Dr.WEB®

Антивирус
для Microsoft ISA Server и
Forefront TMG *Light*

Защити созданное

Руководство администратора

Антивирус Dr.Web для Microsoft ISA Server и Forefront TMG Light
Версия 6.00.1
Руководство администратора
01.11.2012

«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

Условные обозначения и сокращения

В руководстве используются следующие условные обозначения:

Обозначение	Комментарий
Полужирный	Названия кнопок и других элементов пользовательского интерфейса, а так же данные, которые вам необходимо ввести именно так, как они приведены в руководстве.
Зеленый полужирный	Названия продуктов компании **«Доктор Веб»** и их компонентов.
Зеленое подчеркивание	Ссылки на разделы документа и веб-сайты.
Курсив	Текст, замещающий информацию, которую вам нужно ввести. В примерах ввода команд такое выделение указывает на участки команды, которые вам необходимо заменить актуальным значением. Так же могут выделяться термины.
ПРОПИСНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Символ «плюс» (+)	Указывает на одновременное нажатие нескольких клавиш. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
	Важные замечания и указания.

В руководстве используются следующие сокращения:

- ОС – операционная система;
- ПО – программное обеспечение;
- AD – Active Directory;
- CPU – Central Processing Unit (центральное процессорное устройство);
- RAM – Random Access Memory (оперативная память);
- GUI – Graphical User Interface (графический интерфейс пользователя);
- HTML – Hypertext Mark-up Language (язык гипертекстовой разметки);
- HTTP – Hypertext Transfer Protocol (протокол передачи гипертекста);
- FTP – File Transfer Protocol (протокол передачи файлов);
- SP1, SP2, etc. – Service Packs (служебные пакеты обновления для ОС Windows).

Введение

Благодарим вас за приобретение **Антивируса Dr.Web для Microsoft ISA Server и Forefront TMG *Light*** (далее – **Антивируса Dr.Web *Light***). Данный антивирусный продукт использует наиболее передовые технологии и предоставляет возможности для антивирусной проверки и блокирования инфицированных данных, поступающих из сети Интернет по протоколу HTTP (в том числе FTP поверх HTTP) в защищенные межсетевым экраном Microsoft ISA Server и Forefront TMG локальные сети.

Настоящее руководство призвано помочь администраторам корпоративных сетей установить и настроить **Антивирус Dr.Web *Light***. Руководство содержит информацию обо всех основных особенностях использования данного программного обеспечения, а также контактную информацию службы технической поддержки.

Назначение Антивируса Dr.Web Light

Антивирус Dr.Web *Light* – это приложение, созданное с целью защитить корпоративную сеть от вирусных угроз. Оно надежно интегрируется в систему и осуществляет поиск и удаление любых типов вредоносных программ в потоке данных, проходящем через Microsoft ISA Server и Forefront TMG по протоколу HTTP (в том числе FTP поверх HTTP). Приложение проверяет входящий интернет-трафик на вирусы, программы дозвона, рекламные программы, потенциально опасные программы, программы взлома и программы-шутки. При обнаружении угрозы безопасности доступ пользователей к данным блокируется согласно настройкам приложения.

Приложение интегрируется в Microsoft ISA Server и Forefront TMG посредством встраивания собственных фильтров данных в службы Microsoft Firewall Service и Microsoft Forefront TMG Firewall соответственно, что обеспечивает доступ к ним ядру антивирусной системы **Dr.Web**. Приложение функционирует на платформе **Dr.Web CMS** (**Dr.Web Central Management Service**), поддерживающей централизованное управление настройками приложения и его компонентов с возможностью удаленного администрирования через браузер по защищенному протоколу HTTPS. Платформа **Dr.Web CMS** имеет встроенный веб-сервер **Dr.Web CMS Web Console** с аутентификацией клиента, что обеспечивает доступ к управлению приложением только авторизованным администраторам.

Сервисы **Dr.Web CMS**, установленные на разных серверах, могут быть объединены администратором в единое иерархическое дерево для поддержки репликации параметров с атрибутом **Shared** приложений-подписчиков **Dr.Web CMS**. Репликация производится от главного сервера на подчиненный (см. раздел Создание кластеров), таким образом, управление настройками дерева серверов возможно с корневого хоста.

Антивирус Dr.Web *Light* может выполнять следующие функции:

- сканирование всех данных, поступающих через межсетевой экран Microsoft ISA Server или Microsoft Forefront TMG по протоколу HTTP (в том числе FTP поверх HTTP);
- блокирование доступа к инфицированным данным для пользователей локальных сетей, защищенных межсетевым экраном Microsoft ISA Server или Microsoft Forefront TMG;
- изоляция инфицированных и подозрительных объектов в **Карантине**;
- отправка уведомлений о вирусных событиях в журнал событий операционной системы и ведение внутренней базы событий **Dr.Web CMS**;
- ограничение доступа пользователей к интернет-ресурсам с помощью **Офисного контроля**;
- сбор статистики;
- автоматическое обновление вирусных баз и компонентов программы;

- поддержка единых настроек приложения на распределенной системе межсетевых экранов, в том числе, объединенных в кластер.

Антивирус Dr.Web *Light* использует вирусные базы, которые постоянно пополняются новыми записями, что обеспечивает высокий уровень защиты и своевременное реагирование на появление новых угроз. Также в программе реализован эвристический анализатор для дополнительной защиты от неизвестных вирусов.

Проверяемые объекты

Антивирус Dr.Web *Light* сканирует все объекты до того, как они передаются клиенту для обработки.

Объекты проверки трафика, поступающего по протоколам HTTP и FTP поверх HTTP

Антивирус Dr.Web *Light* производит проверку HTTP- и FTP-трафика, проходящего через межсетевой экран Microsoft ISA Server и Forefront TMG, в реальном времени. Объектом проверки является ресурс, указанный в запросе клиента. Microsoft ISA Server и Forefront TMG либо подключаются к указанному в запросе серверу и получают ресурс от него, либо возвращают ресурс из собственного кэша. Фильтры приложения выполняют перехват полученных данных (включая данные в архивах и упакованные данные) и формируют временный буфер либо файл, который потом анализируется антивирусной системой.

В большинстве случаев проведение антивирусной проверки возможно только при наличии всего файла целиком. Поэтому накопление и сканирование запрашиваемых данных может занять дополнительное время.

Лицензирование

Права пользователя на использование **Антивируса Dr.Web *Light*** регулируются при помощи специального файла, называемого *лицензионным ключевым файлом*.

Лицензионный ключевой файл

Ключевой файл имеет расширение .key и содержит, в частности, следующую информацию:

- срок действия лицензии;
- перечень компонентов, разрешенных к использованию;
- другие ограничения (в частности, количество пользователей, защищаемых приложением).

Ключевой файл является *действительным* при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- ключ распространяется на все используемые программой модули;
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится *недействительным*, при этом **Антивирус Dr.Web *Light*** перестает обнаруживать вредоносные программы. Факт нарушения корректности ключевого файла записывается в журнал регистрации событий операционной системы, а также в текстовый журнал регистрации событий программы.

Ключевой файл имеет формат, защищенный от редактирования. Редактирование файла делает его недействительным. Поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.

Получение ключевого файла

Вы можете получить лицензионный ключевой файл одним из следующих способов:

- в виде ZIP-архива по электронной почте;
- вместе с дистрибутивом продукта, если лицензионный файл был включен в состав дистрибутива при его комплектации;
- на отдельном носителе в виде файла с расширением .key.

Ключевой файл необходимо приобрести до установки **Антивируса Dr.Web *Light***, т.к. для установки потребуется указать путь к вашему ключевому файлу.

Получение ключевого файла по электронной почте

1. Зайдите на сайт, адрес которого указан в регистрационной карточке, прилагаемой к продукту.
2. Заполните форму со сведениями о покупателе.
3. Введите регистрационный серийный номер (находится на регистрационной карточке).
4. Ключевой файл будет выслан по указанному вами адресу электронной почты в виде ZIP-архива, содержащего файл с расширением .key.
5. Извлеките ключевой файл на компьютер, на который вы планируете установить **Антивирус Dr.Web *Light***.

Для ознакомления с программой можно получить *демонстрационный ключевой файл*. Такой ключевой файл обеспечивает полную функциональность основных антивирусных компонентов, но имеет ограниченный срок действия и не предполагает оказание технической поддержки пользователю.

Для получения демонстрационного ключевого файла (по электронной почте) следует зарегистрироваться на веб-сайте http://download.drweb.com/demoreq/.

Чтобы купить лицензионный ключевой файл, свяжитесь с ближайшим партнером **«Доктор Веб»** в вашем регионе либо воспользуйтесь услугами интернет-магазина на сайте компании по адресу http://buy.drweb.com/.

Дополнительную информацию о лицензировании и ключевых файлах можно найти на официальном сайте компании **«Доктор Веб»** по адресу http://www.drweb.com/.

Обновление лицензии

В некоторых случаях, например, при окончании срока действия лицензии или при изменении характеристик защищаемой системы или требований к ее безопасности, вы можете принять решение о приобретении новой или расширенной лицензии на **Антивирус Dr.Web *Light***. В таком случае вам потребуется заменить уже существующий и зарегистрированный в системе лицензионный ключевой файл. Приложение поддерживает обновление лицензии «на лету», при котором его не требуется переустанавливать или прерывать его работу.

Замена ключевого файла

1. Чтобы обновить лицензию, замените имеющийся ключевой файл в каталоге установки программы (%DrWeb for ISA Server%) новым ключевым файлом.
2. **Антивирус Dr.Web *Light*** автоматически переключится на использование нового ключевого файла.

Дополнительную информацию о сроках и типах лицензирования можно найти на официальном сайте компании **«Доктор Веб»** по адресу http://www.drweb.com/.

Принципы работы Антивируса Dr.Web Light

Все антивирусные решения **«Доктор Веб»** содержат следующие основные компоненты, обеспечивающие защиту всех операционных систем и платформ: антивирусное ядро **drweb32.dll** и файлы вирусных баз (с расширением **.vdb**), в которых хранятся и регулярно обновляются вирусные записи, содержащие различную информацию о вирусах и иных вредоносных кодах.

Антивирусное решение **Dr.Web для Microsoft ISA Server и Forefront TMG *Light*** интегрирует технологии **«Доктор Веб»** в процесс обработки данных службой межсетевого экрана Microsoft ISA Server и Microsoft Forefront TMG.

Продукт имеет веб-интерфейс администратора для удобного управления настройками сканирования и отслеживания вирусных событий сервера через браузер. Подробное описание настроек см. в главе Dr.Web for ISA Web Console.

Веб-фильтр

Антивирус Dr.Web *Light* осуществляет перехват данных сетевых соединений для последующей антивирусной проверки с помощью специального фильтра, встраиваемого в службу Microsoft Firewall Service (для Microsoft ISA Server) или Microsoft Forefront TMG Firewall (для Microsoft Forefront TMG).

Фильтр реализован в виде динамической библиотеки (основанной на модели ISAPI), запускаемой при старте службы межсетевого экрана Microsoft Firewall Service или Microsoft Forefront TMG Firewall и остающейся в памяти до завершения работы этой службы. В момент старта служба межсетевого экрана назначает фильтру определенные сетевые события, при возникновении которых Microsoft ISA Server или Microsoft Forefront TMG будет передавать ему управление. Фильтр получает доступ к потоку данных,

связанных с сеансом «клиент-сервер» в службе межсетевого экрана. Если на запрос (request) клиента или ответ (response) сервера создается событие, для которого зарегистрирован фильтр, фильтр выполняет перехват и анализирует содержащихся в потоке данные.

В состав **Антивируса Dr.Web *Light*** входит веб-фильтр **Dr.Web HTTP Web Filter**, в задачу которого входит проверка межсетевого трафика на наличие вирусов. Фильтр является самостоятельным модулем-подписчиком главного управляющего сервиса **Dr.Web CMS** и по мере его загрузки в память процесса wspsrv.exe связывается с управляющим сервисом и начинает отображаться в **Административной консоли CMS**.

