Dr.WEB®

Агент

Защити созданное

# Руководство пользователя

**Dr.Web Агент**
**Версия 5.00.1**
**Руководство пользователя**
**11.02.2010**

Dr.Web, 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,
- 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® AV-Desk

Сервис **Dr.Web AV-Desk** строится на базе программной клиент-серверной системы, обеспечивающей управление комплексной антивирусной защитой компьютеров клиентов организаций, специализирующихся на оказании различного рода интернет-услуг (провайдеры доступа в Интернет (ISP), поставщики услуг приложений (ASP), а также банковских услуг (online banking) и т. д.) при условии, что рабочие станции периодически имеют доступ в Интернет.

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

***Программные решения, используемые в Dr.Web AV-Desk, позволяют реализовывать следующие задачи:***

- простая установка ПО компонентов комплекса и быстрая организация антивирусной защиты,
- создание дистрибутивов с уникальными идентификаторами и передачу их пользователям для установки сервиса,
- 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**. Эта программа обеспечивает управление защитой компьютера и поддерживает связь с антивирусным **Сервером**, через который производятся обновления антивирусных программ и их компонентов, а также настройка основных параметров работы антивирусного ПО, установленного на компьютерах.

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

На компьютеры с установленным **Dr.Web Агентом** нельзя устанавливать другие антивирусные программы, в том числе другие программы компании **Dr.Web**.

# 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 AV-Desk**.

Управление защитой компьютера и поддержка связи с антивирусным **Сервером** осуществляется посредством **Агента Dr.Web AV-Desk** (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 антивирусным **Сервером**;
- позволяет вызывать компоненты антивирусного пакета **Dr.Web** через специальный интерфейс;
- передает результаты выполнения заданий антивирусному **Серверу**;
- передает антивирусному **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 программного комплекса **Dr.Web**, в том числе, некоторые настройки самого **Агента**;

- просматривать статистику вирусных событий на компьютере и другую информацию о программном комплексе **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

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

- процессор Intel® Pentium® II с частотой 400 МГц или выше;
- объем оперативной памяти не менее 32 МБ;
- свободное место на жестком диске: не менее 80 МБ для исполняемых файлов + дополнительно для протоколов работы и временных файлов;
- ОС Windows 98, ОС Windows Me, ОС Windows NT4 (SP6) и выше;
  - причем сторож **SpIDer Guard** и компонент самозащиты **Self-Protection** работают только в 32-разрядных системах.
  - **SpiderGate** и **Self-Protection** работают под ОС Windows 2000 (SP4) и выше.

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**).

# 2.3. Установка и удаление антивирусного ПО

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

## Установка антивирусного ПО

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 (провайдера).
2. Запустите скачанный файл `avdinst.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. Откроется окно с текстом лицензионного договора. После ознакомления с условиями лицензионного договора установите флаг **Я принимаю условия данного Лицензионного Соглашения** и нажмите на кнопку **Далее**.
5. 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.

6. 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. 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 **9**.

7. Для варианта установки **Административная**: в следующем окне задайте настройки **Сетевого инсталлятора**:
   - В поле **Dr.Web AV-Desk Server** задается сетевой адрес **AV-Desk 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 **AV-Desk 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 AV-Desk 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 поле **Каталог установки** задается путь для установки антивирусного ПО на компьютере пользователя. По умолчанию - это каталог `Dr.Web AV-Desk`, расположенный в каталоге `Program files` на системном диске (может быть задан при помощи системной переменной `%ProgramFiles%`).
- В разделе **Использовать сжатие при закачке** выберите нужный для вас вариант компрессии трафика: **Да** - использовать сжатие, **Нет** - не использовать, **Возможно** - 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). 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**.

8. 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 **AV-Desk Агента** при помощи инсталлятора, созданного в **Веб-консоли**, 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 AV-Desk**).

Нажмите **Далее**.

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

## Удаление антивирусного ПО

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**.

Для удаления антивирусного ПО выберите:

- для ОС Windows 98, Windows NT, 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 выше (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**.

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

удалено.

### *Удаление при помощи инсталлятора*

Для того чтобы удалить ПО **Dr.Web Агента** и антивирусный пакет при помощи инсталлятора запустите установочный файл `avdinst.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 (элемент рабочего стола Microsoft Windows, отображающий значки активных приложений и располагающийся в правой части Панели задач, которая по умолчанию находится внизу рабочего стола).

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** при помощи команды **Start AgentUI,** расположенной в меню ОС Windows **Пуск** → **Программы** → **Dr.Web (R) AV-Desk**.

