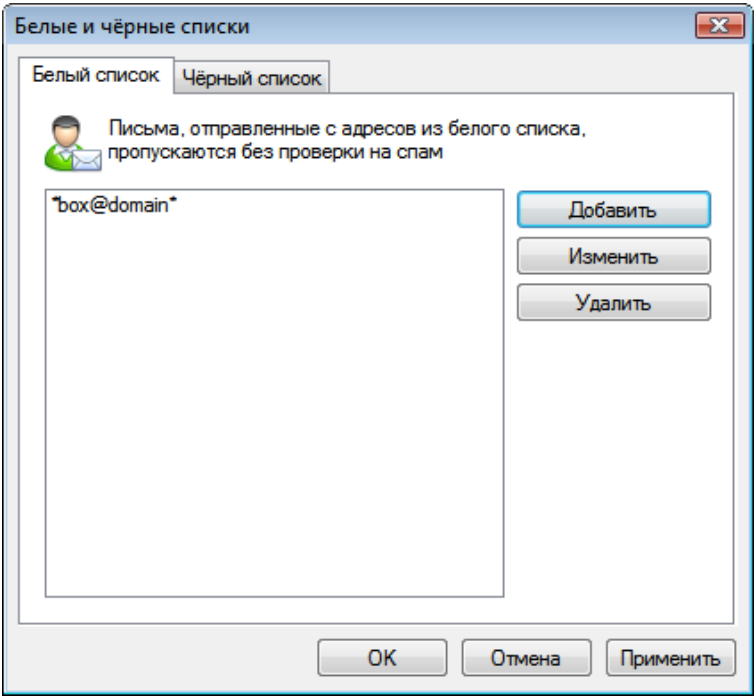

Рисунок 11-4. Окно настроек белого списка спам фильтра.

Чтобы добавить адрес в черный или белый список:

1. Нажмите кнопку **Добавить**.
2. Введите электронный адрес в соответствующее поле (см. методы заполнения белого и черного списков).
3. Нажмите кнопку **ОК** в окне **Редактировать список**.

Чтобы изменить адреса в списке:

1. Выберите адрес в списке, нажмите кнопку **Изменить**.
2. Отредактируйте необходимую информацию.

3. Нажмите **ОК** в окне **Редактировать список**.

Чтобы удалить адрес из списка:

1. Выберите адрес в списке.
2. Нажмите кнопку **Удалить**.

В окне **Белые и Черные списки** нажмите **ОК**, чтобы сохранить внесенные изменения.

Белый список

Если адрес отправителя добавлен в "белый" список, письмо не подвергается анализу на содержание спама. Однако, если доменное имя адресов получателя и отправителя письма совпадают, и это доменное имя занесено в белый список с использованием знака "*", то письмо подвергается проверке на спам.

▸ Методы заполнения списка

- чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, `mail@example.net`). Все письма, полученные с этого адреса, будут доставляться без проверки на спам;
- каждый элемент списка может содержать только один почтовый адрес или одну маску почтовых адресов;
- чтобы добавить в список отправителей адреса определенного вида, введите маску, определяющую данные адреса. Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в почтовых адресах, а также специальный символ *, который заменяет любую (в том числе пустую) последовательность любых символов.

  Например, допускаются следующие варианты:

  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

Знак * может ставиться только в начале или в конце адреса.

Символ @ обязателен.

- чтобы гарантированно получать письма с почтовых адресов в конкретном домене, используйте символ * вместо имени пользователя. Например, чтобы получать все письма от адресатов из домена `example.net`, введите `*@example.net`
- чтобы гарантированно получать письма с почтовых адресов с конкретным именем пользователя с любого домена, используйте символ * вместо имени домена. Например, чтобы получать все письма от адресатов с названием почтового ящика `ivanov`, введите `ivanov@*`.

Черный список

Если адрес отправителя добавлен в "черный" список, то письму без дополнительного анализа присваивается статус спам.

▸ Методы заполнения списка

- чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, `spam@spam.ru`). Все письма, полученные с этого адреса, будут автоматически распознаваться как спам;
- каждый элемент списка может содержать только один почтовый адрес или одну маску почтовых адресов;
- чтобы добавить в список отправителей адреса определенного вида, введите маску, определяющую данные адреса. Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в почтовых адресах, а также специальный символ *, который заменяет любую (в том числе пустую) последовательность любых символов.