Dr.Web HTTP Web Filter (библиотека DrWebHttpMonitor.dll, расположенная в каталоге %Microsoft ISA Server%\DrWeb\ или % Microsoft Forefront Threat Management Gateway%\DrWeb\ в зависимости от используемой версии межсетевого экрана) – веб-фильтр, представляющий собой расширение времени выполнения (run-time extension) встроенного в Microsoft ISA Server/Microsoft Forefront TMG фильтра Web Proxy Filter и реагирующий на его события. **Dr.Web HTTP Web Filter** отображается в дереве консоли управления Microsoft ISA Server или Microsoft Forefront TMG (см. Рисунок 1а, Рисунок 1б):

- на вкладке **Web Filters** в разделе **Configuration** -> **Add-ins** консоли Microsoft ISA Server;
- на вкладке **Web Filters** в разделе **System** в консоли Microsoft Forefront TMG.

При этом фильтр **Dr.Web HTTP Web Filter** не отображается на вкладке свойств HTTP-протокола:

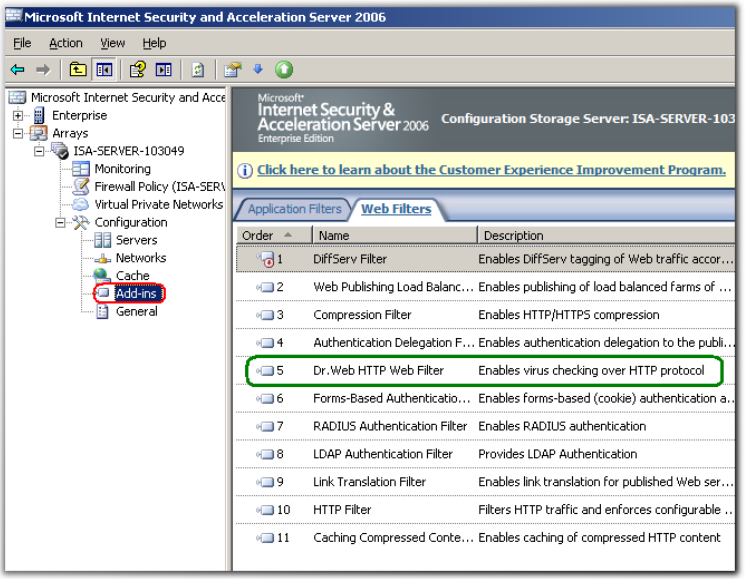

Рисунок 1а. Фильтр Dr.Web HTTP Web Filter в консоли Microsoft ISA Server

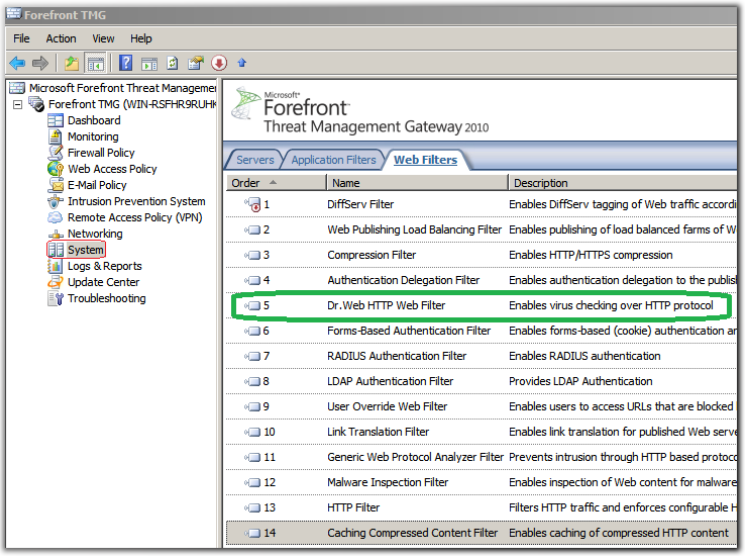

Рисунок 16. Фильтр Dr.Web HTTP Web Filter в консоли Microsoft Forefront TMG

Dr.Web HTTP Web Filter

Работа фильтра **Dr.Web HTTP Web Filter** определяется набором параметров в Административной консоли CMS, доступных в группе настроек **Application Settings** для **DrWebHttpMonitor_1.0**.

Подготовка к антивирусной проверке в контексте сессии «клиент-сервер» начинается с момента отправки сервером данных обратно клиенту, либо извлечения запрашиваемых данных из кэша (cache) Microsoft ISA Server или Microsoft Forefront TMG при установленном значении **false** параметра **PassCached** (значение по умолчанию).

При изменении значения параметра **PassCached** на **true** приложение перестает сканировать объекты, получаемые из кэша межсетевого экарана, поэтому перед включением данного режима работы рекомендуется очистить кэш. Для этого отключите

использование кэша в консоли управления межсетевого экрана, после чего удалите файл кэша (находится в папке Urlcache на каждом диске, настроенном для кэширования). После удаления файла кэша включите кэширование.

Поскольку объектом антивирусной проверки является ресурс, указанный в запросе клиента, фильтр **Dr.Web HTTP Web Filter** анализирует пакеты протокола, собирая ресурс, как буфер, либо временный файл (если размер ресурса достаточно велик) для последующего антивирусного сканирования.

Если URL не заблокирован Офисным контролем, ресурс может находиться в одном из четырех состояний (два неопределенных и два определенных состояния ресурса соответственно):

- не подтвержден (не верифицирован);
- состояние ресурса неизвестно;
- инфицирован;
- чист (не содержит угроз).

Как только получен результат антивирусного сканирования, ресурс переходит в определенное состояние на период верификации, задаваемый параметром **ResetCachePeriodInSec** и равный по умолчанию 30 минутам с момента окончания сканирования:

- если по результатам сканирования ресурс не содержит угроз, для всех защищаемых межсетевым экраном пользователей на весь период верификации разрешается полный доступ к ресурсу;
- если по результатам сканирования ресурс инфицирован, фильтр **Dr.Web HTTP Web Filter** инициирует ответ "**403 Forbidden. Infected by virus**";
- если другие пользователи инициировали собственные циклы проверки ресурса, до наступления определенного состояния ресурса, то по окончании сканирования по их запросам состояние ресурса будет изменено или продлено в зависимости от результата сканирования опять же на период верификации. В конечном счете, по истечении периода верификации с момента последнего сканирования ресурс вернется к состоянию не верифицирован, и любой

его повторный запрос запустит новый цикл подтверждения ресурса;

- если к ресурсу так никто и не обратится, то записи о нем будут удалены из системы через промежуток времени, заданный параметром **CleanupCachePeriodInResetPeriod** (измеряется количеством периодов верификации).

Службы Антивируса Dr.Web Light

Работу **Антивируса Dr.Web *Light*** обеспечивают шесть основных служб (сервисов):

- **Dr.Web Scanning Engine** – содержит ядро антивирусной системы **Dr.Web**.
- **Dr.Web CMS** – поддерживает распределенную систему управления компонентами приложения, реализуя основной функционал по контролю работоспособности отдельных модулей и их функциональную диагностику. Сервис поддерживает базу данных настроек компонентов приложения, базу событий и отслеживает статистику рабочих параметров компонентов.
- **Dr.Web CMS Web Console** – содержит встроенный веб-сервер, предоставляющий возможность запуска административных консолей приложения в браузере.
- **Dr.Web for MSP Component Host** – инстанцирует в себе все запрашиваемые в процессе работы вспомогательные компоненты приложения.
- **Dr.Web for MSP Requests Queue** – поддерживает асинхронную очередь запросов на выполнение заданий приложения, допускающих отложенное выполнение.
- **Dr.Web SSM** – контролирует работу приложений, работающих на платформе CMS, и отвечает за перезапуск основных служб.

Службы **Dr.Web Scanning Engine**, **Dr.Web CMS** и **Dr.Web SSM** запускаются сразу после установки приложения. Остальные службы запускаются по мере возникновения необходимости в их использовании.

При перезапуске служб вручную важно соблюдать правильный порядок остановки служб **Dr.Web CMS** и **Dr.Web SSM** из-за установленных зависимостей между ними: необходимо сначала остановить службу **Dr.Web SSM**, а после нее **Dr.Web CMS**. После того как обе службы будут остановлены, достаточно запустить службу **Dr.Web SSM**, через некоторое время приложение в целом придет в рабочее состояние автоматически.

Установка и удаление

Перед установкой или удалением **Антивируса Dr.Web *Light*** обязательно проверьте, что на компьютере, где установлен Microsoft ISA Server или Microsoft Forefront TMG, включена встроенная учетная запись системного администратора!

В противном случае возможно возникновение ситуаций, когда у системного установочного компонента недостаточно привилегий для создания и/или удаления компонентов приложения. Если по этой причине произошел сбой в процессе удаления, приводящий к неработоспособности межсетевого экрана, см. приложение Удаление Антивируса Dr.Web *Light* вручную.

Антивирус Dr.Web *Light* поставляется в виде установочного файла (**drweb-600-isa-20042006-x86-light.exe** или **drweb-600-tmg-2010-x64-light.exe** в зависимости от используемого межсетевого экрана) или в виде папки, помещенной в ZIP-архив и содержащей установочный файл.

Извлеките установочный файл на локальный диск сервера.

Если вы используете компонент Windows Terminal Services, для установки **Антивируса Dr.Web *Light*** рекомендуется воспользоваться стандартной утилитой Windows **Установка и удаление программ**.

Антивирус Dr.Web *Light* не совместим с другими антивирусными программами. Установка нескольких антивирусных продуктов на один компьютер может привести к системным ошибкам и потере важных данных. Если на компьютере уже установлена какая-либо версия данного антивирусного продукта или другой антивирус, то его необходимо удалить, используя установочный файл или стандартные средства операционной системы (см. Удаление Антивируса Dr.Web *Light*). Кроме того, **Антивирус Dr.Web *Light*** совместим с другими продуктами **Dr.Web** для серверов Windows только в пределах одной версии.

При большой нагрузке на сервер рекомендуется вручную остановить службу Microsoft Firewall Service (или Microsoft Forefront TMG Firewall). По завершении установки запуск службы будет произведен автоматически.

Включение регистрации событий в процессе установки/удаления

При необходимости, вы можете настроить регистрацию событий в процессе установки/удаления для дальнейшего контроля и отладки приложения. Для этого выполните следующие действия:

1. В консоли запуска программ **Пуск** -> **Выполнить**, запущенной от имени администратора, перейдите в директорию, содержащую установочный файл.
2. Запустите установочный файл программы с помощью команды:
   - `drweb-600-isa-20042006-x86-light.exe /V"/lvx* <log_name.log>"` (при использовании межсетевого экрана Microsoft ISA Server)

- `drweb-600-tmg-2010-x64-light.exe /V"/lvx* <log_name.log>"` (при использовании Microsoft Forefront TMG),

где log_name.log - имя файла журнала.

Системные требования

В данном разделе представлены системные требования, необходимые для правильной установки и работы **Антивируса Dr.Web *Light***.