# 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.

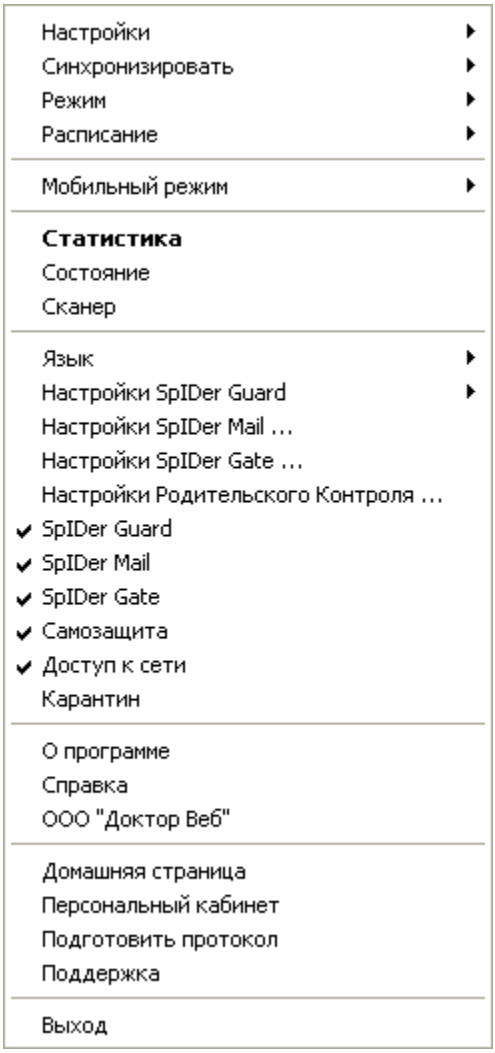


**Рисунок 2-1. Контекстное меню Dr.Web Агента**

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.
- **Персональный кабинет** - открыть страницу на сайте провайдера с персональными данными пользователя.
- **Домашняя страница** - перейти на сайт провайдера.
- **ООО "Доктов 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"**.
- **Доступ к сети** - при наличии этого флага доступ к локальной сети и Интернету разрешен, иначе - заблокирован.
- **Самозащита** - включить/выключить системный монитор. 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**.
- **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.
- **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.

Подробная информация об остальных пунктах меню приведена в Главе 3 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 операционной системой Windows Vista, 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 антивирусном **Сервере**.

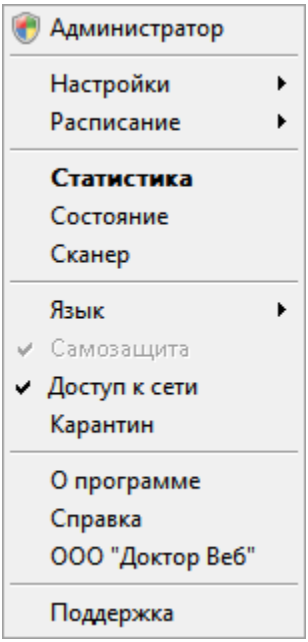


**Рисунок 2-2. Контекстное меню Dr.Web Агента под пользователем ОС Windows Vista**

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 **SelfPROtection** 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. 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;
  - о необходимости перезагрузки компьютера.
- **Малозначительные оповещения** - получать только малозначительные оповещения. К таковым относятся сообщения:
  - о начале обновления антивирусного ПО или какого-либо из его компонентов;
  - о завершении обновления антивирусного ПО или какого-либо из его компонентов.
- **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).

Пункты **Соединение** и **Уровень протокола** доступны 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.

## 3.1.1. Настройки соединения с сервером

Просмотр и редактирование настроек соединения с антивирусным **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 антивирусным **Сервером Dr.Web** (см. рис. 3-1) вы можете изменить настройки подключения к текущему **Серверу** или настроить соединение с новым антивирусным **Сервером**.

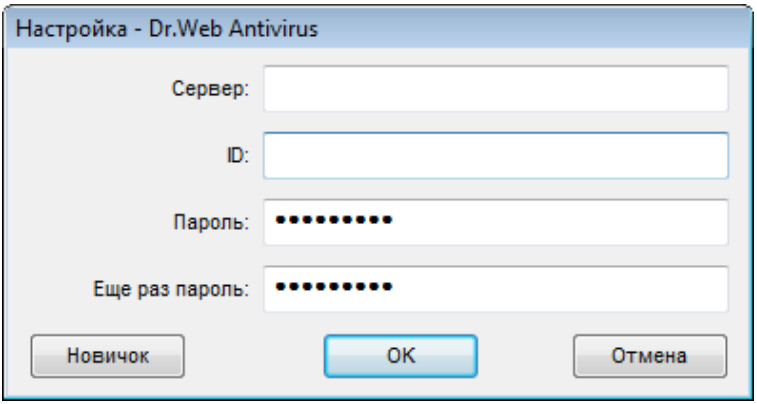


**Рисунок 3-1. Настройки соединения с Сервером**

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

При необходимости измените параметры:

- **Сервер** - введите имя антивирусного **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 антивирусному **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 антивирусным **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 антивирусному **Серверу**.

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.

## 3.1.2. 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.

## 3.2. 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**.

## 3.3. 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 AV-Desk 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 накопления информации о вирусных событиях на вашем компьютере.

## 3.4. 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**.

## 3.4.1. 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
- При завершении

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 или в меню ОС Windows **Пуск**, пункт **Программы**.