  Например, допускаются следующие варианты:

  - `mailbox@domain.com`

- `*box@domain.com`
- `mailbox@dom*`
- `*box@dom*`

Знак `*` может ставиться только в начале или в конце адреса.

Символ `@` обязателен.

- чтобы гарантированно помечать как спам письма с почтовых адресов в конкретном домене, используйте символ `*` вместо имени пользователя. Например, чтобы помечать как спам все письма от адресатов из домена `spam.ru`, введите `*@spam.ru`;
- чтобы гарантированно помечать как спам письма с почтовых адресов с конкретным именем пользователя с любого домена, используйте символ `*` вместо имени домена. Например, чтобы помечать как спам все письма от адресатов с названием почтового ящика `ivanov`, введите `ivanov@*`.
- адреса из домена получателя не обрабатываются. Например, если почтовый ящик получателя (ваш почтовый ящик) находится в домене `mail.ru`, то адреса отправителей с домена `mail.ru` обрабатываться спам-фильтром не будут.

11.3. Регистрация событий

Dr.Web для Outlook регистрирует ошибки и происходящие события в следующих журналах регистрации:

- журнале регистрации событий операционной системы (Event Log);
- текстовом журнале отладки.

11.3.1. Журнал операционной системы

В журнал регистрации операционной системы (Event Log) заносится следующая информация:

- сообщения о запуске и остановке программы;
- параметры лицензионного ключевого файла: действительность или недействительность лицензии, срок действия лицензии (информация заносится при запуске программы, в процессе ее работы и при замене лицензионного ключевого файла);
- параметры модулей программы: сканера, ядра, вирусных баз (информация заносится при запуске программы и при обновлении модулей);
- сообщение о недействительности лицензии: отсутствие ключевого файла, отсутствие в ключевом файле разрешения на использование модулей программы, лицензия заблокирована, нарушение целостности ключевого файла (информация заносится при запуске программы и в процессе ее работы);
- сообщения об обнаружении вирусов;
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 дней до окончания срока).

Чтобы просмотреть журнал регистрации событий операционной системы:

1. Откройте **Панель управления** операционной системы.
2. Выберите раздел **Администрирование** → **Просмотр Событий**.
3. В левой части окна **Просмотр Событий** выберите пункт **Приложение**. Откроется список событий, зарегистрированных в журнале пользовательскими приложениями. Источником сообщений **Dr.Web для Outlook** является приложение **Dr.Web for Outlook**.

11.3.2. Текстовый журнал отладки

В текстовый журнал отладки заносится следующая информация:

- сообщения о действительности или недействительности лицензии;
- сообщения об обнаружении вирусов;
- сообщения об ошибках записи или чтения файлов, ошибках анализа архивов или файлов, защищенных паролем;
- параметры модулей программы: сканера, ядра, вирусных баз;
- сообщения об экстренных остановах ядра программы;
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 дней до окончания срока).

Ведение текстового журнала программы приводит к снижению быстродействия системы, поэтому рекомендуется включать регистрацию событий только в случае возникновения ошибок работы приложения **Dr.Web для Outlook**.

Настройка регистрации событий

1. На вкладке **Антивирус Dr.Web** нажмите кнопку **Журнал**. Откроется окно настроек журнала.
2. Выберите уровень детализации (от 0 до 5) для записи событий:
   - уровень **0** означает, что регистрация событий в текстовом журнале отладки не ведется,
   - уровень **5** соответствует максимальной детализации регистрируемых событий.

   По умолчанию регистрация событий отключена.
3. Задайте максимальный размер (в килобайтах) файла журнала.
4. Нажмите кнопку **ОК** для сохранения изменений.

Окно **Журнал** доступно только при наличии у пользователя прав администратора системы.

Для ОС Windows Vista и старше при нажатии кнопки **Журнал**:

- При включенном UAC: администратору будет выдан запрос на подтверждение действий программы, пользователю без административных прав будет выдан запрос на ввод учетных данных администратора системы.
- При выключенном UAC: администратор сможет изменять настройки программы, пользователь не сможет получить доступ к изменению настроек.

Просмотр журнала событий программы

Для просмотра текстового журнала событий программы нажмите кнопку **Показать в папке**. Откроется каталог, в котором хранится журнал.