Аппаратные требования

Характеристика	Требование	
	при использовании Microsoft ISA Server	при использовании Microsoft Forefront TMG
CPU	Процессор с тактовой частотой 733 МГц и выше	Процессор с тактовой частотой 1.86 ГГц и выше
RAM	1 Гбайт и больше	2 Гбайт и больше
Свободное пространство на диске	300 Мбайт для установки. Дополнительный необходимый размер свободного дискового пространства требуется для временного хранения данных на этапе антивирусной проверки. Он определяется интенсивностью пользовательских запросов и размерами файлов, загружаемых пользователями.	
Монитор	VGA-совместимый монитор	

Требования к ОС и программному обеспечению

Характеристика	Требование	
	при использовании Microsoft ISA Server	при использовании Microsoft Forefront TMG
ОС	Одна из следующих: • Microsoft® Windows Server® 2003 x86 с Service Pack 1 (SP1); • Microsoft® Windows Server® 2003 R2 x86.	Одна из следующих: • Microsoft® Windows Server® 2008 SP2 • Microsoft® Windows Server® 2008 R2
Файловая система	NTFS	
Межсетевой экран	Microsoft® ISA Server 2004 Microsoft® ISA Server 2006	Microsoft® Forefront® TMG 2010 (Standard Edition или Enterprise Edition) с установленным пакетом SP1 или SP2
Прочее ПО	Microsoft Windows Installer 3.1 или выше Microsoft .NET Framework 3.5 SP1 Internet Explorer 7 и выше или Mozilla FireFox 3.5 и выше	

Установка Антивируса Dr.Web Light

Перед установкой настоятельно рекомендуется:

- установить все критические обновления, выпущенные компанией Microsoft для ОС, которая используется на компьютере (они доступны на сайте обновлений по адресу http://windowsupdate.microsoft.com);
- проверить файловую систему при помощи стандартных средств и исправить обнаруженные ошибки;
- завершить работу всех приложений.

Чтобы установить Антивирус Dr.Web *Light*:

1. Остановите сервис межсетевого экрана Microsoft ISA Server/ Microsoft Forefront TMG.
2. Убедитесь, что процесс установки будет запущен под встроенной учетной записью системного администратора.
3. Запустите установочный файл программы:
   - **drweb-600-isa-20042006-x86-light.exe**, если вы используете Microsoft ISA Server;
   - **drweb-600-tmg-2010-x64-light.exe**, если вы используете Microsoft Forefront TMG.

   Откроется окно с предложением выбрать язык установки. Вы можете выбрать русский или английский язык. Нажмите кнопку **OK**.
4. Откроется окно Мастера установки программы. Нажмите кнопку **Далее**.
5. Откроется окно с текстом Лицензионного соглашения. Для продолжения необходимо прочитать и принять соглашение, выбрав пункт **Я принимаю условия лицензионного соглашения**. Нажмите кнопку **Далее**.
6. Выберите вариант лицензирования. Вы можете использовать ключ, полученный от **Центра управления Dr.Web**, либо локальный ключ. Нажмите кнопку **Далее**.

7. Если на предыдущем шаге установки вы выбрали использование локального ключа, необходимо указать путь к нему. Для этого нажмите кнопку **Обзор** и выберите необходимый файл. Нажмите кнопку **Далее**.

Если у вас нет действующего ключевого файла, то нажмите кнопку **Получить ключевой файл**, чтобы перейти на страницу запроса ключевого файла на сайте компании **«Доктор Веб»** по адресу http://www.drweb.com.

8. На шаге **Готова к установке программы** нажмите кнопку **Установить**, после чего начнется установка **Антивируса Dr.Web *Light*** на ваш компьютер.
9. Если сервис межсетевого экрана Microsoft ISA Server/ Microsoft Forefront TMG не был остановлен на шаге 1, будет предпринята попытка автоматически остановить его в течение определенного времени. Если сервис не удастся остановить автоматически, откроется окно, позволяющее повторить попытку или отменить установку программы и вернуть систему в исходное состояние. Чтобы продолжить установку программы, вы можете остановить сервис межсетевого экрана Microsoft ISA Server/Microsoft Forefront TMG вручную.
10. Последующие действия Мастера установки не требуют вмешательства пользователя. По завершении установки нажмите кнопку **Готово**.

Во время установки программы будет перезапущен Microsoft ISA Server/Microsoft Forefront TMG. По завершении установки убедитесь, что сервис Microsoft Firewall Service/Microsoft Forefront TMG Firewall запущен. Если сервис не запустился, необходимо запустить его вручную.

Чтобы переустановить Антивирус Dr.Web *Light*:

1. Остановите сервис межсетевого экрана Microsoft ISA Server/ Microsoft Forefront TMG.
2. Удалите **Антивирус Dr.Web *Light***. Файл настроек приложения **cmsdb** не удаляется автоматически при удалении приложения. Таким образом, все пользовательские настройки сохраняются и могут быть использованы при повторной установке. Однако при установке новой версии приложения набор настроек базовой конфигурации может быть расширен или изменен, в результате чего использование сохраненного файла не представляется возможным, поскольку может привести к сбоям в работе приложения. Если вы хотите использовать сохраненные настройки приложения, обратитесь в техническую поддержку компании **«Доктор Веб»** для уточнения совместимости настроек платформы **Dr.Web CMS** в разных версиях приложения. Если в более поздней версии появились новые параметры, в общем случае достаточно добавить в существующую базу настроек недостающие переменные, правильно указав их тип и значения по умолчанию.
3. Удалите вручную файлы **cmsdb** и **cmstracedb** из каталога %ProgramFiles%\DrWeb for ISA Server.
4. Выполните установку **Антивируса Dr.Web *Light***, следуя описанным выше инструкциям.

Удаление Антивируса Dr.Web Light

Чтобы удалить Антивирус Dr.Web *Light*:

1. Остановите сервис межсетевого экрана Microsoft ISA Server/ Microsoft Forefront TMG.
2. Убедитесь, что процесс удаления будет запущен под встроенной учетной записью системного администратора.

3. Запустите установочный файл программы:
   - **drweb-600-isa-20042006-x86-light.exe**, если вы используете Microsoft ISA Server;
   - **drweb-600-tmg-2010-x64-light.exe**, если используется Microsoft Forefront TMG.

   Откроется окно Мастера установки. Нажмите кнопку **Далее**.

Вы также можете воспользоваться стандартной утилитой Windows **Установка и удаление программ**, доступной через Панель управления.

4. Выберите пункт **Удалить** и нажмите **Далее**.
5. В открывшемся окне нажмите кнопку **Удалить**.
6. По окончании удаления нажмите кнопку **Закрыть**.

Во время удаления будет перезапущен Microsoft ISA Server/ Microsoft Forefront TMG. По окончании удаления убедитесь, что сервис Microsoft Firewall Service/Microsoft Forefront TMG Firewall запущен. Если сервис не запустился, необходимо запустить его вручную.

При возникновении сбоев в работе межсетевого экрана и ошибок при удалении **Антивируса Dr.Web *Light*** вы можете удалить программу вручную.

Dr.Web for ISA Web Console

Работа **Антивируса Dr.Web *Light*** может быть настроена с помощью **Веб-консоли Администратора** (см. Рисунок 2).

Запуск консоли Dr.Web for ISA Web Console

Для корректной работы **Веб-консоли Администратора** необходимо использовать следующие браузеры:

- Internet Explorer 7 или выше;
- Mozilla Firefox 3.5 или выше.

Кроме того, для корректной работы **Веб-консоли Администратора** в браузере Internet Explorer требуется разрешить использование технологии AJAX, отключив режим усиленной безопасности для администраторов:

- в ОС Windows Server 2003: в разделе **Панель управления** -> **Установка и удаление программ** -> **Установка компонентов Windows** снимите флажок **Internet Explorer Enchanced Security Configuration** и нажмите кнопку **Далее**. Затем нажмите кнопку **Готово**;
- в ОС Windows Server 2008: запустите **Менеджер сервера** (**Server manager**) и выберите пункт **Настроить конфигурацию усиленной безопасности Internet Explorer** (**Configure IE ESC**), после чего выберите соответствующую опцию в разделе **Администраторы** (**Administrators**).

Для запуска **Веб-консоли Администратора** откройте в браузере следующую страницу:

`https://`*<ISA Server address>*`:2080/isa`,

где *<ISA Server address>* – это IP-адрес сервера ISA/Forefront TMG.

Для доступа к странице веб-консоли необходимо ввести данные учетной записи администратора. Добавить, изменить или удалить учетные записи администраторов можно с помощью административной веб-консоли Dr.Web CMS Web Console.

При первом запуске веб-консоли используйте данные учетной записи по умолчанию: имя пользователя **root** и пароль **drweb**.

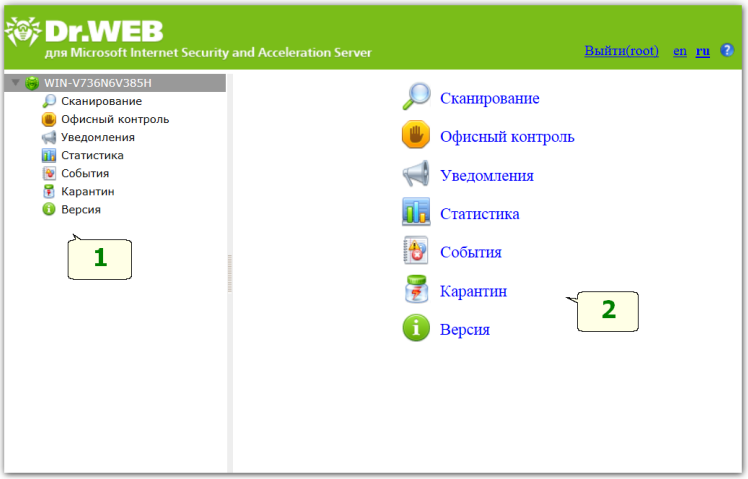

Рисунок 2. Веб-консоль Администратора

Интерфейс

Веб-консоль состоит из двух частей:

1. Дерево веб-консоли, используемое для навигации по различным разделам настроек программы.
2. Область сведений, в которой отображаются настройки выбранного в данный момент раздела и в которой их можно изменять.

В верхней части области сведений находится опция смены языка **Веб-консоли Администратора**. Вы можете выбрать русский или английский язык. Кроме того, справа от опции выбора языка находится опция вызова справки по веб-консоли.

Сканирование

Процесс сканирования настраивается в разделе настроек **Сканирование**. Изменение параметров в этом разделе влияет на типы проверяемых объектов, а следовательно, на уровень защищенности сервера. С другой стороны, увеличение числа типов объектов для проверки может привести к снижению производительности сервера.

Чтобы настроить параметры сканирования:

1. Выберите пункт **Сканирование** для настраиваемого профиля в дереве веб-консоли. Откроется область сведений для настройки сканирования (см. Рисунок 3).

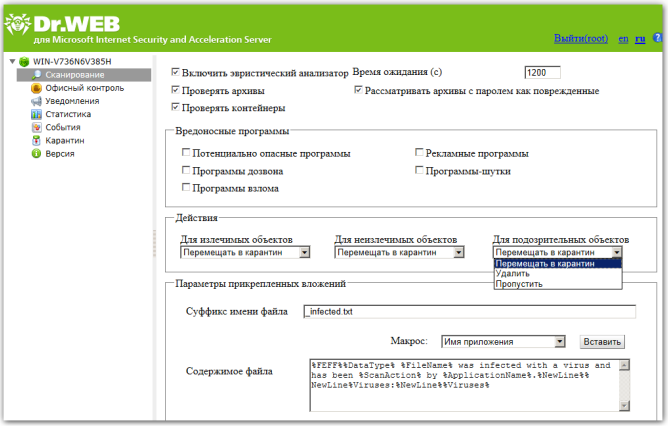

Рисунок 3. Раздел настроек сканирования

2. По умолчанию включены эвристический анализатор и проверка прикрепленных архивов и контейнеров. Это обеспечивает более надежную защиту, но приводит к некоторому уменьшению производительности сервера. Чтобы отключить эти режимы, снимите флажки **Включить эвристический анализатор**, **Проверять архивы** и **Проверять контейнеры** в верхней части области сведений раздела **Сканирование**.

Отключать эвристический анализатор и проверку прикрепленных архивов не рекомендуется, т.к. это приведет к существенному снижению уровня защищенности сервера.

Рядом с этими флажками находится поле ввода для времени ожидания на сканирование одного файла. Если при проверке файла время ожидания истекло, то файл считается поврежденным. По умолчанию задано 1200000 мс. При необходимости вы можете изменить это значение.

Флажок **Рассматривать архивы с паролем как поврежденные** определяет, будет ли программа игнорировать такие архивы или применять к ним действия, заданные для поврежденных объектов.

3. В группе настроек **Вредоносные программы** вы можете указать типы вредоносных объектов, которые следует искать в интернет-трафике. Для этого установите соответствующие флажки.