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

### 3.4.1.1. Ежечасное задание

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

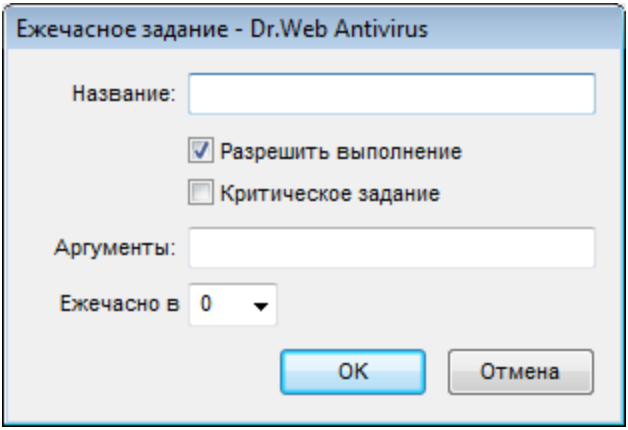


**Рисунок 3-2. Диалоговое окно ежечасного задания**

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**.

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

### 3.4.1.2. Ежедневное задание

Данный тип задания будет выполняться каждый день в указанное время.

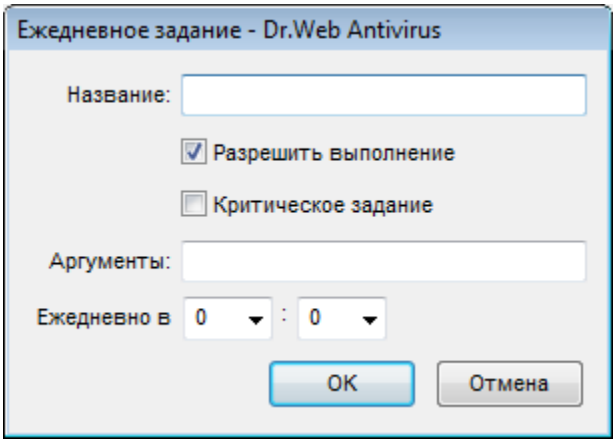


**Рисунок 3-3. Диалоговое окно ежедневного задания**

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.**

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.

### 3.4.1.3. Еженедельное задание

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

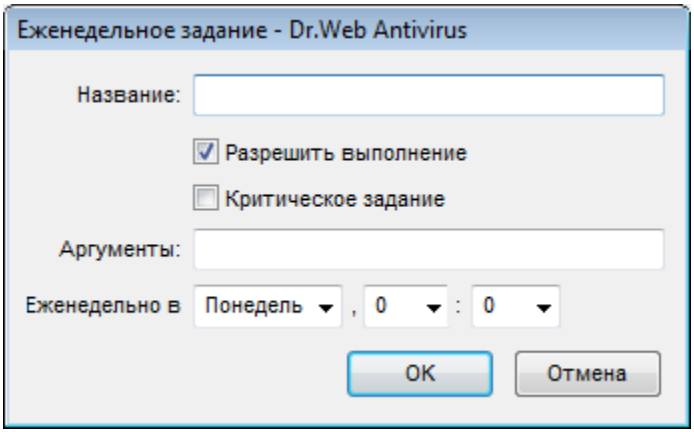


**Рисунок 3-4. Диалоговое окно еженедельного задания**

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.**

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.

### 3.4.1.4. Ежемесячное задание

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

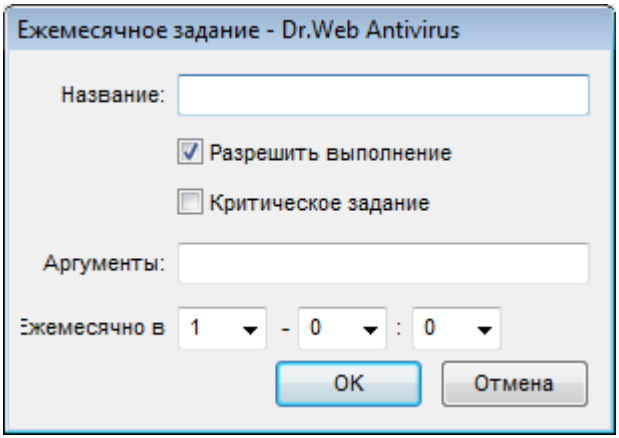


**Рисунок 3-5. Диалоговое окно ежемесячного задания**

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.**

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.

### 3.4.1.5. Задание, выполняемое каждые X минут

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

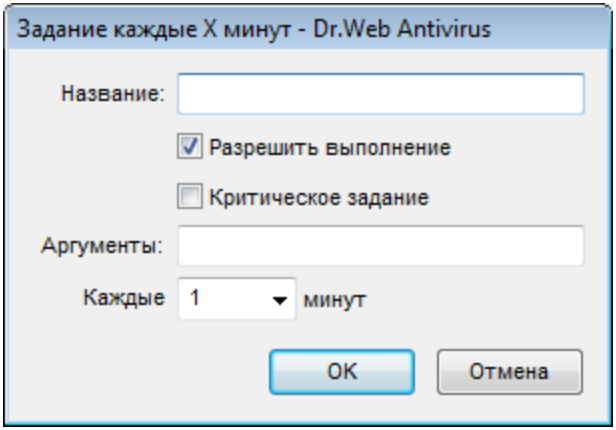


**Рисунок 3-6. Диалоговое окно задания**

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.**

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.