По умолчанию журнал сохраняется в файле `DrWebOutlook.log`, расположенном в профиле пользователя в каталоге `DoctorWeb`.

Файл журнала `DrWebOutlook.log` ведется отдельно для каждого пользователя системы.

11.4. Статистика

В почтовом приложении Microsoft Outlook в разделе **Сервис** → **Параметры** → вкладка **Антивирус Dr.Web** содержится статистическая информация об общем количестве объектов, проверенных и обработанных программой.

Объекты разделяются на следующие категории:

- **Проверено** - общее количество проверенных писем.

- **Инфицированных** - количество писем, содержащие вирусы.
- **Подозрительных** - количество писем, предположительно зараженных вирусом (срабатывание эвристического анализатора).
- **Вылечено** - количество объектов, успешно вылеченных программой.
- **Непроверенных** - количество объектов, проверка которых невозможна или при проверке возникли ошибки.
- **Чистых** - количество писем, не содержащие вредоносных объектов.

Затем указывается количество объектов, которые были:

- **Перемещено** - количество объектов, перемещенных в Карантин.
- **Удалено** - количество объектов, удаленных из системы.
- **Пропущено** - количество объектов, пропущенных без изменений.
- **Спам-писем** - количество писем, распознанных как спам.

Файл статистики

По умолчанию статистика сохраняется в файле `drwebforoutlook.stat`, расположенном в профиле пользователя в каталоге `DoctorWeb`. Для очистки статистики необходимо удалить данный файл.

Файл статистики `drwebforoutlook.stat` ведется отдельно для каждого пользователя системы.

Статистика приложения **Dr.Web для Outlook** передается **Агенту** для отправки на **Сервер** вместе со статистикой остальных антивирусных компонентов **Dr.Web Enterprise Security Suite**.

Приложение А. Ключи командной строки для Dr.Web Сканера NT4

В данном разделе приведены ключи командной строки для **Dr.Web Сканера NT4**.

Ключи для **Dr.Web Сканера** приведены в Руководстве **Антивирус Dr.Web для Windows**, в подразделе **Приложения А**: **Ключи для Сканера и Консольного Сканера**.

При выполнении задания на сканирование запускается **Сканер Dr.Web**. При необходимости можно указать дополнительные параметры проверки. В поле ввода **Аргументы** вы можете указать следующие ключи (через пробел):

- **/@**<*имя_файла*> или **/@+**<*имя_файла*> – предписывает произвести проверку объектов, которые перечислены в указанном файле. Каждый объект задается в отдельной строке файла-списка. Это может быть либо полный путь с указанием имени файла, либо строка `?boot`, означающая проверку загрузочных секторов, а для GUI-версии **Сканера** также имена файлов с маской и имена каталогов. Файл-список может быть подготовлен с помощью любого текстового редактора вручную, а также автоматически прикладными программами, использующими сканер для проверки конкретных файлов. После окончания проверки сканер удаляет файл-список, если использована форма ключа без символа **+**.
- **/AL** – проверять все файлы на заданном устройстве или в заданном каталоге независимо от расширения или внутреннего формата.
- **/AR** – проверять файлы, находящиеся внутри архивов. В настоящее время обеспечивается проверка (без лечения) архивов, созданных архиваторами ARJ, PKZIP, ALZIP, AL RAR, LHA, GZIP, TAR, BZIP2, 7-ZIP, ACE и др., а также MS CAB-архивов – Windows Cabinet Files (пока не поддерживается метод упаковки QUANTUM) и ISO-образов оптических дисков

(CD и DVD). В указанном виде (**/AR**) ключ задает информирование пользователя в случае обнаружения архива, содержащего зараженные или подозрительные файлы. Если ключ дополняется модификатором **D**, **M** или **R**, производятся иные действия:

- **/ARD** – удалять;
- **/ARM** – перемещать (по умолчанию – в каталог Карантина);
- **/ARR** – переименовывать (по умолчанию первая буква расширения заменяется на символ **#**). Ключ может завершаться модификатором **N**, в таком случае не будет выводиться имя программы-архиватора после имени архивного файла.