4. Ниже, в группе настроек **Действия**, укажите желаемые действия для излечимых, неизлечимых и подозрительных объектов, используя соответствующие выпадающие списки. Вы можете выбрать одно из следующих действий:
   - **Перемещать в карантин** – означает, что тело письма будет пропущено, а вложенный файл отправлен в карантин (см. Карантин);
   - **Удалить** – означает, что объект будет удален;
   - **Пропустить** – означает, что письмо будет пропущено и направлено получателю (действие доступно только для подозрительных объектов).

По умолчанию для всех типов объектов выбрано действие **Перемещать в карантин**.

5. В группе настроек **Параметры прикрепленных вложений** вы можете изменить суффикс имени файла, который прилагается к письму после того, как программа совершит над ним выбранное действие. В поле **Текст** можно изменить содержимое прикрепленного текстового файла. При редактировании текста вы можете использовать макросы. Для добавления макроса выберите его в списке **Макрос** и нажмите кнопку **Вставить**.
6. Нажмите кнопку **Сохранить**, когда закончите изменять настройки параметров сканирования.

Офисный контроль

Офисный контроль позволяет ограничить доступ пользователей к интернет-ресурсам и тем самым оградить их от просмотров нежелательных веб-сайтов (сайтов, посвященных насилию, азартным играм и т.п.) или разрешить пользователям доступ только к тем сайтам, которые определены настройками **Офисного контроля**.

Чтобы настроить Офисный контроль:

1. Выберите пункт **Офисный контроль** для настраиваемого профиля в дереве веб-консоли. Откроется область сведений для настройки **Офисного контроля** (см. Рисунок 4).

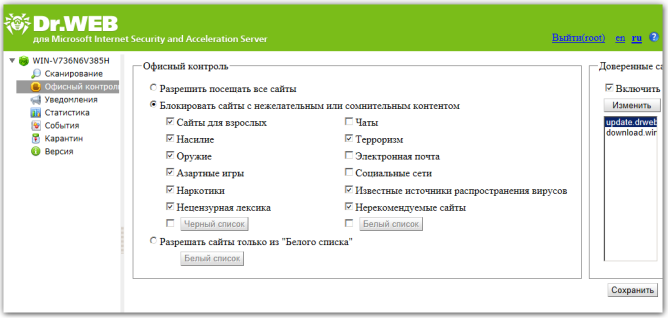

Рисунок 4. Раздел настройки Офисного контроля

2. Вы можете выбрать один из следующих вариантов работы:
   - **Разрешить посещать все сайты** – в этом режиме ограничений на доступ к веб-ресурсам нет;
   - **Блокировать сайты с нежелательным или сомнительным контентом** – в этом режиме вы можете указать категории тех ресурсов, доступ к которым вы хотите ограничить. Также фильтр позволяет вам самостоятельно указать сайты, доступ к которым вы можете запретить или разрешить вне зависимости от других ограничений. Для настройки блокируемых ресурсов нажмите кнопку **Черный список**, укажите ресурс и нажмите **Добавить**. Для настройки разрешенных ресурсов нажмите кнопку **Белый список**, укажите ресурс и нажмите **Добавить**;

Списки адресов веб-сайтов, относящихся ко всем тематическим категориям, регулярно обновляются модулем автоматического обновления вместе с обновлением вирусных баз.

- **Разрешать сайты только из "Белого списка"** – в этом режиме доступ будет запрещен ко всем веб-ресурсам, кроме указанных в Белом списке. Для создания списка разрешенных ресурсов нажмите кнопку **Белый список**, укажите ресурс и нажмите **Добавить**.

3. Кроме того, вы можете дополнительно включить использование списка доверенных сайтов. Для этого установить флажок **Включить** в разделе **Доверенные сайты**. Для редактирования списка доверенных ресурсов, нажмите кнопку **Изменить**, укажите ресурс и нажмите **Добавить**.
4. Нажмите кнопку **Сохранить**, когда закончите изменять настройки **Офисного контроля**.

Формирование списка доменных адресов

1. Введите в поле ввода доменное имя (часть доменного имени):
   - если вы хотите добавить в список определенный сайт, введите его полный адрес (например, **www.example.com**). Доступ ко всем ресурсам, расположенным на этом сайте будет разрешен/запрещен;
   - если вы хотите разрешить/запретить доступ к тем веб-сайтам, в адресе которых содержится определенный текст, введите в поле этот текст. Например: **example**. Доступ к адресам example.com, example.test.com, test.com/example, test.example222.ru и т.п. будет заблокирован/разрешен;

   В том случае, когда введенная строка содержит символ «**.**», данная строка будет рассматриваться как имя домена. Тогда все ресурсы, находящиеся на этом домене будут отфильтрованы.

   Если данная строка содержит и символ «**/**» (например, **example.com/test**), то та часть, что стоит слева от символа, будет считаться доменным именем, а части справа от символа – частью разрешенного/блокируемого на данном домене адреса (таким образом, будут отфильтрованы такие адреса как example.com/test11, template.example.com/test22 и т.п.).

2. Нажмите кнопку **Добавить**, расположенную справа. Адрес (часть адреса) будет добавлен в список, расположенный выше.

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

3. Чтобы удалить какой-либо ресурс из списка, выберите его в этом списке и нажмите кнопку **Удалить**.

Уведомления

Уведомления заносятся в журнал операционной системы и используются для информирования администратора и пользователей сети о различных событиях, связанных с работой **Антивируса Dr.Web *Light*** (например, связанных с обнаружением инфицированных объектов).

Чтобы настроить уведомления:

1. Выберите пункт **Уведомления** в дереве веб-консоли. Откроется область сведений для настройки уведомлений (см. Рисунок 5).

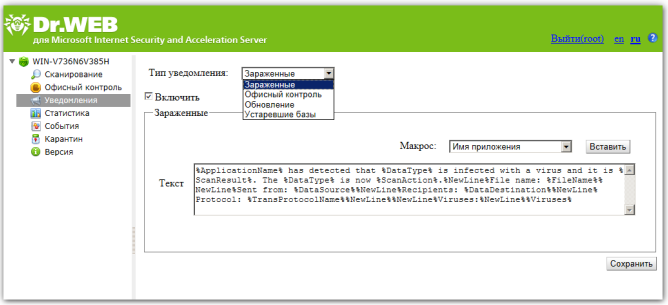

Рисунок 1. Раздел настройки уведомлений

2. В списке **Тип уведомления** выберите тип событий для отправки уведомлений:
   - **Зараженные** – для отправки уведомлений об обнаруженных вирусных угрозах;
   - **Офисный контроль** – для отправки уведомлений о фильтрации сетевых ресурсов с помощью **Офисного контроля**;
   - **Обновление** – для отправки уведомлений с информацией о последнем обновлении;
   - **Устаревшие базы** – для отправки уведомлении о необходимости обновить вирусные базы.
3. Чтобы включить отправку уведомлений выбранного типа, установите флажок **Включить**.
4. В разделе настроек ниже вы можете изменить шаблон уведомления выбранного типа в поле **Текст**. При редактировании текста вы можете использовать макросы.
5. Нажмите кнопку **Сохранить**, когда закончите изменять настройки уведомлений.

Просмотр статистики

Раздел **Статистика** позволяет просмотреть общие или средние количественные данные о работе **Антивируса Dr.Web *Light*** за определенный период времени (см. Рисунок 6).

Чтобы настроить отображение статистики:

1. В верхней части раздела **Статистика** выберите период, информация за который вас интересует, в выпадающем списке **Период статистики**. Вы можете выбрать одно из следующих значений:
   - **За все время** – для просмотра статистики за все время с начала работы **Антивируса Dr.Web *Light***;
   - **За день** – для просмотра статистики за последние сутки работы **Антивируса Dr.Web *Light***;

- **За час** – для просмотра статистики за последний час работы **Антивируса Dr.Web *Light***;
- **За минуту** – для просмотра статистики за последнюю минуту работы **Антивируса Dr.Web *Light***;

2. В выпадающем списке **Тип статистики** выберите тип статистической информации. В зависимости от выбранного периода статистики вы можете настроить просмотр общих количественных показателей, средних за весь указанный период, а также минимальных и максимальных показателей в течение указанного периода.

Типы информации

В зависимости от выбранных настроек отображения раздел **Статистика** может содержать следующие подразделы:

- **Нагрузка**. В данном подразделе вы можете ознакомиться с информацией об общем размере проверенных объектов, а также о среднем, минимальном и максимальном размере объектов, проверенных за выбранный период.

- **Результаты проверки**. Данный подраздел содержит информацию об общем количестве проверенных объектов, а также о количестве обработанных объектов различных типов.

- **Действия над проверенными**. Данный подраздел содержит статистическую информацию о действиях, которые были применены **Антивирусом Dr.Web *Light*** к обнаруженным вредоносным объектам.

- **Типы угроз**. В данном подразделе содержится информация о различных типах угроз, обнаруженных **Антивирусом Dr.Web *Light*** за выбранный период времени.

- **Категории сайтов**. В данном подразделе отображается статистика работы **Офисного контроля**, а также количество заблокированных ресурсов по категориям.

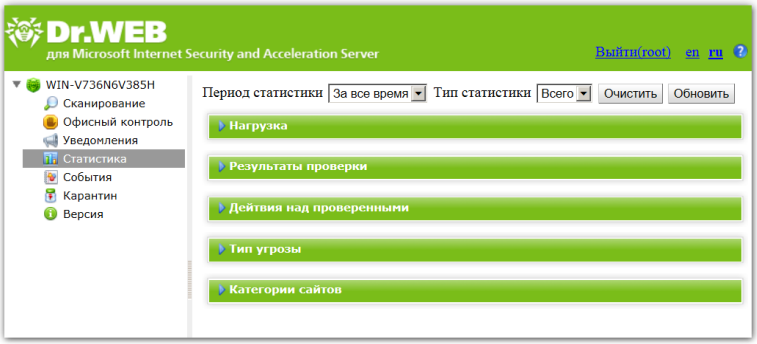

Рисунок 6. Раздел статистики

Чтобы обновить или очистить статистическую информацию, нажмите кнопку **Обновить** или **Очистить** соответственно.

Просмотр списка событий

Раздел **События** позволяет просмотреть все события, связанные с работой **Антивируса Dr.Web *Light*** (см. Рисунок 7).

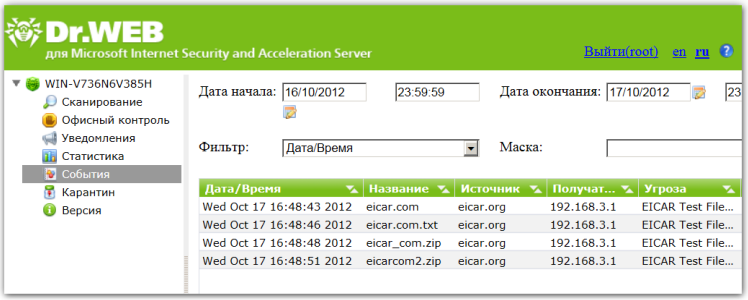

Рисунок 7. Раздел событий

Информация о событиях

Для каждого события в списке отображается следующая информация:

- дата и время;
- название ресурса;
- источник и приемник;
- название угрозы;
- действие.

Действия над списком событий

1. Вы можете настроить просмотр событий за определенный период времени. Для этого укажите дату и время начала и окончания интересующего интервала.
2. Для удобства поиска и просмотра определенного типа событий вы можете использовать фильтры. Выберите тип фильтра в выпадающем списке **Фильтр** и введите значение параметра фильтрации в поле **Маска**, после чего нажмите кнопку **Применить**.
3. Вы можете сохранить список событий в виде текстового файла. Для этого нажмите кнопку **Экспорт**.
4. Для того чтобы отсортировать записи в списке по тому или иному критерию, нажмите на соответствующий заголовок колонки.
5. Для обновления списка событий нажмите кнопку **Обновить**.

