Dr.WEB

для Microsoft ISA Server и Forefront TMG

Руководство администратора

Dr.Web для Microsoft ISA Server и Forefront TMG
Версия 11.0
Руководство администратора
31.01.2018

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: http://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

1. Условные обозначения и сокращения 6

2. Техническая поддержка 7

3. Введение 8

3.1. Назначение Dr.Web 8

3.2. Проверяемые объекты 9

4. Лицензирование 10

4.1. Лицензионный ключевой файл 10

4.2. Получение ключевого файла 10

4.3. Обновление лицензии 11

5. Компоненты Dr.Web 12

5.1. Фильтры Dr.Web 12

5.1.1. Фильтры приложений 12

5.1.2. Веб-фильтр 17

5.2. Службы Dr.Web 20

5.3. Карантин 20

5.4. Мониторинг вирусных событий 20

6. Установка и удаление 21

6.1. Системные требования 21

6.2. Совместимость 22

6.3. Установка Dr.Web 23

6.4. Удаление Dr.Web 24

7. Администативная консоль Dr.Web Administrator Web Console 25

7.1. Группы и профили 26

7.2. Создание и настройка профилей 27

7.2.1. Приоритет профиля 28

7.2.2. Сканирование 28

7.2.3. Антиспам 30

7.2.4. Офисный контроль 32

7.2.5. Фильтрация 34

7.3. Управление группами клиентов 40

7.3.1. Создание новой группы 40

7.3.2. Настройки и формирование групп 41

7.4. Уведомления 43

7.5. Просмотр статистики 44
7.6. Просмотр списка инцидентов 46
7.7. Работа с карантином 48
7.7.1. Просмотр карантина с Dr.Web Administrator Web Console 48
7.7.2. Менеджер карантина 49
8. Обновление вирусных баз 53
8.1. Информация о версии программы и вирусных базах 53
9. Веб-консоль Dr.Web CMS Web Console 55
9.1. Изменение пароля администратора 57
9.2. Добавление новых администраторов 57
9.3. Создание кластеров 58
9.4. Выбор типов поврежденных объектов 60
9.5. Фильтрация файлов в архиве по их расширениям 61
10. Регистрация событий 62
10.1. Журнал операционной системы 62
10.2. Текстовый журнал программы установки 63
10.3. Журнал событий Dr.Web 64
10.3.1. Типы регистрируемых событий 64
10.3.2. Степень детализации 65
10.3.3. Удаление базы данных cmstracedb 65
11. Диагностика 67
11.1. Проверка установки 67
11.2. Проверка модуля обновления 68
11.3. Проверка детектирования вирусов 68
11.4. Проверка детектирования спама 69
12. Приложения 70
12.1. Приложение А. Удаление Dr.Web вручную 70
12.2. Приложение Б. Платформа CMS 71
12.2.1. База данных 71
12.2.2. Статистика 72
12.2.3. Подключение к серверам 73
12.3. Приложение В. Настройка параметров обновления 74
Предметный указатель 77

1. Условные обозначения и сокращения

В руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание
Антивирусная сеть	Новый термин или акцент на термине в описаниях
<IP-address>	Поля для замены функциональных названий фактическими значениями
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса
CTRL	Обозначения клавиш клавиатуры
`C:\Windows\`	Наименования файлов и каталогов, фрагменты программного кода
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы

2. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.ru/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу http://support.drweb.ru/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу http://forum.drweb.com/.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела http://support.drweb.ru/;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу http://company.drweb.ru/contacts/offices/.

3. Введение

Благодарим вас за приобретение Dr.Web для Microsoft ISA Server и Forefront TMG (далее – Dr.Web).

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

3.1. Назначение Dr.Web

Dr.Web – это приложение, созданное для защиты корпоративной сети от вирусных угроз и спама. Оно надежно интегрируется в систему для поиска и удаления любых типов вредоносных программ в потоке данных, проходящем через **Microsoft Internet Security and Acceleration Server** (далее – Microsoft ISA Server) и **Microsoft Forefront Threat Management Gateway** (далее – Microsoft Forefront TMG) по протоколам HTTP, FTP, SMTP и POP3. Приложение проверяет входящий интернет-трафик на вирусы, программы дозвона, рекламные программы, потенциально опасные программы, программы взлома и программы-шутки.

Приложение встраивает собственные фильтры данных в службы Microsoft Firewall Service и Microsoft Forefront TMG Firewall соответственно, что обеспечивает доступ к ним ядру антивирусной системы Dr.Web. Dr.Web функционирует на платформе, которая имеет встроенный веб-сервер с аутентификацией клиента и веб-консоль для управления.

Сервисы Dr.Web, установленные на разных серверах, могут быть объединены администратором в кластер (см. раздел Создание кластеров).

Dr.Web может выполнять следующие функции:

- сканирование всех данных, поступающих через межсетевой экран Microsoft ISA Server или Microsoft Forefront TMG по протоколам FTP (включая FTP поверх HTTP), HTTP, SMTP и POP3;
- 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;
- фильтрация спама в сообщениях, поступающих по протоколу SMTP;
- добавление сопроводительного текста к почтовым сообщениям, которые содержат угрозы безопасности;
- ограничение доступа пользователей к интернет-ресурсам;
- сбор статистики;

- автоматическое обновление вирусных баз и компонентов программы;
- поддержка единых настроек приложения, задаваемых централизованно, на распределенной системе межсетевых экранов, в том числе, объединенных в кластер.

Dr.Web 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.

3.2. Проверяемые объекты

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

Объекты проверки трафика, поступающего по протоколам HTTP и FTP

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

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

Объекты проверки трафика, поступающего по протоколам SMTP и POP3

Dr.Web производит проверку входящих почтовых сообщений в реальном времени. Проверке подвергаются следующие элементы электронных писем:

- тело письма;
- вложения (включая файлы в архивах и упакованные файлы);
- вложенные OLE-объекты.

4. Лицензирование

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

4.1. Лицензионный ключевой файл

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

- срок действия лицензии;
- перечень компонентов, разрешенных к использованию (например, компонент Антиспам доступен только в версии «Антивирус + Антиспам»);
- 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 Dr.Web 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.

4.2. 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 Dr.Web, 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 Dr.Web.

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 https://download.drweb.ru/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.ru/.

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

4.3. 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 Dr.Web. 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 (**%PROGRAMFILES%\DrWeb CMS for MSP**) новым ключевым файлом.
2. Dr.Web 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.ru/.

5. Компоненты Dr.Web

Все антивирусные решения «Доктор Веб» содержат следующие основные компоненты, обеспечивающие защиту операционных систем и платформ:

- антивирусное ядро **drweb32.dll**;
- файлы вирусных баз (с расширением **.vdb**), в которых хранятся и регулярно обновляются вирусные записи, содержащие различную информацию о вирусах и иных вредоносных кодах.

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

В состав Dr.Web так же входит дополнительная веб-консоль Dr.Web CMS Web Console, которая предназначена для выявления и устранения ошибок. Она так же предоставляет возможность задавать расширенные настройки и менять конфигурацию Dr.Web. Подробное описание см. в разделе Веб-консоль Dr.Web CMS Web Console.

5.1. Фильтры Dr.Web

Dr.Web осуществляет перехват данных сетевых соединений для последующей антивирусной проверки с помощью специальных фильтров, встраиваемых в службу Microsoft Firewall Service (для Microsoft ISA Server) или Microsoft Forefront TMG Firewall (для Microsoft Forefront TMG).

Все фильтры реализованы в виде динамических библиотек, запускаемых при старте службы межсетевого экрана Microsoft Firewall Service или Microsoft Forefront TMG Firewall и остающихся в памяти до завершения работы этой службы. Фильтры получают доступ к потоку данных в службе межсетевого экрана. Если на запрос (request) клиента или ответ (response) сервера создается событие, для которого зарегистрирован фильтр, фильтр выполняет перехват и анализирует содержащиеся в потоке данные.

В состав Dr.Web входят три фильтра приложений (application filters) и один веб-фильтр (web filter).

5.1.1. Фильтры приложений

В состав Dr.Web входит три фильтра приложений:

- Dr.Web FTP Filter;
- Dr.Web SMTP Filter;
- Dr.Web POP3 Filter.