- **/CU** – действия над инфицированными файлами и загрузочными секторами дисков. Без дополнительных параметров **D**, **M** или **R** производится лечение излечимых объектов и удаление неизлечимых файлов (если другое не задано параметром **/IC**). Иные действия выполняются только над инфицированными файлами:
  - **/CUD** – удалять;
  - **/CUM** – перемещать (по умолчанию – в каталог Карантина);
  - **/CUR** – переименовывать (по умолчанию первая буква расширения заменяется на символ **#**).
- **/DA** – проверять компьютер один раз в сутки. Дата следующей проверки записывается в файл конфигурации, поэтому он должен быть доступен для создания и последующей перезаписи.
- **/EX** – проверять файлы с расширениями, хранящимися в конфигурационном файле, по умолчанию или при недоступности конфигурационного файла это расширения EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

В случае если элемент списка проверяемых объектов содержит явное указание расширения файла, хотя бы и с применением специальных символов * и ?, будут проверены все файлы, заданные в данном элементе списка, а не только подходящие под список расширений.

- **/FN** – загружать русские буквы в знакогенератор видеоадаптера (только для **Dr.Web для DOS**).
- **/GO** – пакетный режим работы программы. Все вопросы, подразумевающие ожидание ответа от пользователя, пропускаются; решения, требующие выбора, принимаются автоматически. Этот режим полезно использовать для автоматической проверки файлов, например, при круглосуточной проверке электронной почты на сервере.
- **/HA** – производить эвристический анализ файлов и поиск в них неизвестных вирусов.
- **/ICR**, **/ICD** или **/ICM** – действия с зараженными файлами, вылечить которые невозможно:
  - **/ICR** – переименовывать,
  - **/ICD** – удалять,
  - **/ICM** – перемещать.
- **/INI**:*<путь>* – использовать альтернативный конфигурационный файл с указанным именем или путем.
- **/LNG**:*<имя_файла>* или **/LNG** – использовать альтернативный файл языковых ресурсов (`dwl`-файл) с указанным именем или путем, а если путь не указан – встроенный (английский) язык.
- **/ML** – проверять файлы, имеющие формат сообщений E-Mail (UUENCODE, XXENCODE, BINHEX и MIME). В указанном виде **(/ML)** ключ задает информирование пользователя в случае обнаружения зараженного или подозрительного объекта в почтовом архиве. Если ключ дополняется модификатором **D**, **M**, или **R**, производятся иные действия:
  - **/MLD** – удалять;
  - **/MLM** – перемещать (по умолчанию – в каталог Карантина);

- **/MLR** – переименовывать (по умолчанию первая буква расширения заменяется на символ **#**).
- Кроме того, ключ может завершаться дополнительным модификатором **N** (одновременно с этим могут быть заданы и основные модификаторы). В таком случае отключается вывод информации о почтовых файлах.

◆ **/MW** – действия со всеми видами нежелательных программ. В указанном виде (**/MW**) ключ задает информирование пользователя. Если ключ дополняется модификатором **D**, **M**, **R** или **I**, производятся иные действия:

- **/MWD** – удалять;
- **/MWM** – перемещать (по умолчанию – в каталог Карантина);
- **/MWR** – переименовывать (по умолчанию первая буква расширения заменяется на символ #);
- **/MWI** – игнорировать. Действия с отдельными видами нежелательных программ определяются с помощью ключей **/ADW**, **/DLS**, **/JOK**, **/RSK**, **/HCK**.

◆ **/NI** – не использовать параметры, записанные в конфигурационном файле программы `drweb32.ini`.

◆ **/NR** – не создавать файл отчета.

◆ **/NS** – запретить возможность прерывания проверки компьютера. После указания этого параметра пользователь не сможет прервать работу программы нажатием клавиши ESC.

◆ **/OK** – выводить полный список сканируемых объектов, сопровождая незараженные пометкой **OK**.

◆ **/PF** – запрашивать подтверждение на проверку следующей дискеты.

◆ **/PR** – выводить запрос подтверждения перед действием.

◆ **/QU** – сканер выполняет проверку указанных в командной строке объектов (файлов, дисков, каталогов), после чего автоматически завершается (только для GUI-версии **Сканера**).

◆ **/RP**<*имя_файла*> или **/RP+**<*имя_файла*> – записать отчет о работе программы в файл, имя которого указано в ключе. При отсутствии имени записать в файл по умолчанию. При

наличии символа + файл дописывается, при отсутствии – создается заново.