Карантин

Карантин Антивируса Dr.Web *Light* служит для изоляции подозрительных объектов, обнаруженных при проверке сетевого трафика.

В разделе **Карантин** веб-консоли выводится информация о текущем состоянии **Карантина**. Кроме того, для просмотра и редактирования содержимого **Карантина** вы можете

использовать **Менеджер Карантина**.

Управление Карантином с помощью Dr.Web for ISA Web Console

Для просмотра списка объектов в **Карантине** выберите пункт **Карантин** в дереве веб-консоли. Откроется область сведений **Карантина** (см. Рисунок 8).

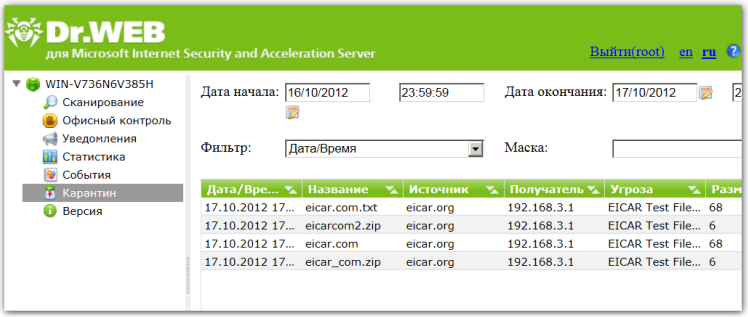

Рисунок 8. Список объектов в Карантине

Просмотр информации об объектах в карантине

Для каждого события в списке отображается следующая информация:

- дата и время;
- имя файла;
- источник и приемник;
- название угрозы;
- размер файла.

При просмотре списка объектов в **Карантине** доступны следующие опции:

1. Для просмотра объектов, перемещенных в **Карантин** в течение определенного периода времени, укажите даты и время начала и окончания интересующего вас интервала.

2. Для удобства поиска и просмотра информации об объектах в **Карантине** вы можете использовать фильтры. Выберите тип фильтра в выпадающем списке **Фильтр** и введите значение параметра фильтрации в поле **Маска**, после чего нажмите кнопку **Применить**.
3. Чтобы отсортировать записи в списке по тому или иному критерию, нажмите на соответствующий заголовок колонки.
4. Для обновления списка событий нажмите кнопку **Обновить**.

Действия над объектами в карантине

1. Чтобы удалить объект из списка, щелкните правой кнопкой мыши по объекту и выберите **Удалить** в контекстном меню. Чтобы удалить все объекты, нажмите Ctrl+A, затем выберите **Удалить**.
2. Чтобы восстановить объект, щелкните правой кнопкой мыши по объекту и выберите **Восстановить** в контекстном меню. Затем укажите путь для восстановления файла.

Менеджер Карантина

Для запуска **Менеджера Карантина** (см. Рисунок 9) выберите **Пуск** -> **Программы** -> **Dr.Web for ISA Server** -> **Quarantine**.

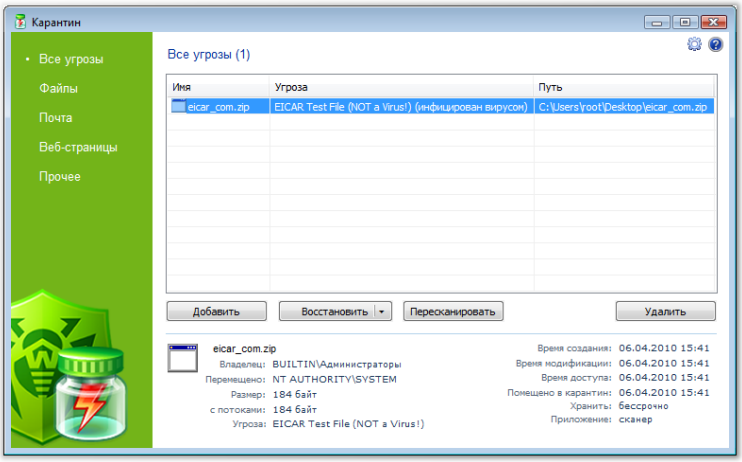

Рисунок 9. Главное окно утилиты Quarantine.

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 Dr.Web *Light*** при автоматическом перемещении объекта в карантин;
- **Путь** – полный путь, по которому находился объект до перемещения в **Карантин**.

В нижней части окна карантина отображается подробная информация о выделенных объектах **Карантина**. Вы можете включить отображение столбцов с подробной информацией об объекте, аналогичной данным в нижней части окна.

Чтобы настроить отображение столбцов:

1. Чтобы задать параметры отображения информации в таблице **Карантина**, щелкните правой кнопкой мыши по заголовку таблицы и выберите в контекстном меню пункт **Настроить колонки**.
2. Выберите типы информации, которые вы хотите включить в таблицу объектов. Чтобы исключить столбцы из таблицы объектов, снимите флажки напротив соответствующих пунктов. Чтобы добавить/исключить все типы информации нажмите кнопку **Отметить все**/**Снять отметки** соответственно.
3. Для изменения порядка следования столбцов в таблице выберите соответствующий столбец в списке и нажмите на одну из следующих кнопок:
   - **Вверх** – для перемещения столбца ближе к началу таблицы (вверх по списку в настройках и левее в таблице объектов);
   - **Вниз** – для перемещения столбца ближе к концу таблицы (вниз по списку в настройках и правее в таблице объектов).
4. 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** пользователи могут видеть только те файлы, к которым имеют права доступа.

Чтобы отобразить скрытые объекты, запустите файл **Карантина** `dwqrui.exe`, расположенный в каталоге установки, с административными правами.

Управление Карантином

Действия над объектами в Карантине

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. Путь для восстановления файла указан в колонке **Путь** на Рисунке 19. Если путь не указан, пользователю будет предложено выбрать папку для восстановления файла;

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

В выпадающем меню доступен 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 не является зараженным, **Карантин** предложит восстановить данный файл;
- **Удалить** – удалить файл из **Карантина** и из системы.

Чтобы применить действие к нескольким объектам одновременно, выберите их в окне **Карантина**, удерживая клавиши SHIFT или CTRL, затем щелкните правой кнопкой мыши на любой строке таблицы и в выпадающем меню выберите необходимое действие.

Кроме того, в контекстном меню в таблице доступна опция **Отправить файл(ы) в лабораторию «Доктор Веб»** для отправки файлов в **Антивирусную Лабораторию «Доктор Веб»** на проверку.

Настройка свойств Карантина

Чтобы настроить свойства Карантина:

1. Нажмите на кнопку  **Настройки** в окне **Карантина**.
2. Откроется окно **Свойства карантина**, в котором вы можете изменять следующие параметры:
   - в разделе **Задать размер карантина** вы можете управлять объемом дискового пространства, занимаемого папкой **Карантина** 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** выберите опцию **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.
3. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

Обновление вирусных баз

Информация о версии приложения, лицензии, вирусных базах, а также о дате, времени и результате последнего обновления программы находится в области сведений веб-консоли **Версия**.

Во время установки **Антивируса Dr.Web *Light*** в Планировщик Задач Windows (**C:\Windows\Tasks**) добавляется задание на обновление (**Dr.Web update for ISA plug-in**). Каждые 30 минут оно запускает модуль обновления **DrWebUpW.exe**, который загружает вирусные базы и компоненты программы.

Вы можете настроить данное задание, изменяя его параметры (для этого дважды щелкните по нему в списке заданий). Вы также можете настроить работу самого модуля обновления, добавляя параметры командной строки (см. Приложение А) в поле ввода **Выполнить** в параметрах задания.

Например, если вам необходимо настроить обновление без подключения к сети Интернет, сделайте следующее:

1. Создайте папку с любым именем на локальном диске (например, C:\MyDocs\DrWebUpdate).
2. Поместите туда обновляемые компоненты. Список доступных компонентов вы можете найти в файле **drweb32.lst**, расположенном в одном из следующих каталогов:
   - %AllUsersProfile%\Application Data\Doctor Web\Bases\, если используется Microsoft ISA Server;
   - %ProgramData%\Doctor Web\Bases\, если используется Microsoft Forefront TMG.
3. Добавьте следующий параметр командной строки в поле **Выполнить** в настройках задания **Dr.Web update for ISA plug-in**: `/URL:` *<путь к созданной папке>* (например, `/URL: "C:\MyDocs\DrWebUpdate"`).

Административная консоль CMS

Административная консоль CMS поддерживается отдельным сервисом **Dr.Web CMS Web Console**, который, в свою очередь, контролируется управляющим сервисом **Dr.Web CMS**.

Dr.Web CMS Web Console подключается к управляющему сервису по административному протоколу.

Запуск Административной консоли CMS

Для запуска **Административной консоли CMS** (см. Рисунок 10) откройте в браузере следующую страницу:

`https://`*<ISA Server address>*`:2080/admin`,

где *<ISA Server address>* – это IP-адрес сервера ISA/Forefront TMG.

Для доступа к странице **Административной консоли CMS** необходимо ввести данные учетной записи администратора. Добавить, изменить или удалить учетные записи администраторов можно с помощью административной веб-консоли Dr.Web CMS Web Console.

При первом запуске **Административной консоли CMS** используйте данные учетной записи по умолчанию: имя пользователя **root**, пароль **drweb**.

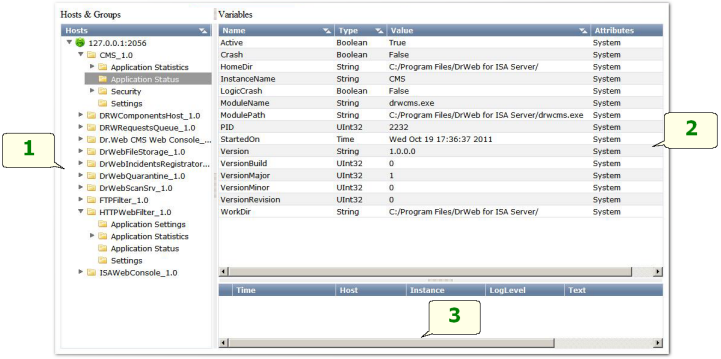

Рисунок 10. Административная консоль CMS

Интерфейс

Административная консоль CMS состоит из трех частей:

1. **Дерево хостов и групп**.

   В дереве отображаются хосты, к которым выполнено подключение. При щелчке по группе в окне переменных выводится список переменных. При щелчке правой кнопкой мыши по группе открывается контекстное меню, в котором доступны следующие функции:

   - создание группы;
   - переименование группы;
   - удаление группы;
   - создание переменной.

   При щелчке правой кнопкой мыши по хосту открывается контекстное меню, в котором доступны все перечисленные выше функции, а также добавляются следующие:

   - добавление хоста (добавляет в дерево подключение к новому хосту);
   - удаление хоста;
   - включение просмотра трассировки (включается отображение трассировки в режиме реального времени);

- загрузка событий (загружаются отфильтрованные сообщения за прошедшие периоды);
- редактирование фильтра событий (редактирование фильтра трассировки в режиме реального времени).

2. **Список переменных**.

   В окне переменных отображается список переменных в выбранной группе, а также их типы, атрибуты и значения. Если это не запрещено атрибутами, то при щелчке по полю можно отредактировать введенное в нем значение. При щелчке правой кнопкой мыши по переменной открывается контекстное меню, в котором доступны следующие функции:

   - создать переменную (открывает окно создания переменной);
   - удалить переменную (если позволяют атрибуты);
   - сбросить статистическую переменную (если переменная имеет атрибут Statistics).

3. **Окно отслеживания сообщений (трассировки)**.

   При включении трассировки в режиме реального времени в окне трассировки отображаются сообщения приложений. Сообщения можно отфильтровать с помощью специального фильтр трассировки. Каждая запись имеет следующие поля:

   - время события;
   - имя хоста;
   - имя приложения;
   - уровень детализации регистрации событий;
   - текст сообщения.

   При щелчке правой кнопкой мыши по списку событий выводится контекстное меню, содержащее опцию очистки списка событий.