Фильтры приложений располагаются в следующих каталогах:

Фильтр	Путь к библиотеке фильтра
Dr.Web FTP Filter	При работе с **Microsoft ISA Server**: %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\FTPFilter.dll При работе с **Microsoft Forefront TMG**: %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\FTPFilter.dll
Dr.Web SMTP Filter	При работе с **Microsoft ISA Server**: %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\SMTPFilter.dll При работе с **Microsoft Forefront TMG**: %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\SMTPFilter.dll
Dr.Web POP3 Filter	При работе с **Microsoft ISA Server**: %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\POP3Filter.dll При работе с **Microsoft Forefront TMG**: %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\POP3Filter.dll

Перечисленные фильтры предназначены для выполнения операций над совокупностью пакетов протоколов. Они осуществляют анализ данных и блокируют их в случае обнаружения вирусных угроз. Все фильтры можно найти в отдельной ветви дерева консоли управления Microsoft ISA Server или Microsoft Forefront TMG (см. Рисунок 1а, Рисунок 1б):

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

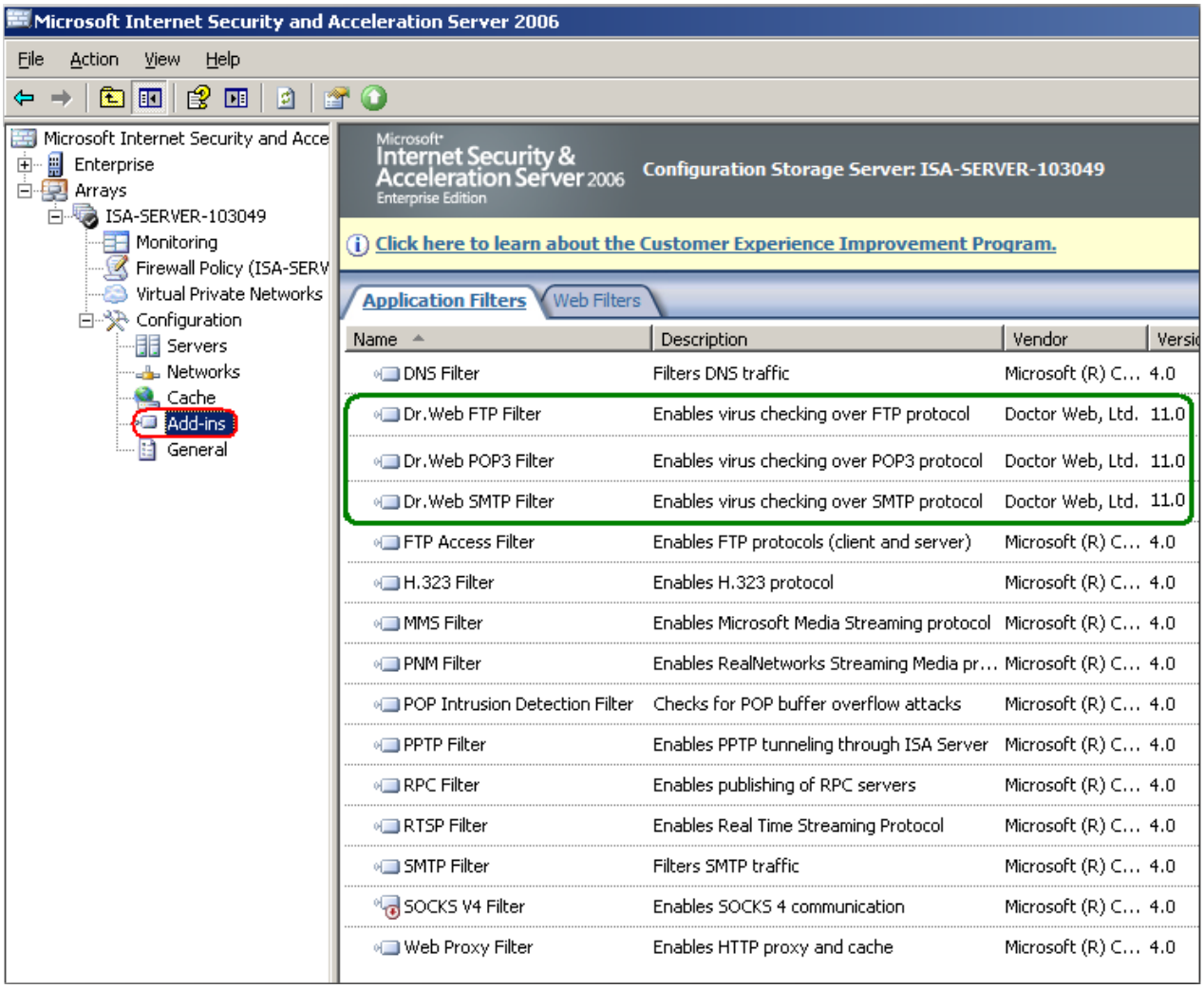

Рисунок 1а. Фильтры приложений Dr.Web в консоли Microsoft ISA Server

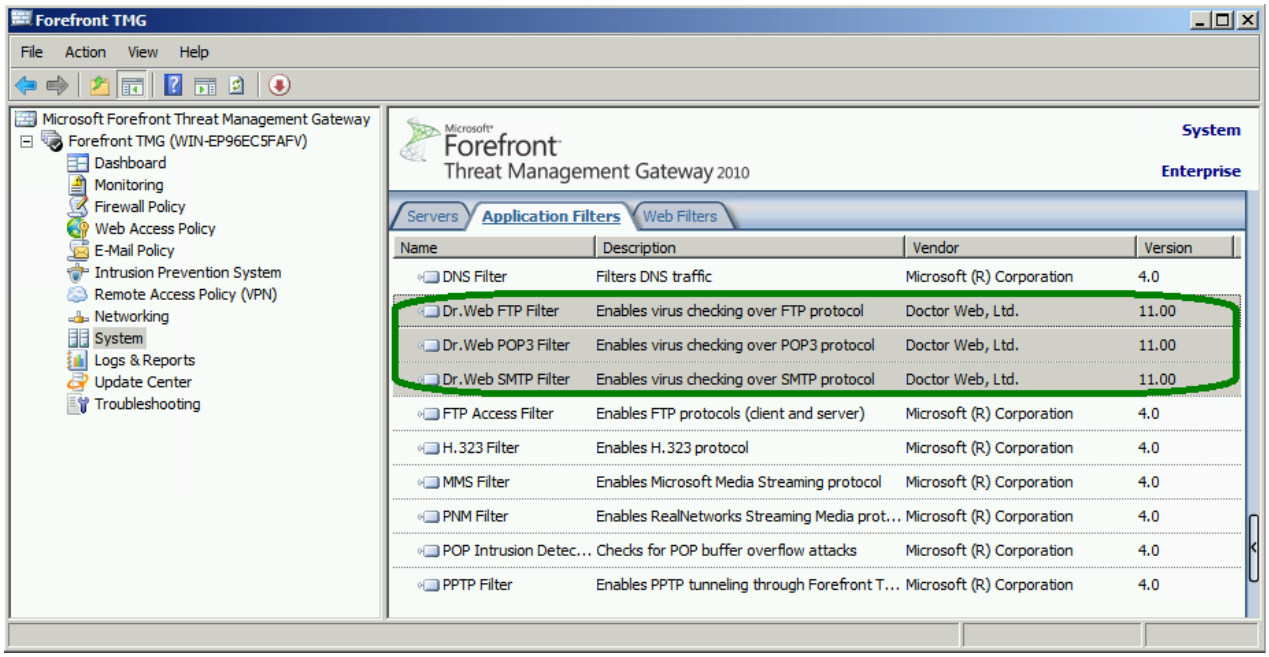

Рисунок 16. Фильтры приложений Dr.Web в консоли Microsoft Forefront TMG

Сразу после установки приложения и успешной регистрации **Dr.Web FTP Filter** подключается к событиям FTP-протокола и отображается на вкладке свойств FTP-протокола в консоли Microsoft ISA Server или Microsoft Forefront TMG (см. Рисунок 2).