- **/SCP:**<*n*> – задает приоритет выполнения сканирования. <*n*> может принимать значения от 1 до 50 включительно.
- **/SD** – проверять подкаталоги.
- **/SHELL** – для GUI-версии **Сканера**. Отменяет показ заставки, отключает проверку памяти и файлов автозагрузки. Также не загружаются для проверки ранее сохраненные списки путей к проверяемым по умолчанию файлам и каталогам. Этот режим позволяет использовать GUI-версию **Сканера** вместо консольной для проверки только тех объектов, которые перечислены в параметрах командной строки.
- **/SO** – включить звуковое сопровождение.
- **/SPR**, **/SPD** или **/SPM** – действия с подозрительными файлами:
  - **/SPR** – переименовывать,
  - **/SPD** – удалять,
  - **/SPM** – перемещать.
- **/SS** – по окончании работы сохранить режимы, заданные при текущем запуске программы, в конфигурационном файле.
- **/ST** – задает скрытый режим работы GUI-версии **Сканера**. Программа работает, не открывая никаких окон и самостоятельно завершаясь. Но если в процессе сканирования были обнаружены вирусные объекты, по завершении работы будет открыто обычное окно **Сканера**. Такой режим работы **Сканера** предполагает, что список проверяемых объектов задается в командной строке.
- **/TB** – выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска.
- **/TM** – выполнять поиск вирусов в оперативной памяти (включая системную область ОС Windows, только для **Сканеров** для ОС Windows).
- **/TS** – выполнять поиск вирусов в файлах автозапуска (по каталогу `Автозагрузка`, системным `ini`-файлам, реестру ОС Windows). Используется только для **Сканеров** для ОС Windows.

- **/UP** или **/UPN** – проверять исполняемые файлы, упакованные программами ASPACK, COMPACK, DIET, EXEPACK, LZEXE и т. п.; файлы, преобразованные программами BJFNT, COM2EXE, CONVERT, CRYPTCOM и т. п., а также файлы, иммунизированные вакцинами CPAV, F-XLOCK, PGPROT, VACCINE и т. п. Чтобы сканер не отображал на экране название программы, использованной для упаковки, преобразования или вакцинирования проверяемого файла, применяется ключ **/UPN**.
- **/WA** – не завершать работу программы до нажатия на любую клавишу, если обнаружены вирусы или подозрительные объекты (только для консольных **Сканеров)**.
- **/?** – вывести на экран краткую справку о работе с программой.

Некоторые параметры допускают задание в конце символа "-". В такой "отрицательной" форме параметр означает отмену соответствующего режима. Такая возможность может быть полезна в случае, если этот режим включен по умолчанию или по выполненным ранее установкам в конфигурационном файле. Список параметров командной строки, допускающих "отрицательную" форму:
/ADW /AR /CU /DLS /FN /HCK /JOK /HA /IC /ML /MW /OK / PF /PR /RSK /SD /SO /SP /SS/TB /TM /TS /UP /WA

Для ключей **/CU**, **/IC** и **/SP** "отрицательная" форма отменяет выполнение любых действий, указанных в описании этих параметров. Это означает, что в отчете будет фиксироваться информация о зараженных и подозрительных объектах, но никаких действий над этими объектами выполняться не будет.

Для ключей **/INI** и **/RP** "отрицательная" форма записывается в виде **/NI** и **/NR** соответственно.

Для ключей **/AL** и **/EX** не предусмотрена "отрицательная" форма, однако задание одного из них отменяет действие другого.

Если в командной строке встречаются несколько взаимоисключающих ключей, то действует последний из них.