Изменение пароля администратора

При первом запуске **Dr.Web for ISA Web Console** или **Административной консоли CMS** вход в систему осуществляется с помощью предустановленной учетной записи **root** с паролем **drweb**. Далее настоятельно рекомендуется изменить пароль для данной учетной записи.

Изменение пароля учетной записи администратора

1. В дереве хостов и групп выберите группу **CMS_1.0** -> **Security** -> **Users** -> **root**.
2. В списке переменных группы **root** дважды щелкните по значению **Value** переменной **Password**. Откроется окно **Change password variable value**.
3. Введите новый пароль в поле **Password**, а также в поле **Confirm password** для подтверждения сделанных изменений.

Добавление новых администраторов

Вы можете добавить необходимое количество учетных записей администратора, помимо предустановленной записи **root**.

Добавление учетной записи администратора

1. В дереве хостов и групп выберите группу **CMS_1.0** -> **Security** -> **Users**.
2. Щелкните по группе **Users**, чтобы открыть контекстное меню. В контекстном меню выберите пункт **Create group**.
3. Откроется окно **Enter new group name**, в котором необходимо ввести имя администратора в поле **Group name**. Далее нажмите кнопку **OK**.
4. Для настройки пароля администратора щелкните по соответствующей группе в дереве хостов и групп. Выберите пункт **Create variable** в контекстном меню.

5. Откроется окно **Add new variable**. Введите имя переменной **Password** и выберите **Password** в качестве ее типа. В поле **Value** введите пароль администратора. Далее нажмите кнопку **Append**.

Создание кластеров

Административная консоль CMS позволяет организовать неограниченное по вложенности дерево соединенных в кластер хостов. В организованном кластере любое изменение переменной с атрибутом **Shared** приводит к аналогичному изменению переменных на всех подчиненных хостах.

Организация кластера

На подчиненном (вводимом в кластер) хосте выполните следующие действия:

1. Создайте группу **/CMS_1.0/Security/Users/host**. Данная группа будет обозначать учетную запись пользователя, под которой головной хост будет иметь возможность транслировать переменные с атрибутом **Shared** на локальный сервер.
2. В группе **host** автоматически будет создана переменная **Password** типа **Password**, содержащая пароль для подключения к учетной записи. По умолчанию устанавливается пароль **drweb**. Из соображений безопасности данный пароль рекомендуется сменить.

На управляющем (головном) хосте выполните следующие действия:

1. Создайте группу с произвольным именем по пути **/CMS_1.0/Shared/**. Данная группа будет обозначать подчиненный хост.
2. В группе хоста автоматически создается переменная **Address** типа **String**, содержащая пустую строку. В качестве значения данной переменной указывается IP-адрес MS-подключения подчиненного хоста в виде <*IP-адрес*>:<*Порт*>, например, 192.168.1.1:2056.

3. В группе хоста также автоматически создается переменная **Password** типа **Password**, содержащая пароль для подключения к учетной записи **host** на подчиненном хосте. По умолчанию устанавливается пароль **drweb**. Из соображений безопасности данный пароль рекомендуется сменить. Если пароль для всех хостов одинаковый, то переменную **Password** можно создать в группе **Shared**. Тогда она будет использоваться по умолчанию для всех соединений.
4. Переменные, определяющие подключение к подчиненному хосту, не могут иметь атрибут **Shared**, соответственно, настройки соединения не могут транслироваться на подчиненные хосты. При попытке изменения атрибутов переменных настроек соединений будет выдано сообщение о запрете доступа.

В папке **Shared** автоматически создается переменная **Enabled** типа Boolean (см. Рисунок 11). Эта переменная включает и выключает функционал кластера. Если для данной переменой установлено значение **True**, все описанные соединения становятся активны, **False** - все соединения разрываются. По умолчанию переменная создается со значением **True**.

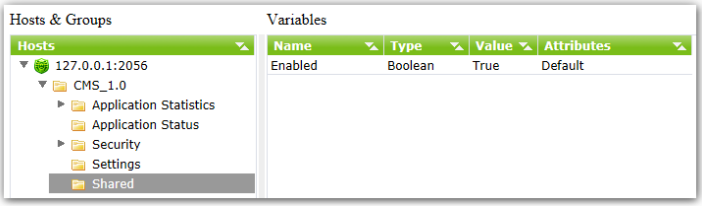

Рисунок 11. Переменная Enabled в папке Shared

При создании группы хоста в папке **Shared**, в ней автоматически создается переменная **Enabled** типа Boolean со значением по умолчанию **False**. Эта переменная включает и выключает конкретное соединение.

Изменение адреса (значения переменной **Address**) приводит к переподключению активного соединения на новый адрес. Изменение пароля не приводит к переподключению соединения. Для переподключения соединения с новым паролем необходимо выключить и включить соединение с помощью переменной **Enabled**.

При правильном создании подключения CMS автоматически установит соединение с подчиненным хостом и протранслирует на него все переменные с атрибутом **Shared**. Если на удаленном хосте уже есть переменная с таким именем, но у нее атрибут не **Shared**, то такая переменная будет проигнорирована с кодом возврата **MB_RC_SKIPPED**.

Список подчиненных хостов можно создать на любом уровне дерева.

Регистрация событий

Антивирус Dr.Web *Light* регистрирует ошибки и происходящие события в следующих журналах регистрации:

- журнале регистрации событий операционной системы (Event Log);
- текстовом журнале регистрации событий программы установки;
- журнал событий CMS.

Информация об обновлениях заносится в отдельный текстовый журнал **drwebupw.log**, расположенный в каталоге %alluserprofile %\AppData\Doctor Web\Logs\ (см. главу Проверка модуля обновления).

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;
- 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);

- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 дней до окончания срока).
- информация об обнаруженных вредоносных объектах (см. раздел Уведомления).

Просмотр журнала регистрации операционной системы

1. Чтобы просмотреть журнал регистрации событий операционной системы, откройте **Панель управления** операционной системы.
2. Выберите **Администрирование**, а затем выберите **Просмотр Событий**.
3. В левой части окна **Просмотр Событий** выберите **Приложение**. Откроется список событий, зарегистрированных в журнале пользовательскими приложениями. Источниками сообщений **Антивируса Dr. Web *Light*** являются приложения Dr.Web® Scanning Engine, Dr.Web CMS, Dr.Web CMS Web Console, Dr.Web for MSP Component Host и Dr.Web for MSP Requests Queue.

Текстовый журнал программы установки

Для упрощения процесса отладки в случае возникновения проблем и ошибок в процессе установки, программа установки ведет регистрацию событий. Файл регистрации событий drweb-isa-setup.log или drweb-tmg-setup.log (в зависимости от версии используемого межсетевого экрана) создается в каталоге C:\Windows\Temp, или же может быть найден по переменной окружения %temp%, т.е. при вызове **%temp%** в консоли запуска программ **Пуск** -> **Выполнить**.

Журнал событий CMS

Управляющий сервис ведет регистрацию событий приложений с различной степенью детализации:

Значение	Типы сообщений с различной степенью детализации
Audit	Сообщения этого уровня записываются самим управляющим сервисом и описывают события, возникающие при действиях администратора, например изменение значений переменных.
Incident	События безопасности, регистрируемые внешними приложениями, например обнаружение вирусов.
Fatal	События, приводящие к потере работоспособности приложения.
Error	Ошибки, после которых возможно нормальное функционирование приложения.
Warning	Сообщения о событиях, которые требуют внимания администратора.
Information	Информационные сообщения.
Debug	Отладочные сообщения.

Список событий сохраняется управляющим сервисом в отдельную базу данных.

Управляющий сервис имеет возможность отображения регистрируемых событий в режиме реального времени, фильтрации происходящих событий по различным параметрам, выгрузки зарегистрированных событий за прошедшие периоды с фильтрацией по различным параметрам.

С помощью изменения значения переменной **LogLevel** (UInt32) в группе **Settings**, обозначающей степень детализации регистрации событий приложения, можно выбрать оптимальный уровень детализации:

Значение	Степень детализации
0	Записываются только сообщения уровней Error, Fatal, Incident, Audit.
1	Ко всем предыдущим уровням добавляются сообщения уровня Warning.
2	Ко всем предыдущим уровням добавляются сообщения уровня Information.
3	Ко всем предыдущим уровням добавляются сообщения уровня Debug.

По умолчанию у всех приложений-подписчиков службы **Dr.Web CMS** устанавливается уровень детализации журнала событий, равный 2. При выборе опции **Debug Traces** в контекстном меню, открывающемся при щелчке правой кнопки мыши по корневому элементу дерева **Административной консоли CMS**, уровень детализации станет равным 3 для всех приложений-подписчиков. Однако включение данной опции сказывается на нагрузке и производительности системы, поэтому по возможности избегайте одновременного включения уровня 3 сразу для всех модулей. Если вам удалось локализовать проблему конкретного приложения-подписчика, вы можете изменить уровень детализации только для этого приложения.

При изменении уровня детализации событий на равный 3 в **Административной консоли CMS**, открытой в браузере Internet Explorer, и последующем включении опции просмотра событий в режиме реального времени **View Traces** необходимо контролировать объем памяти, выделяемой для процесса iexplorer.exe, соответствующего окну консоли. В таком режиме просмотра через некоторое время данный процесс может занять всю доступную память, что приведет к потере работоспособности системы.

Диагностика

Для проверки работоспособности приложения выполните следующие тесты, приведенные в данной главе:

- проверку правильности установки антивирусного приложения;
- проверку модуля обновления;
- проверку способности обнаруживать вирусы.

Проверка установки

Антивирус Dr.Web *Light* должен быть установлен в следующие папки:

1. Для Microsoft ISA Server:
   - %ProgramFiles%\DrWeb for ISA Server;
   - %Microsoft ISA Server%\DrWeb;
   - %ProgramFiles%\Common Files\Doctor Web;
   - %Documents and Settings%\All Users\Application Data\Doctor Web;
   - скрытая папка %DrWeb Quarantine%.
2. Для Microsoft Forefront TMG:
   - %ProgramFiles(x86)%\DrWeb for ISA Server;
   - %ProgramFiles(x86)%\Common Files\Doctor Web\Scanning Engine;
   - %ProgramFiles%\DrWeb for ISA Server;
   - %Microsoft Forefront Threat Management Gateway% \DrWeb;
   - скрытые папки %ProgramData%\Doctor Web и %DrWeb Quarantine%.

Убедитесь, что эти папки созданы и содержат файлы программы.

После этого откройте стандартную утилиту Windows **Просмотр Событий** (**Event Viewer**) и убедитесь, что не было зафиксировано ошибок, связанных с **Антивирусом Dr.Web**.

Наконец, убедитесь, что запущены следующие локальные сервисы:

- Dr.Web Scanning Engine (DrWebEngine);
- Dr.Web CMS;
- Dr.Web SSM;
- Dr.Web CMS Web Console;
- Dr.Web for MSP Component Host;
- Dr.Web for MSP Requests Queue.

Проверка модуля обновления

Модуль обновления **DrWebUpW.exe** автоматически запускается после установки **Антивируса Dr.Web *Light***. Он загружает последние версии антивирусного ядра **drweb32.dll**, а также обновляет вирусные базы.

Чтобы убедиться, что обновление прошло успешно:

1. В зависимости от версии операционной системы выполните команду **Tasks**, чтобы открыть папку C:\WINDOWS\Tasks или откройте Планировщик заданий Windows.
2. Проверьте наличие задания **Антивируса Dr.Web *Light*** в открывшейся папке (для правильно отработавшего задания код возврата в столбце **Последний результат** должен быть `0x0`).
3. Затем откройте файл журнала событий модуля обновления **%AllUsersProfile%\Application Data\Doctor Web\Logs\drwebupw.log** (если используется Microsoft ISA Server) или **%ProgramData%\Doctor Web\Logs\drwebupw.log** (если используется Microsoft Forefront TMG) и убедитесь, что в нем не зафиксировано ошибок.