### 3.4.1.6. Задание, выполняемое при старте

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

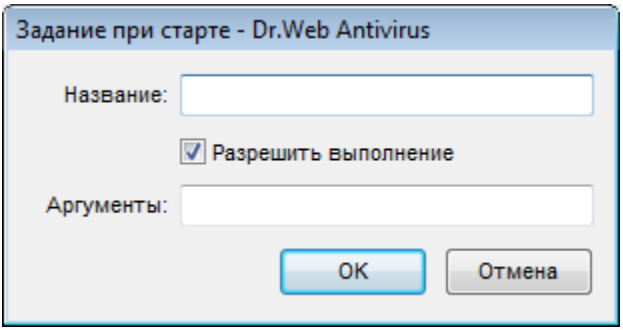


**Рисунок 3-7. Диалоговое окно задания**

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.**

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.

### 3.4.1.7. Задание, выполняемое при завершении

Данный тип задания будет выполняться при завершении работы **Dr.Web Агента** (при выходе из операционной системы).

Завершающее задание для **Dr.Web AV-Desk Сканера** и **Dr.Web Сканера для Windows** не выполняется.

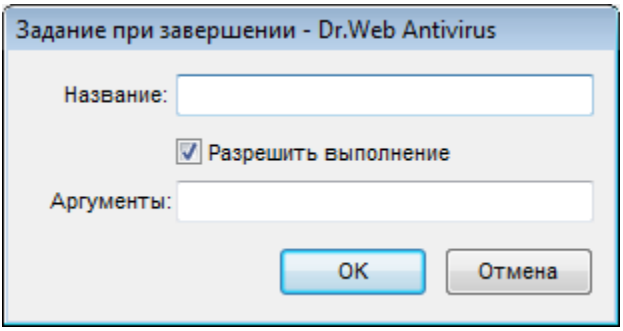


**Рисунок 3-8. Диалоговое окно задания**

В диалоговом окне задания (см. рис. 3-8) 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.**

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.

### 3.4.2. Централизованное расписание

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

## 3.5. Настройка языка интерфейса

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.

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

## 3.6. Настройки мобильного режима

Если ваш компьютер (или ноутбук) долгое время не будет иметь

связи с антивирусным **Сервером**, для своевременного получения обновлений с серверов **ВСО 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**.

Если вы планируете длительную поездку и берете с собой ваш компьютер (или ноутбук), то заранее попросите провайдера разрешить вам использование мобильного режима.

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

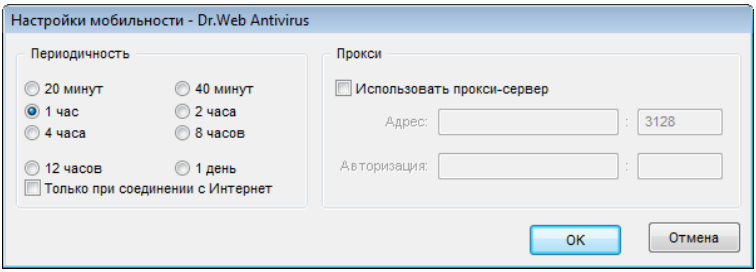


**Рисунок 3-9. Диалоговое окно настроек мобильного режима**

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 **Сервером Dr.Web AV-Desk** 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.

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.

## 3.7. 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**, установленные на вашем компьютере. В остальных столбцах указано количество проверенных ими объектов (просканированных).

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** Руководства **Антивирус Dr.Web для Windows**, прилагаемого к антивирусным программам **Dr.Web**.

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. Работа с карантином

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.

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

При обнаружении зараженных объектов на съемном носителе, если запись на носителе возможна, на нём создается папка `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.

Если файлы перемещаются в **Карантин GUI-Сканером** или **сторожами**, то они располагаются в папке `Infected.!!!` каталога установки **Антивируса**.

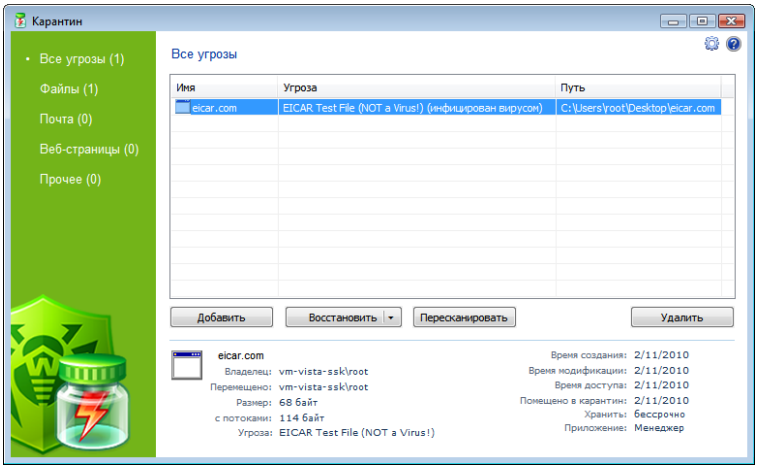


**Рисунок 3-10. Окно карантина**

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**. Для настройки отображения 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**.

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** файлы могут видеть только те пользователи, которые имеют права доступа к этим файлам.

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

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

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

В выпадающем меню вы можете выбрать вариант **Восстановить в** – переместить файл под заданным именем в папку, указанную пользователем.