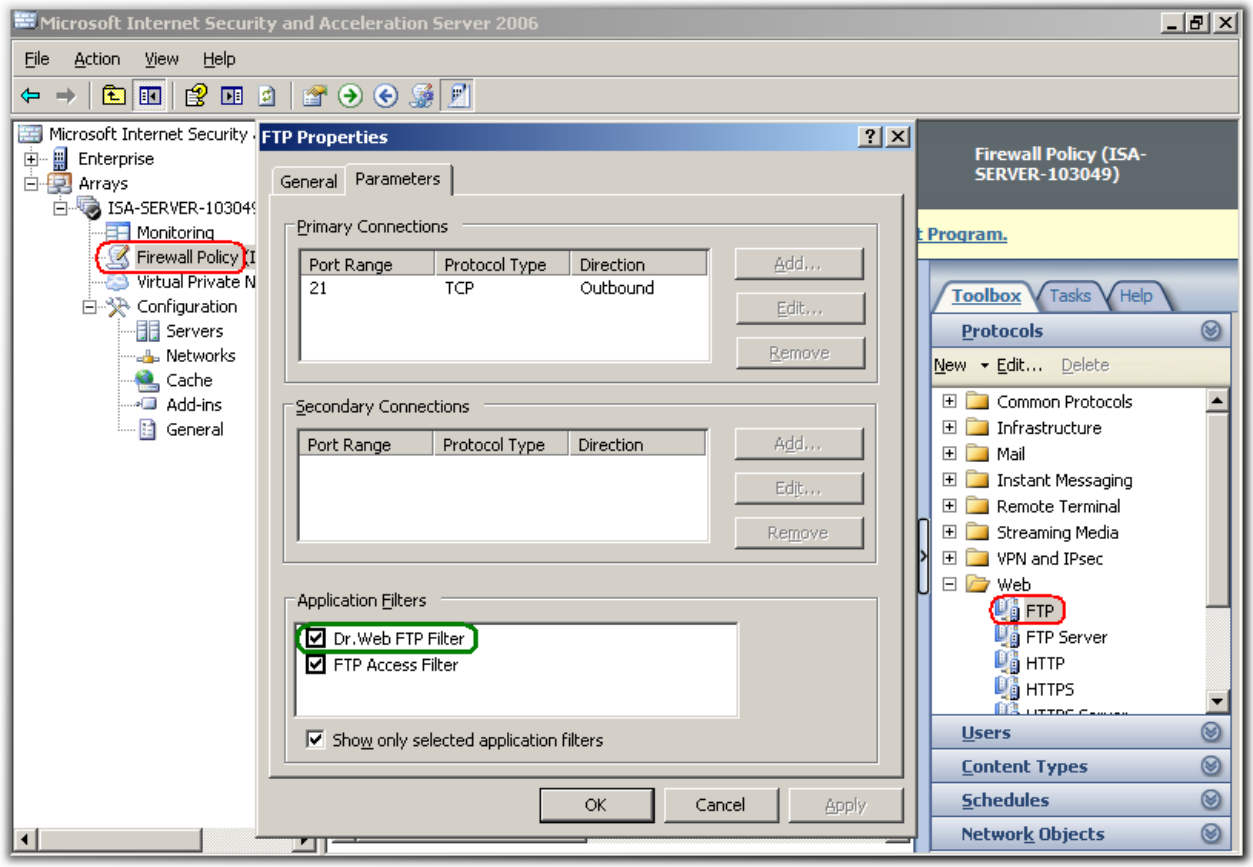

Рисунок 2. Фильтр Dr.Web FTP Filter на вкладке свойств протокола FTP

Microsoft ISA Server и Microsoft Forefront TMG поставляются со встроенным фильтром доступа к FTP – FTP Access Filter. Если фильтр доступа к FTP отключен, то межсетевой экран Microsoft ISA Server или Microsoft Forefront TMG не отслеживает взаимодействие приложений уровня протокола FTP. Таким образом, для того чтобы Dr.Web FTP Filter функционировал, необходимо, чтобы FTP Access Filter был включен и активирован на вкладке свойств протокола FTP (см. Рисунок 2).

5.1.1.1. Dr.Web FTP Filter

Во время установки Dr.Web FTP Filter регистрируется как обработчик событий при работе с FTP-протоколом. Подготовка к антивирусной проверке начинается, как только установлена связь клиента с FTP-сервером. В этот момент Microsoft ISA Server или Microsoft Forefront TMG начинает обрабатывать данные, передаваемые от клиента серверу и в обратном направлении:

1. Анализируя запросы клиента, Dr.Web FTP Filter определяет момент поступления запроса загрузки файла клиентом.
2. После получения запроса на загрузку файла, Dr.Web FTP Filter проверяет IP-адрес сервера на предмет соответствия черным и белым спискам IP-адресов.
3. Из запроса на загрузку файла Dr.Web FTP Filter выбирает имя запрашиваемого файла и запрашивает данные о размере файла. клиентом. В случае, когда размер запрошенного

файла не превышает некоторого предела (по умолчанию 0,5 Мбайт) для сохранения полученных данных используется буфер в памяти. В случае, когда предел превышен, для сохранения данных используется файл.

4. Передача файла клиенту происходит до определенного уровня (по умолчанию 80%). После этого передача приостанавливается, Dr.Web FTP Filter накапливает оставшиеся данные и проверяет файл. Если файл не содержит угроз, оставшиеся данные передаются клиенту. Если файл инфицирован, передача останавливается. Клиент не получит файл целиком, но сигнатура вируса может попасть на машину клиента.

Если соединение между FTP-клиентом и сервером было разорвано из-за обнаружения угрозы при загрузке файла, то для продолжения работы с FTP-протоколом необходимо выполнить повторное подключение к серверу.

5.1.1.2. Dr.Web SMTP Filter и Dr.Web POP3 Filter

По протоколам POP3 и SMTP Dr.Web производит проверку только незашифрованного потока данных.

Проверка выполняется в два этапа:

1. На первом этапе полученное сообщение передается модулю Антиспама **Vade Retro** для проверки текста сообщения. По результатам формируется заключение, на основе которого определяется степень вероятности того, что данное сообщение является спамом. Если письмо определено как спам, то к нему применяется действие, установленное администратором для данной категории спама в разделе **Антиспам** административной консоли Dr.Web Administrator Web Console.
2. На втором этапе сообщения, успешно прошедшие проверку на спам (или проигнорированные в соответствии с настройками приложения), передаются далее для проверки на наличие вредоносного кода. По результатам сканирования объектам (телу письма или вложениям) присваиваются определенные статусы (**Зараженные** или **Подозрительные**). На основе результатов сканирования выполняются дальнейшие действия над этими объектами (в соответствии с настройками, заданными администратором в разделе **Сканирование** административной консоли Dr.Web Administrator Web Console).
   Если в настройках включено использование эвристического анализатора, приложение может определять объекты, содержащие модифицированный или неизвестный вредоносный код. Таким объектам присваивается статус **Подозрительные**.
   К письмам с зараженными объектами прикрепляется текстовый файл с сообщением об обнаруженных угрозах и выполненных над этими объектами действиями.

5.1.2. Веб-фильтр

В состав Dr.Web входит веб-фильтр Dr.Web HTTP Web Filter. Он представляет собой

расширение (run-time extension) фильтра Web Proxy Filter, встроенного в Microsoft ISA Server или Microsoft Forefront TMG. Таким образом веб-фильтр Dr.Web реагирует на события встроенного фильтра Web Proxy Filter.

Dr.Web HTTP Web Filter располагается в библиотеке HTTPWebFilter.dll в каталогах:

%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG (для Microsoft ISA Server);

%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG (для Microsoft Forefront TMG).

Dr.Web HTTP Web Filter отображается в дереве консоли управления Microsoft ISA Server или Microsoft Forefront TMG (см. Рисунок 3а, Рисунок 3б):

- 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.