Ключи для Консольного Сканера DWScancl

- **/AR** – проверять архивы. По умолчанию опция включена.
- **/AC** – проверять контейнеры. По умолчанию опция включена.
- **/AFS** – использовать прямой слеш при указании вложенности внутри архива. По умолчанию опция отключена.
- **/ARC:**<*число*> – максимальный уровень сжатия. Если **Консольный сканер** определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка не производится. По умолчанию – без ограничений.
- **/ARL:**<*число*> – максимальный уровень вложенности проверяемого архива. По умолчанию – без ограничений.
- **/ARS:**<*число*> – максимальный размер проверяемого архива, в килобайтах. По умолчанию – без ограничений.
- **/ART:**<*число*> – порог проверки уровня сжатия (минимальный размер файла внутри архива, начиная с которого будет производиться проверка коэффициента сжатия), в килобайтах. По умолчанию – без ограничений.
- **/ARX:**<*число*> – максимальный размер проверяемых объектов в архивах, в килобайтах. По умолчанию – без ограничений.
- **/BI** – вывести информацию о вирусных базах. По умолчанию опция включена.
- **/DR** – рекурсивно сканировать директории (проверять поддиректории). По умолчанию опция включена.
- **/E:**<*число*> – использовать указанное количество движков.
- **/FL:**<*имя_файла*> – сканировать пути, указанные в файле.
- **/FM:**<*маска*> – сканировать файлы по маске. По умолчанию сканируются все файлы.
- **/FR:**<*регулярное_выражение*> – сканировать файлы по регулярному выражению. По умолчанию сканируются все файлы.
- **/H** или **/?** – вывести на экран краткую справку о работе с программой.

- **/HA** – производить эвристический анализ файлов и поиск в них неизвестных вирусов. По умолчанию опция включена.
- **/KEY:**<*ключевой_файл*> – указать путь к ключевому файлу. Параметр необходим в том случае, если ключевой файл находится не в той же директории, что и **Консольный сканер**. По умолчанию используется ключевой файл из каталога установки **Антивируса**.
- **/LN** – сканировать файлы, на которые указывают ярлыки. По умолчанию опция отключена.
- **/LS** – сканировать под учетной записью LocalSystem. По умолчанию опция отключена.
- **/MA** – проверять почтовые файлы. По умолчанию опция включена.
- **/MC:**<*число*> – установить максимальное число попыток вылечить файл. По умолчанию – без ограничений.
- **/NB** – не создавать резервные копии вылеченных/ удаленных файлов. По умолчанию опция отключена.
- **/NI[:X]** – уровень использования ресурсов системы, в процентах. Определяет количество памяти используемой для сканирования и системный приоритет задачи сканирования. По умолчанию – без ограничений.
- **/NT** – сканировать NTFS-потоки. По умолчанию опция включена.
- **/OK** – выводить полный список сканируемых объектов, сопровождая незараженные пометкой **Ok**. По умолчанию опция отключена.
- **/P:**<*приоритет*> – приоритет запущенной задачи сканирования в общей очереди задач на сканирование:
  - *0* – низший.
  - *L* – низкий.
  - *N* – обычный. Приоритет по умолчанию.
  - *H* – высший.
  - *M* – максимальный.
- **/PAL:**<*число*> – уровень вложенности упаковщиков. По умолчанию – 1000.
- **/RA:**<*имя файла*> – дописать отчет о работе программы в указанный файл. По умолчанию – отчет не создается.

- **/RP:**<*имя файла*> – записать отчет о работе программы в указанный файл. По умолчанию – отчет не создается.
- **/RPC:**<*число*> – таймаут соединения с **Scanning Engine**, в секундах. По умолчанию – 30 секунд.
- **/RPCD** – использовать динамический идентификатор RPC.
- **/RPCE** – использовать динамический целевой адрес RPC.
- **/RPCE:**<*целевой_адрес*> – использовать указанный целевой адрес RPC.
- **/RPCH:**<*имя_хоста*> – использовать указанное имя хоста для вызовов RPC.
- **/RPCP:**<*протокол*> – использовать указанный протокол RPC. Возможно использование протоколов: lpc, np, tcp.
- **/QL** – вывести список всех файлов, помещенных в **Карантин** на всех дисках.
- **/QL:**<*имя_логического_диска*> – вывести список всех файлов, помещенных в **Каранатин** на указанном логическом диске.
- **/QR[:[d][:p]]** – удалить файлы с указанного диска <*d*> *(имя_логического_диска)*, находящиеся в **Карантине** дольше <*p*> *(количество)* дней. Если <*d*> и <*p*> не указаны, то будут удалены все файлы, находящиеся в **Карантине**, со всех логических дисков.
- **/QNA** – выводить пути в двойных кавычках.
- **/REP** – сканировать по символьным ссылкам. По умолчанию опция отключена.
- **/SCC** – выводить содержимое составных объектов. По умолчанию опция отключена.
- **/SCN** – выводить название контейнера. По умолчанию опция отключена.
- **/SPN** – выводить название упаковщика. По умолчанию опция отключена.
- **/SLS** – выводить логи на экран. По умолчанию опция включена.
- **/SPS** – отображать процесс проведения сканирования. По умолчанию опция включена.
- **/SST** – выводить время сканирования файла. По умолчанию опция отключена.