- **Пересканировать** – сканировать файл из **Карантина** повторно. Если при повторном сканировании файла обнаружится, что он незаражен, **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**, и в выпадающем меню выберите необходимое действие.

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

Для настройки свойств **Карантина** нажмите на кнопку  в окне **Карантина**. Откроется окно **Свойства карантина**, в котором вы

можете изменять следующие параметры:

- Раздел **Задать размер карантина** позволяет управлять объемом дискового пространства, занимаемого папкой **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 папки **Карантина**). Значение `100%` означает снятие ограничений для максимального размера папки **Карантина**.
- В разделе **Вид** установите флаг **Показывать резервные копии**, чтобы отобразить в таблице объектов резервные копии файлов, находящихся в **Карантине**.

Резервные копии создаются автоматически при перемещении файлов в **Карантин**. Даже при хранении файлов в **Карантине** **бессрочно**, их резервные копии сохраняются **временно**.

При переполнении диска осуществляется 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.

Для отображения справки нажмите на кнопку  .

# 3.10. Запуск антивирусного сканера

При помощи команды **Сканер** из контекстного меню **Агента** вы можете запускать антивирусный **Сканер Dr.Web** для периодической проверки вашего компьютера на вирусы и вредоносное ПО. При этом откроется главное окно сканера (подробнее см. Руководство **Антивирус Dr.Web для Windows**, раздел **Главное окно сканера**), в котором после предварительной проверки компьютера вы можете запустить антивирусное сканирование в одном из доступных режимов.

Также - в зависимости от установок на **Сервере** - вы можете оптимизировать параметры антивирусной проверки: выбрать объекты, подлежащие проверке, типы действий над обнаруженными объектами и пр. в настройках сканера (подробнее см. Руководство **Антивирус Dr.Web для Windows**, раздел **Сканер Dr.Web для Windows**).

Для перехода на справку **Антивирус Dr.Web для Windows** нажмите клавишу F1 в любом окне сканера. Чтобы получить контекстную справку о каком-либо элементе окна, нажмите на него правой кнопкой мыши.

# 3.11. Настройки файлового монитора

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

В зависимости от установок на **Сервере** вы можете настраивать файловый монитор **SpIDer Guard**. Для этого выберите в контекстном меню **Агента** 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.

Чтобы просмотреть или изменить параметры сканирования, выберите в контекстном меню **Агента** пункт **Настройки SpIDer Guard** → **Настройки сканирования**. Откроется окно настроек **SpIDer Guard**. Подробное описание настроек приведено в Руководстве **Антивирусный сторож SpIDer Guard**, в разделе **Настройки SpIDer Guard**.

Чтобы просмотреть или изменить параметры запуска сторожа, настройки его работы и оповещения о событиях, выберите в контекстном меню **Агента** пункт **Настройки SpIDer Guard** → **Управление**. Откроется окно управления **SpIDer Guard**. Подробное описание управлением приведено в Руководстве **Антивирусный сторож SpIDer Guard**, в разделе **Управление**.

Для перехода на справку **Антивирусный сторож SpIDer Guard** нажмите клавишу F1 в любом окне сторожа.

## 3.12. Настройки почтового монитора

**SpIDer Mail для рабочих станций Windows** - почтовый сторож. При настройках по умолчанию **SpIDer Mail** автоматически проверяет все обращения любых почтовых программ вашего компьютера к серверам электронной почты.

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

В зависимости от установок на **Сервере** вы можете настраивать

почтовый монитор **SpIDer Mail**. Для этого выберите в контекстном меню **Агента** 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.

Откроется окно настроек **SpIDer Mail**. Подробное описание управления компонентом **SpIDer Mail** приведено в Руководстве **Антивирус Dr.Web для Windows**, в разделе **Настройка SpIDer Mail для рабочих станций Windows**.

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

## 3.13. Настройки HTTP-монитора

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 AV-Desk**. 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.

## 3.14. Настройки Родительского Контроля

Модуль **Родительского 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 **Родительского контроля**.

В зависимости от установок на **Сервере** вы можете настраивать модуль **Родительского контроля**. Для этого выберите в контекстном меню **Агента** пункт **Настройки Родительского контроля.**

Пункт **Настройки Родительского 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.

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.

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

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

***Для того чтобы изменить настройки модуля:***

1. Введите ранее сохраненный пароль. Задание пароля производится при вызове настроек параметров модуля в первый раз. Для того чтобы изменить пароль нажмите кнопку  (**Сменить пароль**), расположенную в окне настроек.
2. Внесите необходимые изменения на вкладках настроек (подробнее см. п. Фильтр URL и п. Локальный доступ).
3. Для того чтобы получить информацию о настройках, расположенных на вкладке, нажмите кнопку  **(Справка).**
4. Нажмите кнопку **Применить** для сохранения внесенных изменений без закрытия окна настроек.
5. По окончанию редактирования настроек нажмите кнопку **ОК** для сохранения всех внесенных изменений или кнопку **Отмена** - для отказа от них с последующим закрытием окна настроек.