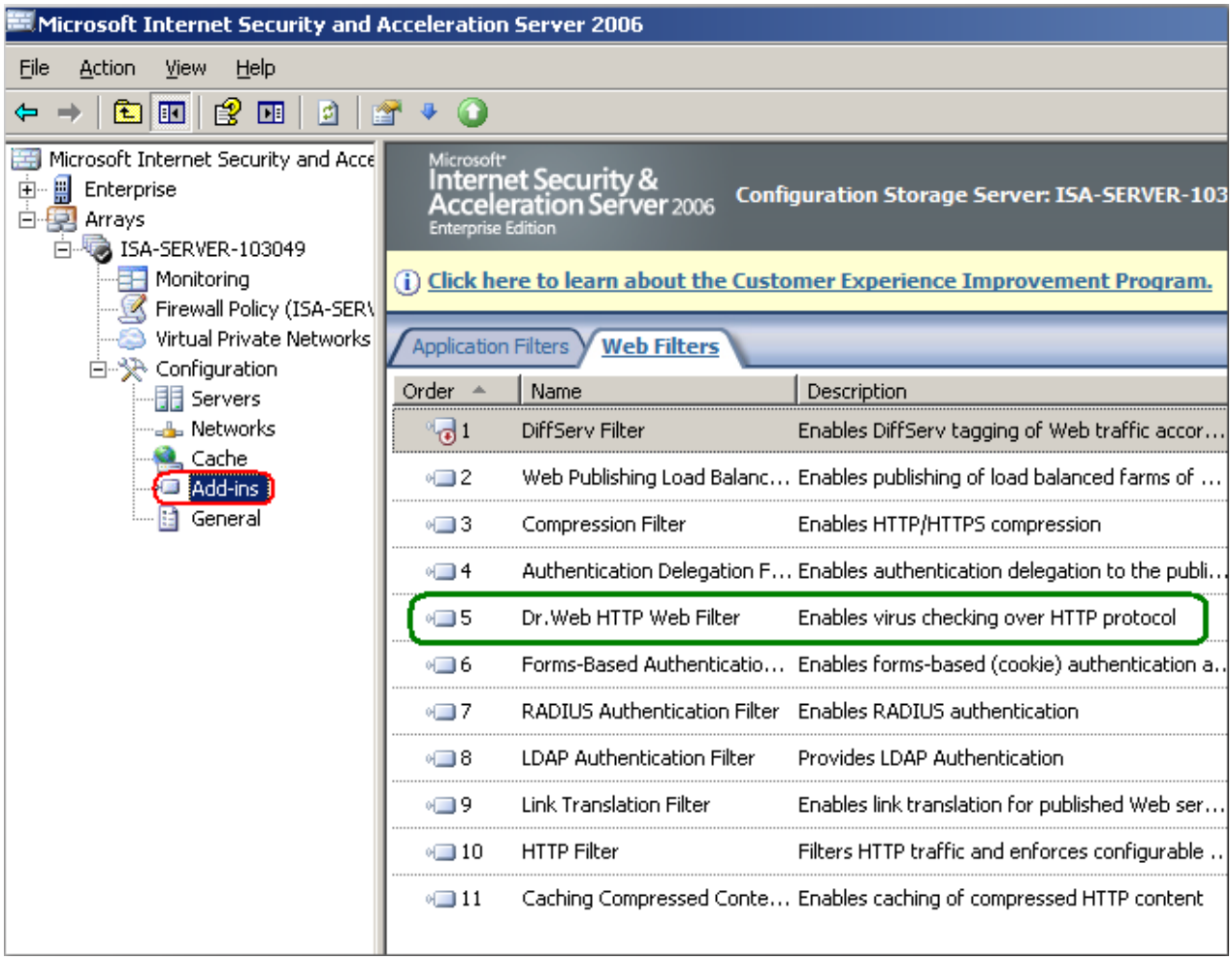

Рисунок 3а. Фильтр Dr.Web HTTP Web Filter в консоли Microsoft ISA Server

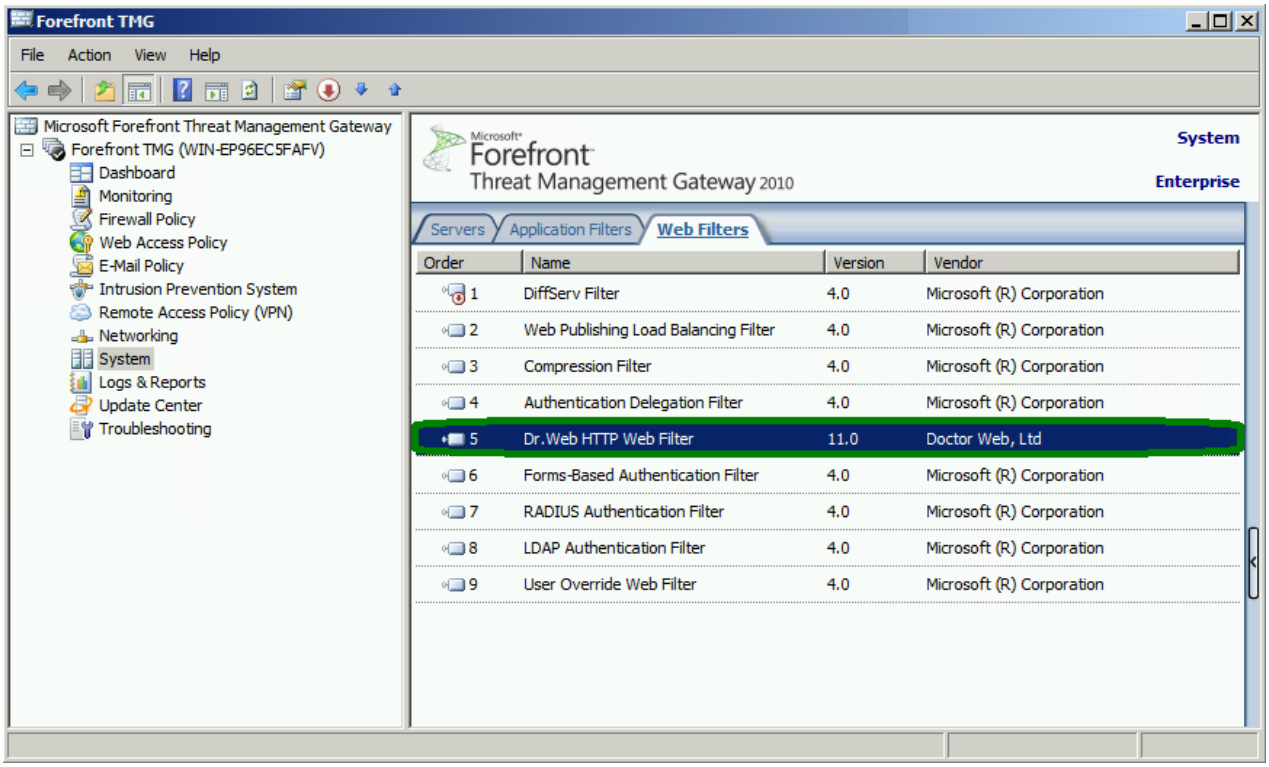

Рисунок 3б. Фильтр Dr.Web HTTP Web Filter в консоли Microsoft Forefront TMG

5.1.2.1. Dr.Web HTTP Web Filter

Подготовка к антивирусной проверке начинается с момента отправки сервером данных обратно клиенту, либо извлечения запрашиваемых данных из кэша (cache) Microsoft ISA Server или Microsoft Forefront TMG.

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, ему присваивается один из четырех статусов (два неопределенных и два определенных состояния ресурса соответственно):

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

Состояние ресурса хранится 30 минут с момента окончания сканирования. По истечении указанного времени ресурс переходит в состояние «не верифицирован». По прошествии 60 периодов верификации записи о ресурсе будут удалены из системы.

5.2. Службы Dr.Web

Работу Dr.Web обеспечивают семь основных служб (сервисов):

- **Dr.Web CMS** – поддерживает распределенную систему управления компонентами приложения, контролирует работу отдельных модулей. Сервис поддерживает базу данных настроек компонентов приложения.
- **Dr.Web CMS Web Console** – обеспечивает работу веб-консолей.
- **Dr.Web for MSP Component Host** и **Dr.Web for MSP Scanning Service** – обеспечивают взаимодействие компонентов плагина.
- **Dr.Web for MSP Requests Queue** – поддерживает асинхронную очередь запросов на выполнение заданий приложения, допускающих отложенное выполнение.
- **Dr.Web Scanning Engine** – содержит ядро антивирусной системы Dr.Web.
- **Dr.Web SSM** – контролирует запуск и остановку служб Dr.Web.

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.

5.3. Карантин

Для объектов можно установить действие **Перемещать в карантин**. Объекты указанного типа помещаются в служебную базу, выполняющую функции карантина, т.е. блокирующую возможность выполнения кода этих объектов любыми приложениями в системе. Получить информацию об объектах, находящихся в карантине, можно в разделе Работа с карантином.

5.4. Мониторинг вирусных событий

Чтобы получать информацию о событиях, отслеживаемых Dr.Web, вы можете настроить систему оповещения. Она включает следующие возможности:

- Журнал операционной системы. События плагина записываются в журнал регистрации операционной системы (Event Log).
- Инциденты. Предоставляет список объектов, обработанных Dr.Web, в которых обнаружены вирусы или спам, а также отфильтрованных писем.
- Статистика. Содержит информацию о количестве проверенных объектов за указанный промежуток времени.

6. Установка и удаление

Перед установкой или удалением Dr.Web 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 удаления компонентов приложения. Если по этой причине произошел сбой в процессе удаления, приводящий к неработоспособности межсетевого экрана, см. приложение Удаление Dr.Web вручную.

Dr.Web поставляется в виде установочного файла (`drweb-[version]-av-isa-windows-x86.exe` или `drweb-[version]-av-tmg-windows-x64.exe`, в зависимости от используемого межсетевого экрана), где `[version]` - номер текущей версии Dr.Web, либо 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 Dr.Web рекомендуется воспользоваться стандартной утилитой Windows **Установка и удаление программ** (в Windows Server 2003) или **Программы и компоненты** (в Windows Server 2008).

Установка нескольких антивирусных продуктов на один компьютер может привести к системным ошибкам и потере важных данных. Если на компьютере уже установлена версия Dr.Web, отличная от версии 11, или антивирус другого производителя, то его необходимо удалить.

6.1. Системные требования

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

Характеристика	Требование	
	при использовании Microsoft ISA Server	**при использовании Microsoft Forefront TMG**
RAM	1 Гбайт и больше	2 Гбайт и больше
Свободное пространство на диске	700 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	
ОС	Одна из следующих: • Microsoft® Windows Server® 2003 x86 с: ▫ MSXML 4.0 Service Pack 3 (Microsoft XML Core Services) ▫ Service Pack 1 (SP1) и выше • Microsoft® Windows Server® 2003 R2 x86 с: ▫ MSXML 4.0 Service Pack 3 (Microsoft XML Core Services)	Одна из следующих: • Microsoft® Windows Server® 2008 SP2 x64 • Microsoft® Windows Server® 2008 R2 x64
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 .NET Framework 3.5 SP1	

6.2. Совместимость

Перед установкой Dr.Web необходимо обратить внимание на следующую информацию о совместимости программы:

1. Dr.Web для Microsoft ISA Server и Forefront TMG версии 11 совместим только с Dr.Web для серверов Windows версии 11.
2. Dr.Web для Microsoft ISA Server и Forefront TMG версии 11 не совместим с Dr.Web ES Агентом и Dr.Web AV-Desk.
3. Dr.Web для Microsoft ISA Server и Forefront TMG 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

установлен другой антивирус, то его необходимо удалить, используя установочный файл или стандартные средства операционной системы.