- **/TB** – выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска. По умолчанию опция отключена.
- **/TM** – выполнять поиск вирусов в оперативной памяти (включая системную область Windows). По умолчанию опция отключена.
- **/TS** – выполнять поиск вирусов в файлах автозапуска (по папке Автозагрузка, системным ini-файлам, реестру Windows). По умолчанию опция отключена.
- **/TR** – сканировать системные точки восстановления. По умолчанию опция отключена.
- **/W:**<*число*> – максимальное время сканирования, в секундах. По умолчанию – без ограничений.
- **/WCL** – вывод, совместимый с drwebwcl.
- **/X:S[:R]** – по окончании сканирования перевести машину в указанный режим: выключение/перезагрузка/ждущий режим/спящий режим по причине **R** (для выключения/перезагрузка).

Задание действий с различными объектами (**C** – вылечить, **Q** – переместить в карантин, **D** – удалить, **I** – игнорировать, **R** – информировать. По умолчанию для всех – информировать):

- **/AAD:**<*действие*> – действия для рекламных программ (возможные действия: DQIR).
- **/AAR:**<*действие*> – действия с инфицированными архивами (возможные действия: DQIR).
- **/ACN:**<*действие*> – действия с инфицированными контейнерами (возможные действия: DQIR).
- **/ADL:**<*действие*> – действия с программами дозвона (возможные действия: DQIR).
- **/AHT:**<*действие*> – действия с программами взлома (возможные действия: DQIR).
- **/AIC:**<*действие*> – действия с неизлечимыми файлами (возможные действия: DQR).
- **/AIN:**<*действие*> – действия с инфицированными файлами (возможные действия: CDQR).
- **/AJK:**<*действие*> – действия с программами-шутками

(возможные действия: DQIR).

- **/AML:**<*действие*> – действия с инфицированными почтовыми файлами (возможные действия: QIR).
- **/ARW:**<*действие*> – действия с потенциально опасными файлами (возможные действия: DQIR).
- **/ASU:**<*действие*> – действия с подозрительными файлами (возможные действия: DQIR).

Некоторые ключи могут иметь модификаторы, с помощью которых режим явно включается либо отключается. Например:

/AC- режим явно отключается,
/AC, **/AC+** режим явно включается.

Такая возможность может быть полезна в случае, если режим включен/отключен по умолчанию или по выполненным ранее установкам в конфигурационном файле. Список ключей, допускающих применение модификаторов: **/AR**, **/AC**, **/AFS**, **/BI**, **/DR**, **/HA**, **/LN**, **/LS**, **/MA**, **/NB**, **/NT**, **/OK**, **/QNA**, **/REP**, **/SCC**, **/SCN**, **/SPN**, **/SLS**, **/SPS**, **/SST**, **/TB**, **/TM**, **/TS**, **/TR**, **/WCL**.

Для ключа **/FL** модификатор "-" означает: проверить пути, перечисленные в указанном файле, и удалить этот файл.

Для ключей **/ARC**, **/ARL**, **/ARS**, **/ART**, **/ARX**, **/NI[:X]**, **/PAL**, **/RPC**, **/W**, принимающих в качестве значения параметра <число>, "0" означает, что параметр используется без ограничений.

Пример использования ключей при запуске **Консольного сканера DWScancl**:

```
[<путь_к_программе>]dwscancl /AR- /AIN:C /AIC:Q C:\
```

проверить все файлы, за исключением архивов, на диске C, инфицированные файлы лечить, неизлечимые поместить в **Карантин**.