Проверка детектирования вирусов

Для проверки конфигурации и способности **Антивируса Dr.Web *Light*** обнаруживать вирусы рекомендуется использовать тестовый скрипт EICAR (European Institute for Computer Antivirus Research). Текстовый файл, содержащий только тестовый скрипт EICAR, не является вирусом, не способен к саморепликации и не представляет опасности, однако определяется антивирусными программами как вирус. Вы можете загрузить тестовый файл с веб-сайта EICAR по адресу http://www.eicar.org/85-0-Download.html или создать его самостоятельно.

Чтобы создать тестовый файл EICAR:

- Откройте Блокнот и скопируйте в него следующую строку:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Для проверки детектирования вирусов **Антивирусом Dr.Web *Light*** по протоколу HTTP загрузите тестовый файл EICAR по данному протоколу (например, со страницы http://www.eicar.org/85-0-Download.html).

Передача файла должна быть заблокирована. В окне браузера должно появиться следующее сообщение:

Forbidden

URL is blocked by anti-virus

Reason: Infected by virus

В журнале событий приложения вы найдете событие типа Warning со следующим описанием (если в настройках сканирования выбрано действие **Перемещать в карантин**):

Infection detected. Dr. Web for ISA Server has detected that File is infected with a virus and it is incurable. The File is now moved to quarantine

В **Веб-консоли Администратора** должны появиться соответствующие уведомления о событиях в разделе **События** (см. Рисунок 12).

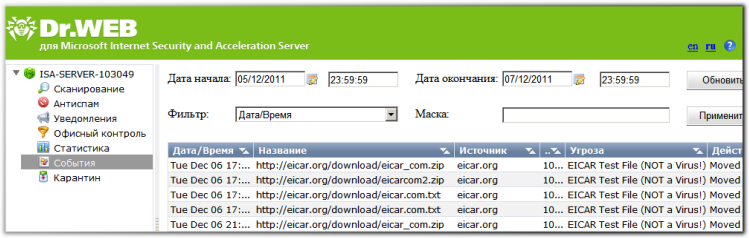

Рисунок 12. Уведомления о загрузке файлов EICAR в разделе События.

Если включено перемещение вредоносных объектов в **Карантин**, то в разделе **Карантин** должны появиться соответствующие записи о добавленных объектах (см. Рисунок 13).

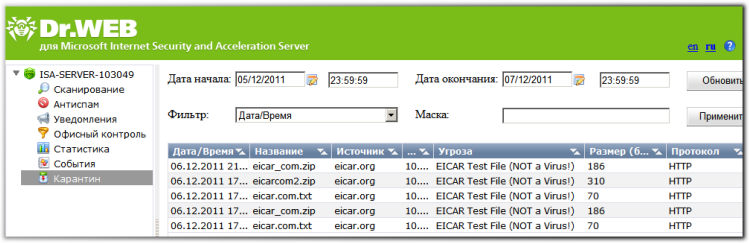

Рисунок 13. Список загруженных файлов EICAR в разделе Карантин.

Ни в коем случае не используйте настоящие вирусы для проверки работоспособности антивирусных программ!

Приложения

Приложение А. Параметры командной строки для модуля обновления

Ниже приведен список параметров командной строки, которые могут быть добавлены в поле **Выполнить** в настройках задания на обновление (**Dr.Web update for ISA plug-in**), чтобы настроить работу модуля обновления.

Параметр	Описание
/DBG	Вести подробный отчет.
/DIR: *<каталог>*	Переназначение папки, в которую загружаются обновляемые файлы; по умолчанию это папка, из которой модуль обновления был запущен.
/INI: *<путь>*	Использовать альтернативный конфигурационный файл с указанным именем или по указанному пути.
/NI	Не использовать параметры, записанные в конфигурационном файле **drweb32.ini**.
/GO	Пакетный режим работы, без диалоговых остановок.
/LNG: *<имя файла>*	Имя файла языковых ресурсов; если не указано, используется английский язык.
/PASS: *<пароль>*	Пароль пользователя сервера обновлений.
/USER: *<имя>*	Имя пользователя сервера обновлений.
/PPASS: *<пароль>*	Пароль пользователя прокси-сервера.
/PUSER: *<имя>*	Имя пользователя прокси-сервера.
/PURL: *<адрес>*	Адрес прокси-сервера.

Параметр	Описание
/URL: *<URL сервера обновлений>*	Допускаются только UNC-пути.
/QU	Принудительно закрывать модуль обновления после окончания сеанса обновления независимо от того, успешно оно прошло или нет. Успешность обновления можно проверить по коду возврата программы **drwebupw.exe**, например, из BAT-файла по значению переменной **errorlevel**: • нулевое значение указывает на успех; • другие значения указывают на неудачу.
/REG	Запуск модуля обновления в режиме регистрации и получения регистрационного ключа.
/UPD	Обычное обновление; применяется в паре с ключом /REG, чтобы запустить обновление в режиме регистрации.
/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.
/SO	Включить звуковое сопровождение (только при возникновении ошибок).
/ST	Запускать модуль обновления в невидимом режиме (*stealth mode*).
/UA	Загружать все файлы, заявленные в списке обновления, независимо от используемой системы и установленных компонентов. Режим предназначен для получения полной локальной копии серверной области обновления **Dr.Web**; этот режим нельзя использовать для обновления антивируса, установленного на компьютере.

Параметр	Описание
/UVB	Обновлять только вирусные базы и антивирусное ядро **drweb32.dll** (отменяет действие ключа /UA, если он задан).
/UPM: *<режим>*	Режим использования прокси-сервера, может принимать следующие значения: • direct – не использовать прокси-сервер; • ieproxy – использовать системные настройки; • userproxy – использовать настройки, задаваемые пользователем (ключи /PURL, /PUSER и /PPASS).
/URM: *<режим>*	Режим перезагрузки после обновления; может принимать следующие значения: • prompt – по окончании сеанса обновления, в случае необходимости перезагрузки, спросить пользователя; • noprompt – в случае необходимости, перезагружаться, не спрашивая пользователя; • force – перезагружать принудительно всегда (независимо от того, требуется перезагрузка или нет); • disable – запретить перезагрузку.

Приложение Б. Платформа CMS

CMS (Central Management System) представляет собой кроссплатформенную распределенную систему управления приложениями (здесь и далее под приложением понимается любой модуль-подписчик главного управляющего сервиса). Центром системы является управляющий сервис **Dr.Web CMS**. Данный сервис реализует основные функции системы по контролю функционирования приложений, а также управление приложениями, настройками приложений и регистрацией событий.

Взаимодействие между приложениями происходит посредством протокола TCP. Взаимодействие приложений с управляющим сервисом может происходить двумя способами:

- контролируемое приложение взаимодействует с управляющим сервисом посредством протокола MB (Management Base);
- управляющие (администраторские) приложения взаимодействуют с управляющим сервисом посредством протокола MS (Management System).

Сервис **Dr.Web CMS** использует для хранения данных о приложениях встроенную древовидную базу данных.

База данных

База данных управляющего сервиса **Dr.Web CMS** представляет собой дерево, состоящее из групп и переменных. Переменные могут быть разных типов (данных) и иметь разные атрибуты.

Типы данных переменных, поддерживаемые управляющим сервисом **Dr.Web CMS**:

Тип данных	Комментарий
Int32	32-разрядное целое со знаком
UInt32	32-разрядное целое без знака

Тип данных	Комментарий
Int64	64-разрядное целое со знаком
UInt64	64-разрядное целое без знака
Float	32-разрядное вещественное число
Double	64-разрядное вещественное число
String	Строка неограниченной длины
Boolean	Логическое значение (true или false)
Time	Дата и время
Binary	Бинарные данные неограниченной длины
Password	Тип данных для хранения паролей

Атрибуты переменных могут быть следующими:

Атрибут	Комментарий
Default	Обычная переменная
Shared	Распределенная переменная
Statistics	Статистическая переменная
System	Системная переменная
Hidden	Скрытая системная переменная
Readonly	Переменная, которую нельзя изменять.

Контроль приложений

Для контроля приложения с помощью CMS происходит регистрация его имени и версии в базе управляющего сервиса. Сервис **Dr.Web CMS** присваивает приложению уникальное имя, состоящее из имени приложения и версии. После этого сервис создает в базе данных группу с именем зарегистрированного приложения. По умолчанию в этой группе создаются служебные подгруппы с именами **Application Status** и **Settings**. Во время работы приложения управляющий сервис ведет сбор статистики

по протоколам взаимодействия. Статистика ведется в группе **Application Statistics/Connections**, в ее подгруппах **MB** и **MS** ведется статистика взаимодействия по протоколам. Используя данные статистики, можно оценить степень нагрузки на эти сервисы и приложения.

Группа Application Status

Данная группа содержит информацию о зарегистрированном приложении в виде значений переменных различных типов:

Переменная (в скобках указан тип переменной)	Комментарий
Active (Boolean)	Обозначает, запущено ли сейчас приложение. Значение **true** означает, что приложение запущено.
Crash (Boolean)	Обозначает, корректно ли было остановлено приложение. Значение **true** означает, что завершилось некорректно.
HomeDir (String)	Каталог приложения в файловой системе
InstanceName (String)	Имя, под которое приложение заявило при регистрации
LogicCrash (Boolean)	Состояние логики приложения. Значение **true** означает, что приложение работает некорректно.
ModuleName (String)	Имя исполняемого файла приложения. В случае если приложением-подписчиком является библиотека *.dll, то переменная указывает на имя инстанцировавшего ее процесса.
ModulePath (String)	Путь к исполняемому файлу приложения в файловой системе
PID (UInt32)	Номер процесса приложения в операционной системе
StartedOn (Time)	Время последнего запуска приложения
StoppedOn (Time)	Время последней остановки приложения

Переменная (в скобках указан тип переменной)	Комментарий
Version (String)	Версия приложения
VersionBuild (UInt32)	Номер сборки приложения
VersionMajor (UInt32)	Основной номер версии приложения
VersionMinor (UInt32)	Второй номер версии приложения
VersionRevision (UInt32)	Номер ревизии приложения
WorkDir (String)	Рабочий каталог приложения в файловой системе

Группа Settings

Данная группа содержит базовые настройки зарегистрированного приложения.

Статистика

Система позволят вести интервальную статистику приложений. Со стороны приложений есть возможность создания статистических переменных, которые могут вести учет происходящих в приложении событий и создавать совокупность статистических данных через определенные интервалы времени в зависимости от настроек статистической переменной.

В базе данных управляющего сервиса **Dr.Web CMS** такие переменные имеют атрибут **Statistics**. Переменные с таким атрибутом являются временными, они не сохраняются в постоянную базу данных и существуют только пока работает управляющий сервис. После перезапуска сервиса такие переменные теряются.

Администрирование

Управление системой производится по протоколу администрирования. Протокол позволяет произвольно изменять значения переменных, выполнять сброс накопленной статистики статистических переменных, отслеживать трассировку в реальном времени с применением фильтров и выгружать накопленные сообщения за прошлые периоды с фильтрацией.

Изменение значений переменных

Изменение значений переменных происходит синхронно. Все зарегистрированные приложения получают уведомления об изменении значений переменных и могут разрешить или запретить их изменение. При изменении переменной использующие ее приложения гарантированно получают ее актуальное значение.

Сброс статистики

Протокол администрирования позволяет сбрасывать накопленную по настройке переменной статистику. Это приводит к тому, что накопление статистики по данной настройке начинает происходить с нуля.

Ограничения при работе с переменными

При работе с переменными вводятся следующие ограничения:

- переменные с атрибутом **Hidden** существуют в базе, но недоступны для просмотра и редактирования. Они создаются самим управляющим сервисом для служебного использования;
- переменные с атрибутом **System** создаются управляющим сервисом для отображения служебной информации, предназначенной для администратора. Эти переменные не могут быть изменены или удалены;
- переменные с атрибутом **Statistics** создаются приложением. Эти переменные не могут быть изменены;

- переменные с атрибутом **Readonly** создаются приложением для информирования администратора, они не могут быть изменены;
- переменные с атрибутом **Default** являются обычными переменными, к ним применимы любые действия;
- переменные с атрибутом **Shared** являются распределенными переменными. Значения таких переменных изменяются синхронно по всей распределенной системе;
- переменные, которые не могут быть изменены, также не могут быть и удалены. Однако группы с такими переменными доступны для удаления вместе с этими переменными, если приложение, связанное с этой группой, не запущено.