6.3. Установка Dr.Web

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 Dr.Web:

1. Остановите службу межсетевого экрана Microsoft ISA Server или Microsoft Forefront TMG.
2. Убедитесь, что процесс установки будет запущен под встроенной учетной записью системного администратора.
3. Запустите установочный файл программы. Откроется окно с предложением выбрать язык установки. Вы можете выбрать русский или английский язык. Нажмите кнопку **OK**.
4. В окне с текстом Лицензионного соглашения необходимо прочитать и принять соглашение, выбрав пункт **Я принимаю условия лицензионного соглашения**. Нажмите кнопку **Далее**.
5. Если служба межсетевого экрана все еще запущена, вам будет предложено ее остановить.
6. Выберите вариант лицензирования.

   По умолчанию Мастер установки ищет лицензионный файл с расширением **.key** в каталоге запуска и в каталоге **%PROGRAMFILES%\DrWeb CMS for MSP**. Если Мастер установки найдет ключ, он выведет информацию о нем в окно выбора варианта лицензирования.

   Вы можете использовать локальный ключ, указав его расположение вручную. При выборе пункта **Активировать продукт позже** проверка трафика не будет происходить.

   Нажмите кнопку **Далее**.
7. На шаге **Система готова к установке программы** нажмите кнопку **Установить**, после чего начнется установка Dr.Web на ваш компьютер.
8. Последующие действия Мастера установки не требуют вмешательства пользователя. По завершении установки вам будет предложено перезагрузить компьютер.

Во время установки программы необходимо перезапустить Microsoft ISA Server или Microsoft Forefront TMG. Остановка связана с необходимостью избежать нарушения целостности установки на сервере, работающем под нагрузкой.

Так же может потребоваться перезагрузка оперативной системы, в том числе после обновления Dr.Web.

6.4. Удаление Dr.Web

Чтобы удалить Dr.Web:

1. Остановите сервис межсетевого экрана Microsoft ISA Server или Microsoft Forefront TMG.
2. Убедитесь, что процесс удаления будет запущен под встроенной учетной записью системного администратора.
3. Запустите стандартную утилиту Windows **Установка и удаление программ** (в Windows Server 2003) или **Программы и компоненты** (в Windows Server 2008).
4. Выберите в списке установленных программ Dr.Web и нажмите **Удалить**.
   Откроется окно Мастера установки.
5. Если служба межсетевого экрана все еще запущена, будет предложено ее остановить. Остановите службу и нажмите кнопку **Далее**.
6. При необходимости выберите пункт **Сохранить настройки**. Нажмите **Удалить**.
7. По завершении удаления вам будет предложено перезагрузить компьютер.

Во время удаления программы необходимо перезапустить Microsoft ISA Server/Microsoft Forefront TMG. Остановка связана с необходимостью избежать нарушения целостности установки на сервере, работающем под нагрузкой. По завершении удаления запустите сервис Microsoft Firewall Service/Microsoft Forefront TMG Firewall.

7. Администативная консоль Dr.Web Administrator Web Console

Работа Dr.Web может быть настроена с помощью административной консоли Dr.Web Administrator Web Console (см. Рисунок 4).

Запуск административной консоли Dr.Web Administrator Web Console

Для корректной работы административной консоли Dr.Web Administrator Web Console используйте следующие браузеры:

- Internet Explorer версии 11 или выше;
- Chrome версии 46 или выше;
- Microsoft Edge 20 или выше.

Кроме того, для корректной работы административной консоли Dr.Web Administrator Web Console 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 Enhanced Security Configuration** и нажмите кнопку **Далее**. Затем нажмите кнопку **Готово**.
- В ОС Windows Server 2008: запустите **Диспетчер сервера** и выберите пункт **Настроить конфигурацию усиленной безопасности Internet Explorer**, после чего выберите соответствующую опцию в разделе **Администраторы**.
- В ОС Windows Server 2012: запустите **Диспетчер серверов**, перейдите на вкладку **Локальный сервер** и выберите пункт **Конфигурация усиленной безопасности Internet Explorer**, после чего выберите соответствующую опцию в разделе **Администраторы**.

Для запуска административной консоли Dr.Web Administrator Web Console откройте в браузере следующую страницу:

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

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

Для доступа к странице Dr.Web Administrator Web Console необходимо ввести данные учетной записи администратора.

При первом запуске Dr.Web Administrator Web Console используйте данные учетной записи по умолчанию: имя пользователя **root** и пароль **drweb**. Далее настоятельно рекомендуется изменить пароль для данной учетной записи (подробнее в разделе Изменение пароля администратора).

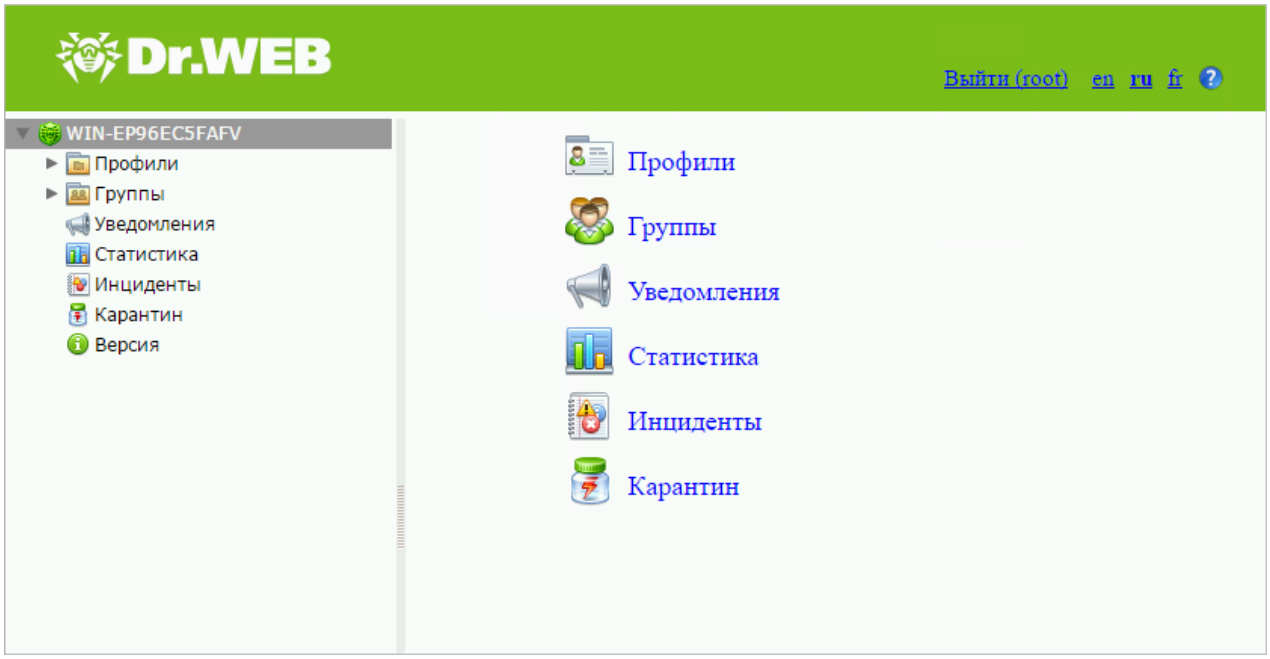

Рисунок 4. Административная консоль Dr.Web Administrator Web Console

Интерфейс

Административная консоль Dr.Web Administrator Web Console состоит из двух частей:

1. Дерево 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 административной консоли Dr.Web Administrator Web Console. Вы можете выбрать русский, английский или французский язык. Кроме того, справа от опции выбора языка находится значок вызова справки по этой консоли.

7.1. Группы и профили

Для упрощения организации антивирусной защиты пользователей внутренней сети, защищаемой межсетевым экраном Microsoft ISA Server и Microsoft Forefront TMG, в Dr.Web реализована возможность создания групп клиентов и присвоения им определенных профилей.

Профиль представляет собой набор настраиваемых параметров обработки интернет-трафика, от которых зависит то, как именно будет осуществляться защита локальной сети. Настройки профиля находятся в разделе дерева административной консоли **Профили**, который имеет следующие подразделы:

- Сканирование – позволяет настроить работу вашего основного компонента обнаружения вирусов;
- Антиспам – позволяет настроить работу компонента Антиспам (настройки в этом разделе доступны только при наличии версии «Антивирус + Антиспам», т.е. в том случае, если у вас есть соответствующий ключевой файл (см. Лицензионный ключевой файл);
- Офисный контроль – позволяет настроить ограничения доступа пользователей к интернет-ресурсам;
- Фильтрация – позволяет настроить фильтрацию интернет-трафика.