## 3.14.1. Фильтр URL

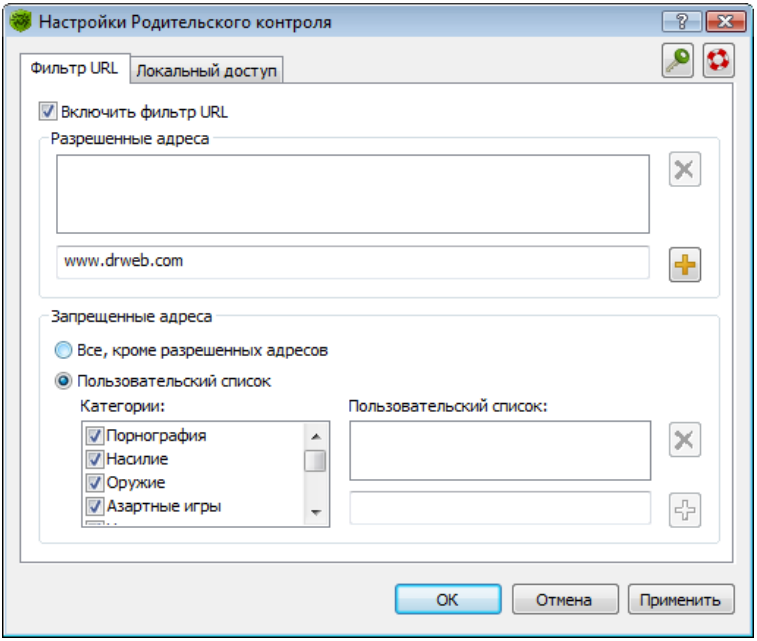


**Рисунок 3-11. Настройки Родительского контроля. Вкладка Фильтр URL**

На вкладке **Фильтр URL** задается блокировка интернет-ресурсов.

1. Для того чтобы активировать средства блокировки интернет-ресурсов, установите флаг **Включить фильтр URL**. После этого вы получите доступ к изменению управляющих полей.

Для того чтобы полностью ограничить доступ к сети Интернет установите флаг **Доступ к сети** на вкладке настроек Локальный доступ.

Фильтрация URL производится только при работающей антивирусной проверке входящего трафика.

2. В группе **Разрешенные адреса** вы можете указать адреса проверенных веб-сайтов, к которым всегда будет разрешен доступ с вашего компьютера. Подробнее о том, как задать список доступных веб-сайтов, см. раздел Управление списком доменных адресов.
3. Группа **Запрещенные адреса** служит для задания настроек запрета доступа к интернет-ресурсам. Возможны два варианта блокировки:
   - **Все, кроме разрешенных адресов** - запрещает доступ ко всем веб-ресурсам, кроме разрешенных ресурсов, URL которых указаны в поле **Разрешенные адреса** (см. шаг 2).
   - **Пользовательский список** - для включения фильтрации интернет-ресурсов на основе тематических категорий и пользовательского списка адресов веб-сайтов.

   В поле **Категории** установите флаги для тех тематик ресурсов, которые вы хотите заблокировать. Эти флаги активируют встроенный фильтр и заблокируют веб-сайты, соответствующие данным категориям.

При обновлениях антивирусного ПО **Dr.Web**, вместе с вирусными базами производится автоматическая загрузка обновленных списков адресов веб-сайтов по всем тематическим категориям.

В списке **Пользовательский список** вы можете задать адреса интернет-ресурсов, доступ к которым будет заблокирован. Подробнее о том, как задать список запрещенных веб-сайтов, см. раздел Управление списком доменных адресов.

4. Нажмите кнопку **Применить** для сохранения внесенных изменений без закрытия окна настроек. Для принятия указанных настроек и закрытия окна нажмите кнопку **ОК**. Для отмены изменений и закрытия окна настройки **Родительского контроля** нажмите кнопку **Отмена**.

## *Управление списком доменных адресов*

Списки доменных адресов используются для задания прав доступа к веб-ресурсам. На вкладке **Фильтр URL** могут указываться как списки блокируемых ресурсов, так и списки ресурсов, доступ к которым будет разрешен (см. процедуру блокировки ресурсов выше).

***Для того, чтобы внести изменения в списки доменных адресов необходимо:***

1) Если вы хотите добавить в список определенный сайт, укажите в поле ввода его адрес. При этом допускается ввод не только конкретных полных URL, но и фрагментов URL, содержащих определяющие комбинации символов.

   Примеры отфильтрованных (разрешенных/ заблокированных) ресурсов, в зависимости от введенной строки приведены в таблице 4.

**Таблица 4. Примеры фильтрации интернет-ресурсов**

| Пример строки | Фильтруемые ресурсы |
|---|---|
| domainame | Фильтруется любой интернет-ресурс, в адресной строке которого содержится последовательность символов "**domainame**". Например, будут отфильтрованы ресурсы:<br>◆ www.**domainame**.com<br>◆ www.top**domainame**.com<br>◆ www.**domainame**.com/path/index.html<br>◆ www.subdomain.**domainame**.org<br>◆ www.toplevel.org/**domainame**system.html<br>◆ и т.п. |