Безопасность

Для доступа к системе требуется ввести имя пользователя и пароль. По умолчанию в системе существует пользователь **root** с паролем **drweb**, который после установки системы настоятельно рекомендуется сменить. Кроме того, вы можете добавить новых пользователей.

Пользователи и их пароли хранятся в группе управляющего сервиса, в подгруппе **Security** -> **Users**, т.е. по пути /CMS_1.0/Security/Users. Именем пользователя является имя группы. Пароль хранится в переменной **Password**.

Приложение В. Служба Dr.Web SSM

Служба **Dr.Web SSM** (**Dr.Web Start/Stop Manager**) контролирует работу приложений, работающих на платформе CMS, выполняя следующие функции:

- поддержание работоспособности сервиса **Dr.Web CMS** в автоматическом режиме;
- автоматический запуск зарегистрированных (имеющих группу переменных **SSM** в **Административной консоли CMS**) службой приложений в случае сбоев в их работе;
- форсированный запуск приложений даже в случае их корректной остановки;
- запуск приложений с помощью Windows Service Manager;
- запуск сервисов в виде приложений, реализованных с использованием CService из CommonComponents;
- запуск сервисов с помощью назначенных скриптов;
- остановка и запуск приложений в ручном режиме по команде пользователя.

Параметры контроля приложения службой **Dr.Web SSM** определяются группой переменных **SSM** в **Административной консоли CMS**. Группа **SSM** может содержать следующие переменные:

Переменная (в скобках указан тип переменной)	Комментарий
Enabled (Boolean)	Обозначает, запущено ли включение/выключение SSM-контроля.
Run (Boolean)	Позволяет запустить/остановить приложение
KeepAlive (Int32)	Обозначает тип поддержания активности приложения: • 0 – приложение отключено; • 1 – приложение включено;

Переменная (в скобках указан тип переменной)	Комментарий
	• 2 – форсированное, т.е. приложение будет включено даже в случае его корректной остановки.
StartType (Int32)	Обозначает способ запуска приложения: • 0 – как сервис Windows; • 1 – как приложение CService; • 2 – запуск с помощью скрипта.
StartScript (String)	Содержит скрипт для запуска приложения
StopScript (String)	Содержит скрипт для остановки приложения
Restart (Boolean)	Выполняет перезапуск приложения
Timeout (UInt32)	Обозначает время ожидания реакции приложения (в секундах). По умолчанию установлено значение 10 сек.
ServiceName (String)	Обозначает имя сервиса в Windows Service Manager. По умолчанию используется значение переменной "/Application Status/ InstanceName".

В разделе настроек самой службы **Dr.Web SSM** могут содержаться следующие переменные:

- **KeepAlivePeriod** (UInt32) – время проверки сервиса (в секундах). По умолчанию установлено значение 60 секунд.
- **RestartCMSPause** (UInt32) – время задержки перед перезапуском CMS (в секундах). По умолчанию установлено значение 5 секунд.

Приложение Г. Удаление Антивируса Dr.Web Light вручную

При возникновении сбоев в работе межсетевого экрана вы можете удалить **Антивирус Dr.Web *Light*** вручную. Для этого выполните следующие действия:

1. Остановите сервис межсетевого экрана Microsoft ISA Server/ Microsoft Forefront TMG.
2. Запустите командную консоль (cmd) от имени администратора.
3. Удалите регистрацию веб-фильтра с помощью команды:
   - `regsvr32 /u /s "C:\Program Files\Microsoft Forefront Threat Management Gateway\DrWeb\DrWebHttpMonitor.dll"` (в случае использования межсетевого экрана Microsoft Forefront TMG);
   - `regsvr32 /u /s "C:\Program Files\Microsoft ISA Server\DrWeb\DrWebHttpMonitor.dll"` (в случае использования межсетевого экрана Microsoft ISA Server).
3. Остановите службы приложения в указанном порядке:

   ```
   net stop "Dr.Web SSM"
   net stop "Dr.Web for MSP Components Host"
   net stop "Dr.Web for MSP Requests Queue"
   net stop "Dr.Web CMS Web Console"
   net stop "Dr.Web CMS"
   ```

4. Запустите стандартную утилиту Windows Installer Cleanup Utility (msicuu.exe) и с ее помощью удалите приложение из системы.
5. Удалите службы приложения:

   ```
   sc delete "Dr.Web SSM"
   ```

```
sc delete "Dr.Web for MSP Components Host"
sc delete "Dr.Web for MSP Requests Queue"
sc delete "Dr.Web CMS Web Console"
sc delete "Dr.Web CMS"
```

6. Удалите следующие каталоги:
   - в случае использования Microsoft ISA Server

     ```
     rd /S /Q "C:\Program Files\DrWeb for ISA Server"
     rd /S /Q "C:\Documents and Settings\All Users\Application Data\Doctor Web"
     rd /S /Q "C:\Program Files\DrWeb for ISA Server\DrWeb"
     ```

   - в случае использования Microsoft Forefront TMG

     ```
     rd /S /Q "C:\Program Files\DrWeb for ISA Server"
     rd /S /Q "C:\Program Files (x86)\DrWeb for ISA Server"
     rd /S /Q "C:\ProgramData\Doctor Web"
     rd /S /Q "C:\Program Files\Microsoft Forefront Threat Management Gateway\DrWeb"
     ```

Приложение Д. Работа в режиме централизованной защиты

Антивирус Dr.Web *Light* может функционировать в сети, контролируемой **Центром Управления Dr.Web**. Организация централизованной антивирусной защиты позволяет автоматизировать и упростить настройку и управление информационной безопасностью компьютеров, объединенных в единую логическую структуру (например, компьютеры одной компании, расположенные как внутри локальной сети, так и вне ее). Защищаемые компьютеры объединяются в единую *антивирусную сеть*, безопасность которой контролируется и управляется администраторами с центрального сервера (**Центра Управления Dr.Web**). Подключение к системам централизованной защиты позволяет получить гарантированно высокий уровень защиты компьютера при минимальных усилиях со стороны конечных пользователей.

Взаимодействие компонентов антивирусной сети

Решения компании **«Доктор Веб»** по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (см. Рисунок 14).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз безопасности и спама *локальными антивирусными компонентами* (клиентами; в данном случае – **Антивирусом Dr.Web *Light***), которые обеспечивают антивирусную защиту и упрощают соединение с сервером централизованной защиты.

Обновление и конфигурация локальных компонентов производится через *центральный сервер*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты. Объем трафика между защищенными компьютерами и антивирусным сервером может быть весьма значительным, поэтому предусматривается

возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.

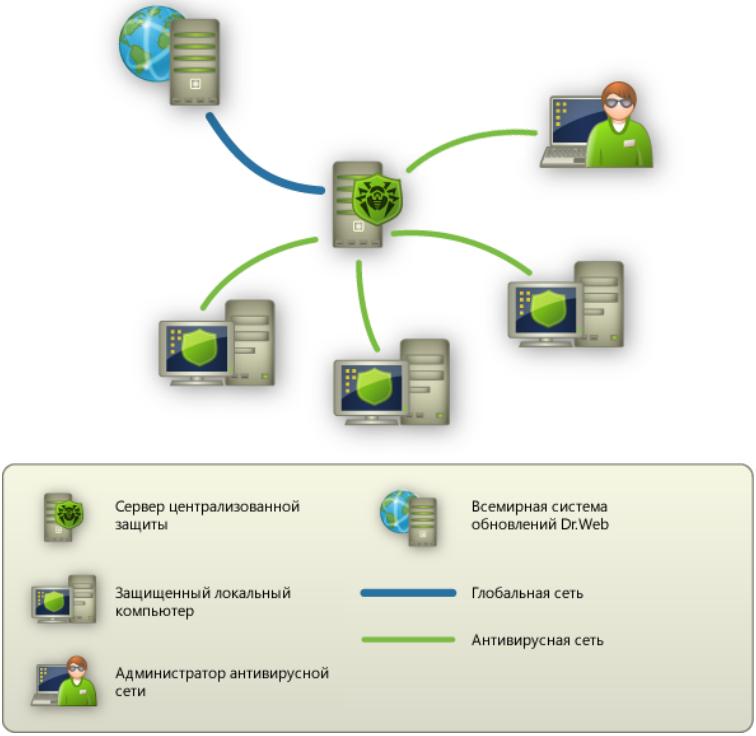

Рисунок 14. Логическая структура антивирусной сети.

Все необходимые обновления загружаются на сервер централизованной защиты с сервера **Всемирной системы обновлений Dr.Web**.

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется антивирусным сервером по указанию *администраторов антивирусной сети*. Администраторы управляют конфигурацией центрального сервера и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной станции к сети), а также при необходимости задают настройки работы конкретных локальных антивирусных компонентов.

Работа Антивируса Dr.Web *Light* в режиме централизованной защиты

Для работы **Антивируса Dr.Web *Light*** в режиме централизованной защиты необходимо, чтобы в операционной системе был установлен и корректно работал **Dr.Web Agent** версии 6.

Антивирус Dr.Web *Light* версии 6.00.1 не совместим с **Dr.Web Agent** версии 5.

Для **Антивируса Dr.Web *Light*** реализованы следующие возможности работы в режиме централизованной защиты:

- регистрация запуска межсетевого экрана Microsoft ISA Server и Microsoft Forefront TMG с установленным **Антивирусом Dr.Web *Light***. События запуска будут отображаться в таблице **Запуск/Завершение** **Центра Управления Dr.Web**. Время остановки межсетевого экрана Microsoft ISA Server и Microsoft Forefront TMG с установленным приложением не регистрируется;
- отправка статистики работы **Антивируса Dr.Web *Light***. Статистика работы отображается в таблицах **Статистика** и **Суммарная статистика** **Центра Управления Dr.Web**;

- отправка оповещений об обнаружении вирусов, а также информации об угрозах и предпринятых действиях. Эти события отображаются в таблице **Инфекции** **Центра Управления Dr.Web**;
- обновление антивирусных баз и антивирусного ядра из репозитория **Центра Управления Dr.Web**. Это позволяет отключить стандартный модуль обновления **Dr.Web Updater**, запускаемый по расписанию. В этом случае обновление компонентов будет выполняться согласно расписанию **Центра Управления Dr.Web** и из его репозитория;
- использование лицензионного ключевого файла **Антивируса Dr.Web *Light***, зарегистрированного для данной станции в антивирусной сети. Если на этапе установки был выбран режим лицензирования **Enterprise**, то при запуске Microsoft ISA Server или Microsoft Forefront TMG с установленным **Антивирусом Dr.Web *Light*** будет предпринята попытка использовать лицензионный ключ для данной станции в антивирусной сети. Если ключ не действителен, то антивирусная проверка производиться не будет.

Приложение Е. Техническая поддержка

Страница службы технической поддержки **«Доктор Веб»** находится по адресу http://support.drweb.com/.

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу http://download.drweb.com/;
- прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com/;
- попытаться найти ответ в базе знаний **Dr.Web** по адресу http://wiki.drweb.com/;
- посетить форум **Dr.Web** по адресу http://forum.drweb.com/.

Если после этого вам не удалось решить проблему, то вы можете заполнить веб-форму вопроса в соответствующей секции раздела http://support.drweb.com/.

Найти ближайшее к вам представительство **«Доктор Веб»** и всю контактную информацию, необходимую пользователю, вы можете по адресу http://company.drweb.com/contacts/moscow.

Предметный Указатель

Предметный Указатель

Предметный Указатель

Предметный Указатель