Более подробно о работе с профилями читайте в разделе Создание и настройка профилей.

Любой профиль можно назначить группе клиентов. Эти группы формируются в разделе дерева консоли **Группы** (см. Управление группами клиентов).

7.2. Создание и настройка профилей

В процессе установки Dr.Web автоматически создает стандартный профиль **Default**. Этот профиль нельзя удалить и переименовать. Он будет применяться ко всему трафику, пока вы не создадите другой профиль и не назначите его определенной группе клиентов.

Для управления существующими профилями и создания новых перейдите к области сведений раздела **Профили**, выбрав пункт **Профили** в дереве административной консоли Dr.Web Administrator Web Console (см. Рисунок 5).

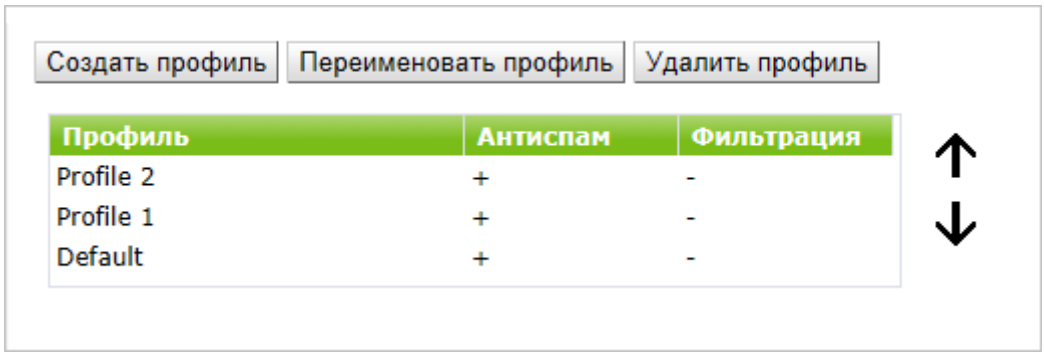

Рисунок 5. Настройка профиля

Для каждого профиля в списке содержится также информация о его настройках и приоритете.

Создание нового профиля

Чтобы создать новый профиль:

- нажмите кнопку **Создать профиль**, расположенную над списком существующих профилей;
- щелкните правой кнопкой на пункте **Профили** в дереве консоли и выберите **Создать профиль** в контекстном меню.

В окне **Создать профиль** укажите имя для нового профиля и нажмите **ОК**.

Имя профиля должно быть задано латинскими символами.

По умолчанию настройки созданного профиля будут такими же, как настройки стандартного (**Default**) профиля.

Переименование профиля

Чтобы изменить имя существующего профиля, выберите нужный профиль в списке, расположенном в области сведений раздела **Профили**, и нажмите кнопку **Переименовать профиль**.

Изменение настроек профиля

Чтобы изменить настройки профиля, выберите его имя в дереве административной консолиDr.Web Administrator Web Console и перейдите к нужному разделу: Сканирование, Антиспам или Офисный контроль.

Удаление профиля

Чтобы удалить профиль, выберите его в списке, расположенном в области сведений раздела **Профили**, и нажмите кнопку **Удалить профиль**.

7.2.1. Приоритет профиля

У каждого профиля есть определенный уровень приоритета, назначаемый администратором. В случае если клиент состоит в нескольких группах, которым назначены разные профили, при обработке трафика, получаемого или посылаемого этим клиентом, будет использован профиль с наивысшем уровнем приоритета.

Приоритет профиля изменяется в области сведений раздела **Профили** перемещением существующих профилей вверх или вниз по списку. Для перемещения существующих профилей используйте кнопки ↑ и ↓справа от списка. Чем выше профиль расположен в списке, тем выше уровень его приоритета.

Стандартный профиль всегда обладает самым низким уровнем приоритета, он располагается на нижней строки в списке профилей.

7.2.2. 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 административной консоли. Откроется область сведений для настройки сканирования (см. Рисунок 6).

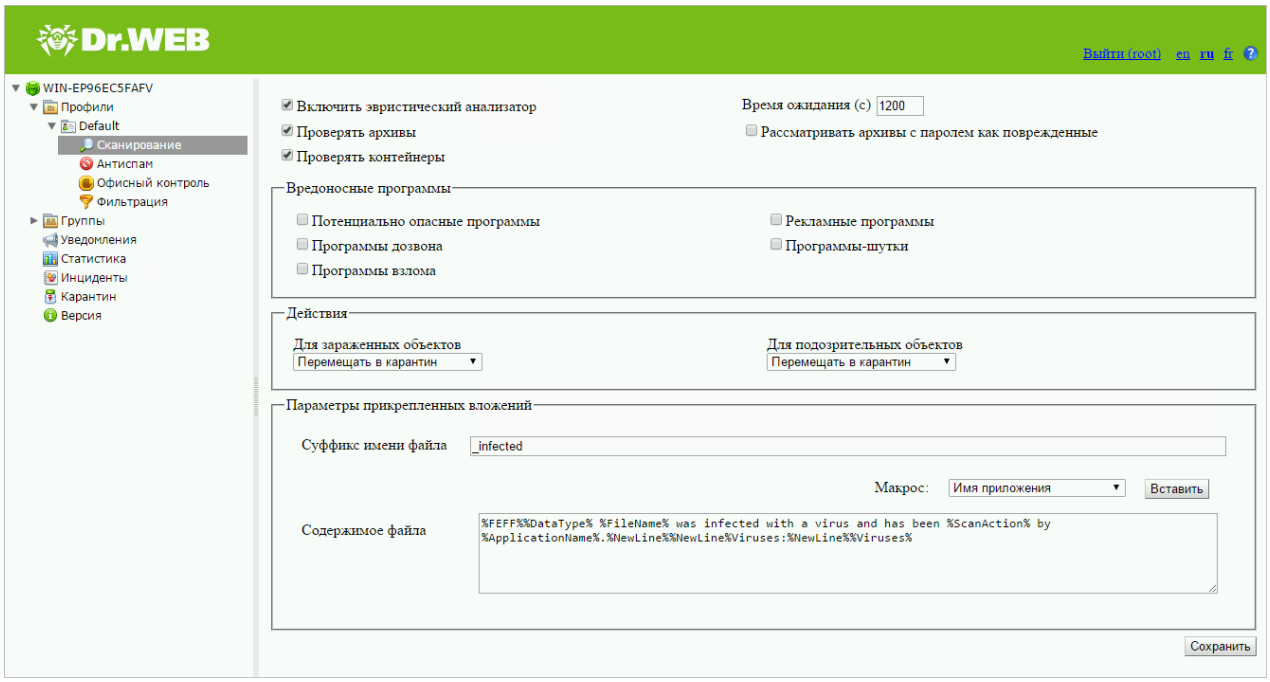

Рисунок 6. Раздел настроек сканирования

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 значение 1200 с. При необходимости вы можете изменить это значение.

Флажок **Рассматривать архивы с паролем как поврежденные** определяет, будет ли программа игнорировать защищенные паролем архивы или рассматривать их как поврежденные. Если архивы с паролем рассматриваются как поврежденные, к ним

применяется действие, установленное для зараженных объектов (см. Выбор типов 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 зараженных 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;
   - **Игнорировать** – означает, что письмо будет 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.

7.2.3. Антиспам

Антиспам анализирует содержимое электронных сообщений. На основе получаемых показателей компонент делает заключение о том, являются ли они спамом.

Работа **Антиспама** настраивается в разделе настроек **Антиспам**. Он доступен только для версии «Антивирус + Антиспам». Если ваш ключевой файл поддерживает использование компонента Антиспам, то фильтрация спама включена по умолчанию (т.е. в верхней части области сведений раздела **Антиспам** установлен флажок **Включить Антиспам**).

Если настройки в разделе **Антиспам** недоступны, то скорее всего ваша лицензия не поддерживает компонент **Антиспам** (см. Лицензионный ключевой файл).

Проверить, поддерживается ли компонент Антиспам вашей лицензией, можно в разделе **Версия** в административной консоли Dr.Web Administrator Web Console. Если модуль поддерживается, информация о нем будет отображена в секции **Информация о продукте**.

Любое редактирование ключевого файла делает его недействительным! Поэтому не открывайте лицензионный файл в текстовом редакторе.

Чтобы настроить работу Антиспама:

1. Выберите пункт **Антиспам** для настраиваемого профиля в дереве административной консоли. Откроется область сведений раздела **Антиспам** (см. Рисунок 7).