| Пример строки | Фильтруемые ресурсы |
|---|---|
| domainame.com | Поскольку введенная строка содержит символ ".", данная строка будет рассматриваться как имя домена. Все ресурсы, находящиеся на этом домене будут отфильтрованы.<br><br>Т. обр., фильтруется полностью домен www.**domainame.com**. |
| domainame.com/path | Данная строка содержит символ "/", и часть, стоящая слева от символа, будет считаться доменным именем, а часть справа от символа - фрагментом отфильтрованного на данном домене адреса.<br><br>Т. обр., фильтруется любой интернет-ресурс, на домене "**domainame.com**", адрес которого начинается с "**path**". Например, будут отфильтрованы ресурсы:<br>◆ www.**domainame.com/path**<br>◆ www.**domainame.com/path**/index.html<br>◆ www.subdomain.**domainame.com/path**/<br>◆ www.**domainame.com/path**etic<br>◆ и т.п.<br><br>Но при этом **не** фильтруются интернет-ресурсы, в адресной строке которых содержится только часть последовательности символов "**domainame.com/path**". Например, **не** будут отфильтрованы ресурсы:<br>◆ www.domainame.com<br>◆ www.domainame.com/wrongpath<br>◆ и т.п. |
| domainame.com?param=256 | Фильтруется запрос параметра "**param=256**" к домену "**domainame.com**", включая вложенные запросы. Например, будут отфильтрованы:<br>◆ www.**domainame.com?param=256**<br>◆ www.**domainame.com?**first=512&**param=256**<br>◆ и т.п. |

2) Нажмите кнопку  (**Добавить**) справа от поля ввода. Адрес (фрагмент адреса) будет добавлен в список над полем ввода.

Введенная строка при добавлении в список может быть преобразована модулем к универсальному виду. (Например: http://www.domainame.com будет преобразована в www.domainame.com).

3) Для того чтобы удалить какой-либо ресурс из списка, выберите его в этом списке и нажмите кнопку  **(Удалить).**

## 3.14.2. Локальный доступ

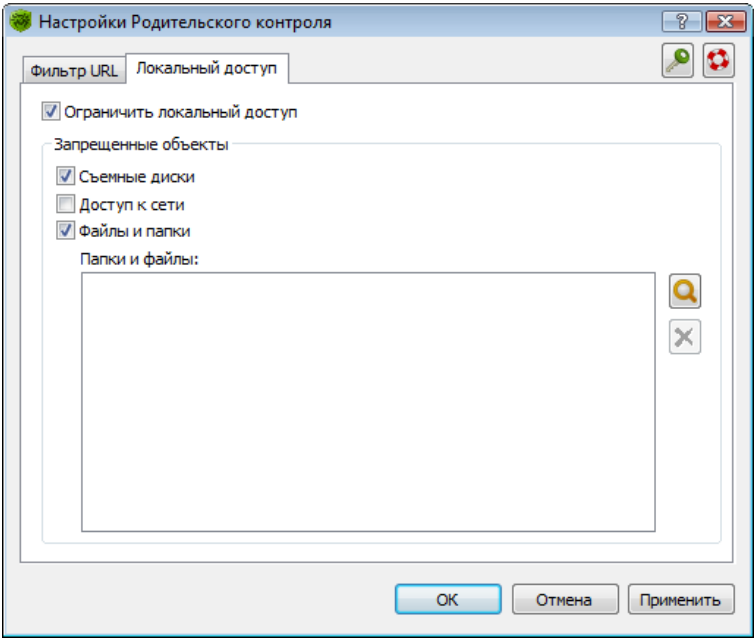


**Рисунок 3-12. Настройки Родительского контроля. Вкладка Локальный доступ**

На вкладке **Локальный доступ** задается блокировка локальных ресурсов на вашем компьютере.

1. Для того, чтобы активировать средства блокировки локальных ресурсов, установите флаг **Ограничить локальный доступ**. После этого вы получите возможность изменения настроек на данной вкладке.
2. В группе **Запрещенные объекты** вы можете указать ресурсы, к которым будет закрыт доступ с вашего компьютера. Описание флагов для настройки запрета доступа к локальным ресурсам приведено в таблице 5.

**Таблица 5. Описание флагов блокировки доступа**

| Флаг | Описание |
|---|---|
| Съемные диски | Установите этот флаг, чтобы запретить доступ ко всем съемным носителям информации.<br>Уберите этот флаг, чтобы разрешить использование съемных устройств.<br>К съемным носителям информации относятся, например:<br>◆ CD, DVD диски;<br>◆ магнитные диски (FDD);<br>◆ flash-накопители и прочие носители информации, подключаемые через USB-порт;<br>◆ и т.д. |
| Доступ к сети | Установите этот флаг, чтобы запретить весь сетевой трафик. При этом закрывается доступ к локальной сети и Интернету.<br>Уберите этот флаг, чтобы разрешить доступ к локальной сети и Интернету. |
| Файлы и папки | Установите этот флаг, чтобы создать список локальных ресурсов (файлов и папок), к которым вы хотите запретить доступ. Пути к блокируемым папкам и файлам задаются в поле **Папки и файлы**. Подробнее о том, как задать список запрещенных локальных ресурсов, см. раздел Управление списком блокируемых файлов и папок. |

В настройках **Родительского контроля** запрещается ставить под защиту следующие папки, включая их корневые каталоги:

- системный диск,
- папки с учетными записями пользователей,
- папку `Program Files`.

При этом допускается блокировка их подкаталогов.