Приложение В. Полный список поддерживаемых версий ОС

ОС семейства UNIX:

Linux glibc 2.7 и выше
FreeBSD 7.3 и выше
Sun Solaris 10 (только для платформы Intel)

ОС Windows:

- 32 bit:

Windows 98
Windows Millennium Edition
Windows NT4 (SP6a)
Windows 2000 Professional (SP4 также с Update Rollup 1)
Windows 2000 Server (SP4 также с Update Rollup 1)
Windows XP Professional (также с SP1 и выше)
Windows XP Home (также с SP1 и выше)
Windows Server 2003 (также с SP1 и выше)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)
Windows 7
Windows 8

- 64 bit:

Windows Server 2003 (также с SP1 и выше)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)
Windows Server 2008 R2
Windows 7

Windows Server 2012
Windows 8

SelfPROtect, SplDer Gate, Офисный Контроль, FireWall

- 32 bit:

Windows 2000 Professional (SP4 также с Update Rollup 1)
Windows 2000 Server (SP4 также с Update Rollup 1)
Windows XP Professional (также с SP1 и выше)
Windows XP Home (также с SP1 и выше)
Windows Server 2003 (также с SP1 и выше)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)
Windows 7
Windows 8

- 64 bit:

Windows Server 2003 (также с SP1 и выше)
Windows Vista (также с SP1 и выше)
Windows Server 2008 (также с SP1 и выше)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

ОС Windows Mobile

Windows Mobile 2003
Windows Mobile 2003 Second Edition
Windows Mobile 5.0
Windows Mobile 6.0
Windows Mobile 6.1
Windows Mobile 6.5

ОС Novell NetWare

Novell NetWare 4.11 SP9
Novell NetWare 4.2
Novell NetWare 5.1
Novell NetWare 6.0
Novell NetWare 6.5

Mac OS X

Mac OS 10.6 (Snow Leopard)
Mac OS 10.6 Server (Snow Leopard Server)
Mac OS 10.7 (Lion)
Mac OS 10.7 Server (Lion Server)
Mac OS 10.8 (Mountain Lion)
Mac OS 10.8 (Mountain Lion Server)

ОС Android

Android 1.6
Android 2.0
Android 2.1
Android 2.2
Android 2.3
Android 3.0
Android 3.1
Android 3.2
Android 4.0.

Описание функциональности **Агента** под ОС Windows Mobile и Novell NetWare приведено в руководствах пользователя **Dr.Web Агент для Windows Mobile** и **Dr.Web Агент для Novell NetWare**.

Приложение С. Методы обнаружения вирусов

Все антивирусные компоненты **Dr.Web** одновременно используют несколько методов обнаружения вредоносных объектов, что позволяет максимально тщательно проверить подозрительные файлы и контролировать поведение программ:

1. В первую очередь применяется *сигнатурный* анализ. Он выполняется путем анализа кода подозрительных файлов на предмет соответствия сигнатурам известных вирусов *(сигнатурой* называется непрерывная конечная последовательность байт, необходимая и достаточная для опознания вируса). При этом сравнение проводится по контрольным суммам сигнатур, что позволяет значительно снизить размер записей в вирусных базах данных, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения и лечения зараженных файлов. **Вирусные базы Dr.Web** составлены таким образом, что благодаря одной записи можно обнаруживать целые классы угроз.
2. После завершения сигнатурного анализа применяется уникальная технология **Origins Tracing™**, которая позволяет определить новые или модифицированные вирусы, использующие известные механизмы заражения файлов. Так, например, эта технология защищает пользователей антивирусных решений **Dr.Web** от таких вирусов, как вирус-шантажист Trojan.Encoder.18 (так же известный под названием gpcode). Кроме того, именно введение **Origins Tracing** позволяет значительно снизить количество ложных срабатываний эвристического анализатора.
3. Работа эвристического анализатора основывается на неких знаниях (*эвристиках*) о характерных признаках вирусного и, наоборот, безопасного кода. Каждый признак имеет определенный вес (число, показывающее серьезность и достоверность данного признака). На основании суммарного веса, характеризующего каждый конкретный

файл, эвристический анализатор вычисляет вероятность заражения файла неизвестным вирусом. Как и любая система проверки гипотез в условиях неопределенности, эвристический анализатор может допускать ошибки как первого (пропуск неизвестных вирусов), так и второго рода (ложная тревога).

Во время любой из проверок компоненты антивируса **Dr.Web** используют самую свежую информацию об известных вредоносных программах. Сигнатуры вирусов, информация об их признаках и моделях поведения обновляется сразу же, как только специалисты **Антивирусной Лаборатории «Доктор Веб»** обнаруживают новые угрозы, иногда – до нескольких раз в час. Таким образом, регулярное автоматическое обновление вирусных баз позволяет обнаруживать даже самые новые вирусы.

Предметный Указатель

Предметный Указатель

Предметный Указатель

Предметный Указатель

Ф

Ц

Я