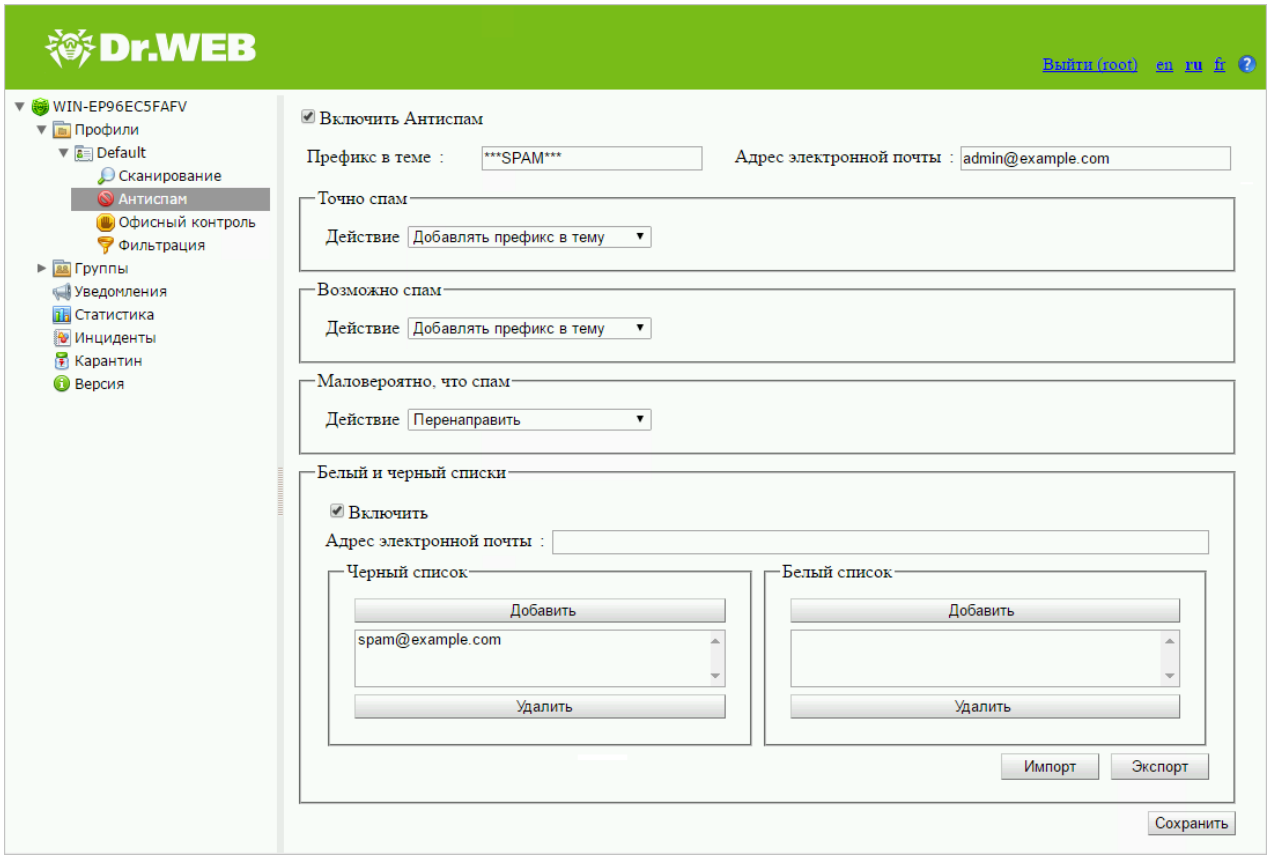

Рисунок 7. Раздел настроек Антиспама

2. Чтобы отключить **Антиспам**, снимите флажок **Включить Антиспам**. При этом все настройки параметров компонента **Антиспам** станут недоступны. Чтобы включить фильтрацию спама, установите флажок **Включить Антиспам**.
3. В поле **Префикс в теме** вы можете изменить префикс, добавляемый в тему письма, которое признано спамом. По умолчанию установлен префикс *****SPAM*****.
4. В полях ниже вы можете задать действия программы по отношению к сообщениям в зависимости от степени вероятности их принадлежности к спаму (**Точно спам**, **Возможно, спам**, **Маловероятно, что спам**). Для этого выберите желаемые действия из выпадающих списков для каждой категории:
   - **Игнорировать** – означает, что письмо будет доставлено получателю.

- **Добавлять префикс в тему –** означает, что к теме письма будет добавлен префикс, указанный в поле **Префикс в теме**.
- **Поставить штамп Move to junk –** означает, что письмо будет доставлено получателю, но помечено штампом Move to junk.
- **Перенаправить –** означает, что письмо будет перенаправлено другому получателю. При выборе этой опции станет активно поле **Адрес электронной почты**, расположенное в правом верхнем углу. В этом поле вы можете указать адрес электронной почты, на который должно быть перенаправлено письмо. Вы можете указать только один адрес.
- **Блокировать –** означает, что письмо будет заблокировано и не будет доставлено получателю.

5. В разделе **Белый и черный списки** вы можете настроить использование списков доверенных и ненадежных адресов:
   - установите флажок **Включить**, чтобы включить использование списков. Вы можете добавить электронные адреса, которым вы доверяете, в белый список. Письма с данных адресов не будут проходить проверку на спам. Если же вы добавите адрес в черный список, то всем письмам с этого адреса будет присваиваться статус **Точно спам**;
   - чтобы добавить электронный адрес, введите его в поле **Адрес электронной** почты в соответствующем списке, а затем нажмите кнопку **Добавить**;
   - чтобы удалить электронный адрес из списка, выберите его в нужном списке и нажмите кнопку **Удалить**;
   - с помощью кнопок **Импорт** и **Экспорт** сохраните списки в специальный файл с расширением **.lst** или загрузите их из файла. Вы можете создавать и редактировать списки вручную с помощью текстового редактора, например, Блокнота. Текстовый файл должен быть сохранен с расширением **.lst** в формате **Unicode**.

     Электронные адреса должны указываться с префиксом «**+**» (для добавления адреса в белый список) или «**-**» (для добавления адреса в черный список).

     Вы можете использовать подстановочный символ **«*»** вместо части адреса (например, запись вида ***@domain.org** означает все адреса в домене **domain.org**).

     Например:

     +trusted@example.com;+trusted_email@example.com;-suspicious@example.com;-spam@example.com;+*example.com.
6. Нажмите кнопку **Сохранить**, когда закончите изменять настройки **Антиспама**.

7.2.4. Офисный контроль

Офисный контроль позволяет ограничить доступ пользователей к интернет-ресурсам и нежелательным веб-сайтам (посвященным 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 административной консоли. Откроется область сведений для настройки **Офисного контроля** (см. Рисунок 8).

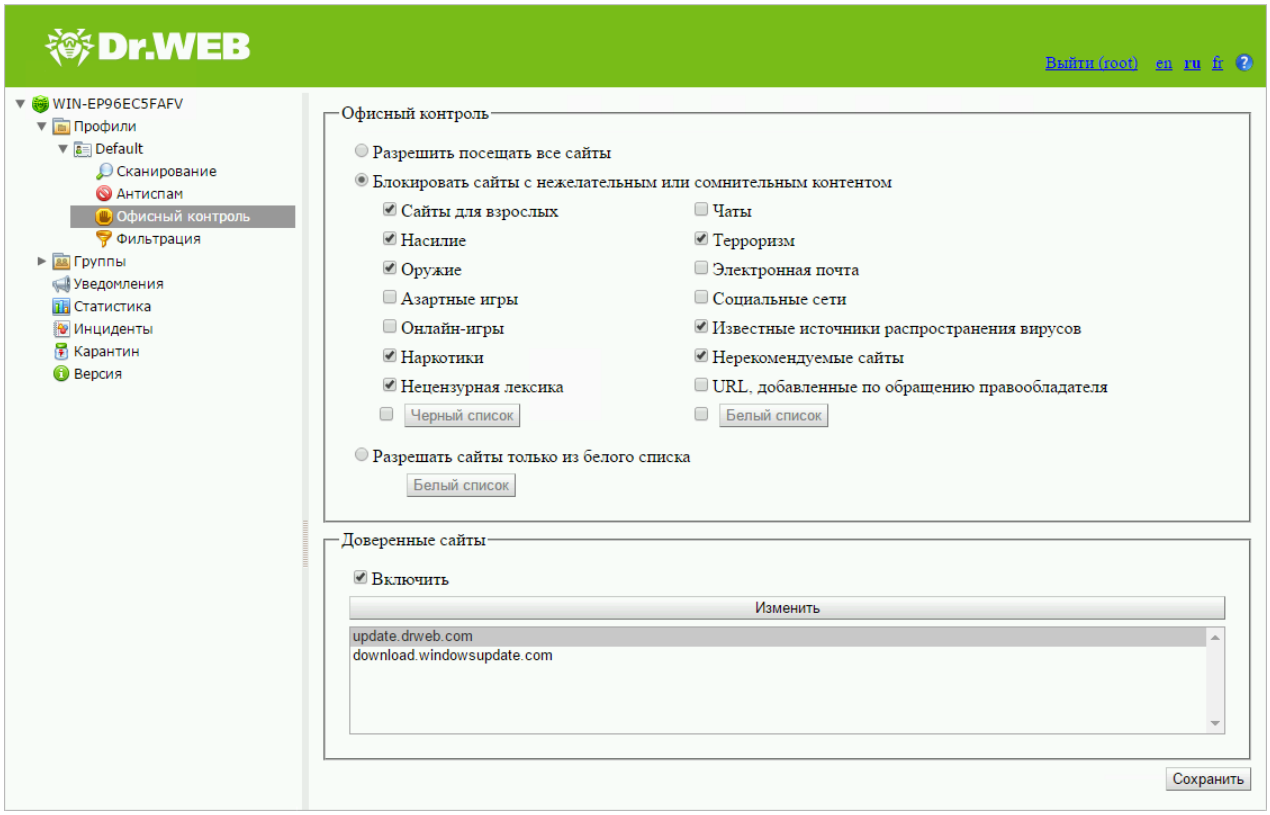

Рисунок 8. Раздел настройки Офисного контроля

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. Доверенные сайты – сайты из списка доверенных имеют наиболее высокий приоритет и исключаются из дальнейшей проверки.
   Установите 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 белого и черного списков