Модуль **Родительского контроля** не позволяет блокировать сетевые файлы и папки.

3. Нажмите кнопку **Применить** для сохранения внесенных изменений без закрытия окна настроек. Для принятия указанных настроек и закрытия окна нажмите кнопку **ОК**. Для отмены изменений и закрытия окна настройки **Родительского контроля** нажмите кнопку **Отмена**.

***Управление списком блокируемых файлов и папок:***

1. Для возможности задания блокировки доступа к файлам и папкам на вашем компьютере установите флаг **Папки и файлы**.
2. Для добавления нового блокируемого ресурса нажмите кнопку  (**Обзор**). Откроется браузер по файловой системе. Выберите требуемый ресурс и нажмите кнопку **Открыть**. Ресурс будет добавлен в список **Папки и файлы.**
3. Для того чтобы удалить объект из списка, выберите его в этом списке и нажмите на кнопку  (**Удалить**).

# 3.15. 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 (провайдера).

## 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. 3-13) имеет диалоговый формат и содержит кнопки, позволяющие произвести перезагрузку компьютера или отложить напоминание об ее необходимости на заданное время. Для этого выберите в выпадающем списке требуемый промежуток времени и нажмите **Позднее**.


**Рисунок 3-13. 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),

- состоянию компонентов антивирусного ПО,
- дате последнего обновления.

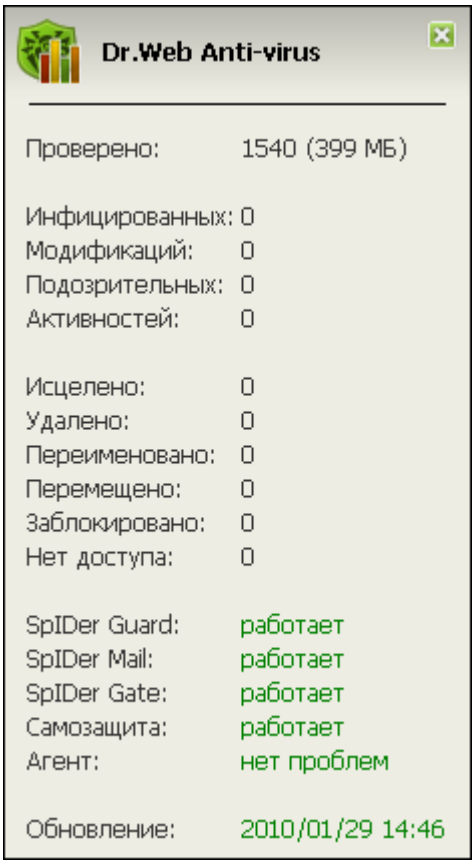


**Рисунок 3-14. Информационное окно Dr.Web Агента**

## *Сообщения от провайдера*

Пользователь может получать от системного администратора антивирусной сети (провайдера) 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. 3-15).

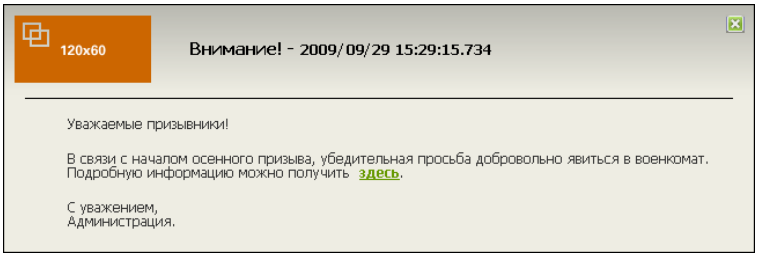


**Рисунок 3-15. Окно сообщения от провайдера**

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 (провайдера) будут отображаться, пока пользователь самостоятельно их не закроет.

# Приложение А. Ключи командной строки для 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 подкаталог infected.!!!);
- /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 подкаталог infected.!!!);
- /CUR – переименовывать (по умолчанию первая буква расширения заменяется на символ #).

◆ /SPR, /SPD или /SPM

действия с подозрительными файлами:

- /SPR – переименовывать,
- /SPD – удалять,
- /SPM – перемещать.

◆ /ICR, /ICD или /ICM

действия с зараженными файлами, вылечить которые невозможно:

- /ICR – переименовывать,
- /ICD – удалять,

- /ICM – перемещать.

◆ /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 подкаталог infected.!!!);
- /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.

◆ /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.

- /SCP: <*n*>

  задает приоритет выполнения сканирования. <*n*> может принимать значения от 1 до 50 включительно.

- /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.

- /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.

- /HA

  производить эвристический анализ файлов и поиск в них неизвестных вирусов.

- /INI: *<путь>*

  использовать альтернативный конфигурационный файл с указанным именем или путем.

- /NI

  не использовать параметры, записанные в конфигурационном файле программы drweb32.ini.

- /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 подкаталог infected.!!!);
  - /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.

- /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.

- /NR

  не создавать файл отчета.

- /SD

  проверять подкаталоги.

- /SO

  включить звуковое сопровождение.

- /SS

  по окончании работы сохранить режимы, заданные при текущем запуске программы, в конфигурационном файле.

- /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 папке 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.

# Предметный Указатель

# Предметный Указатель

# Предметный Указатель