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.
     Если 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 часть, которая 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**.

7.2.5. Фильтрация

Приложение позволяет задать правила для фильтрации сообщений и их вложений. Фильтрация трафика настраивается в разделе настроек профиля **Фильтрация** (см. Рисунок 9).

Чтобы приступить к созданию правил, установите флажок **Включить фильтрацию** в верхней части раздела.

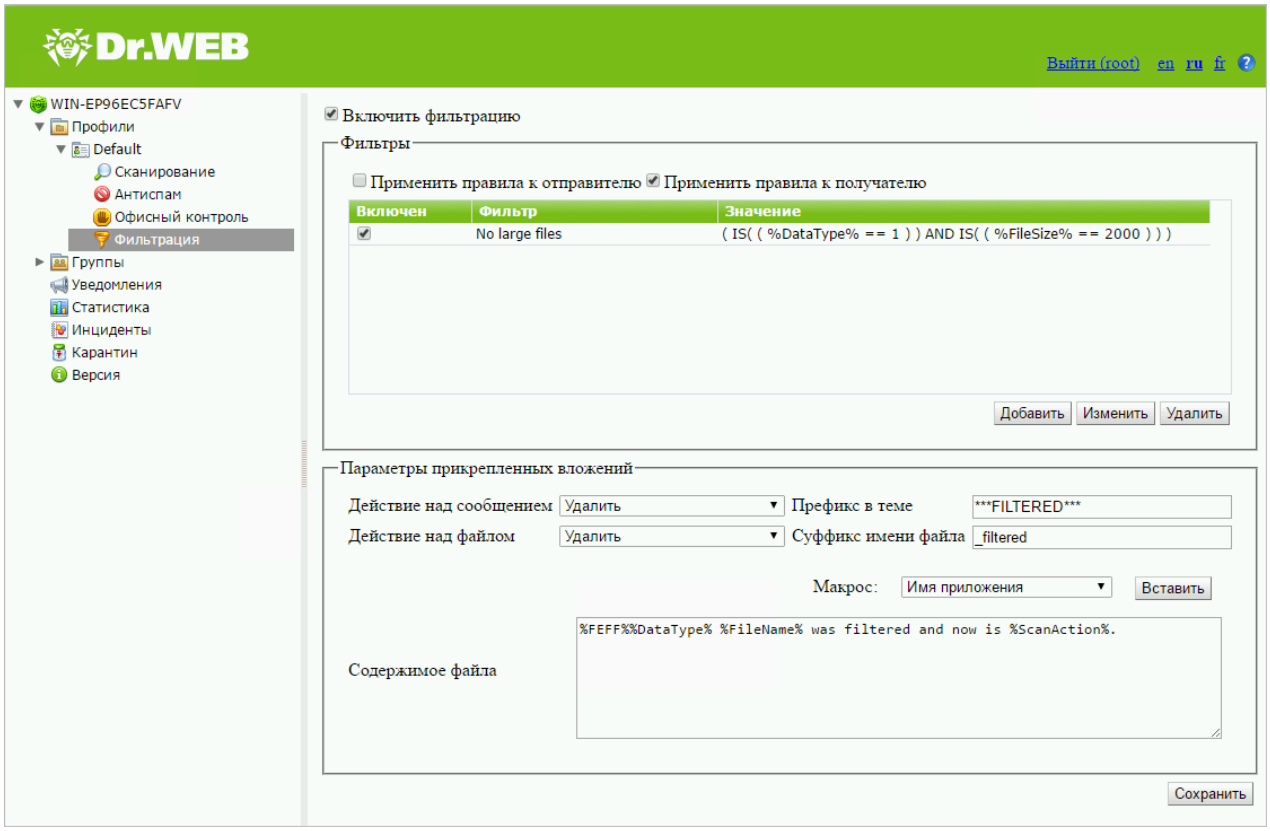

Рисунок 9. Раздел настройки фильтрации

Если вы работаете с разделом **Фильтрация** в первый раз, список правил будет пустым. Вы можете создать и настроить правила фильтрации.

Создание правила фильтрации

1. Нажмите кнопку **Добавить** под списком правил. Откроется окно **Правило фильтрации** (см. Рисунок 10), в котором вы можете задать имя правила и его условия.
2. Вы можете добавить одно или несколько условий, выбрать одновременное выполнение всех условий или выполнение любого из них.

   Чтобы добавить новое условие, нажмите кнопку **Добавить**. В открывшемся окне вы можете выбрать тип условия, указать значение и тип соответствия условия заданному значению (типы условий, соответствия и возможные значения приведены в таблице ниже).
3. Нажмите **ОК**, чтобы сохранить правило. Нажмите **Отмена**, чтобы закрыть окно без сохранения изменений.

Чтобы изменить или удалить добавленное правило, выделите его в списке и нажмите кнопку **Изменить** или **Удалить**.

Ниже приведен пример создания правила фильтрации.

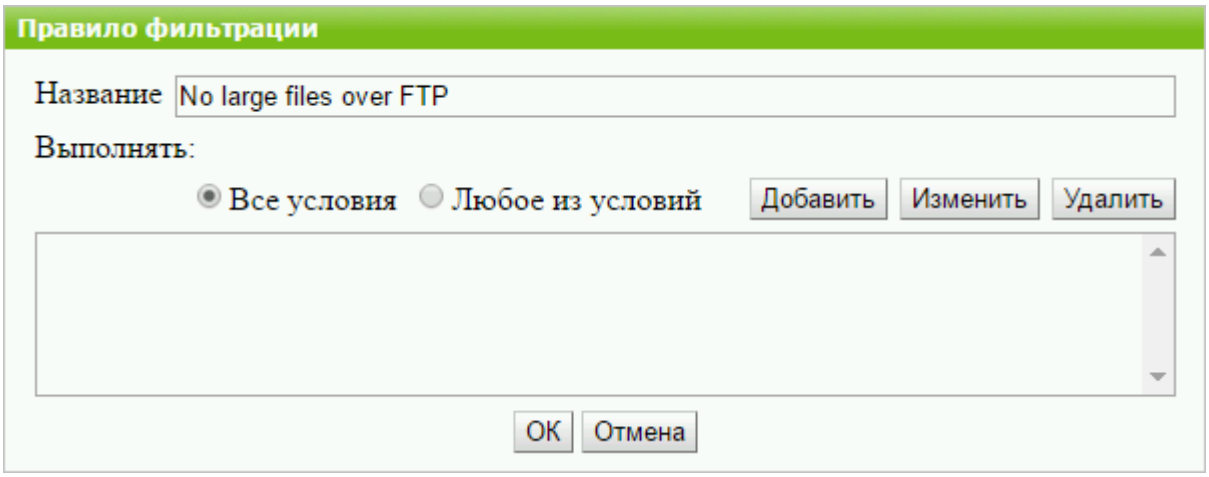

Рисунок 10. Создание правила фильтрации

Чтобы настроить фильтрацию сообщений:

1. Включите использование одного или нескольких правил из списка, установив соответствующие флажки.

   Правила фильтрации могут применяться как и к отправителю и получателю, так и либо только к отправителю, либо только к получателю.
   Например, вы можете создать правило, в котором тема сообщения включает слово «Attention». Если вы установите это правило только для отправителя, то вы не сможете отправлять сообщения со словом «Attention» в теме письма. Если вы установите это правило только для получателя, то вы не сможете получать сообщения со словом «Attention» в теме. Если вы установите это правило для отправителя и для получателя, то вы не сможете ни отправлять, ни получать сообщения со словом «Attention» в теме письма.
2. В разделе **Параметры прикрепленных вложений** настройте действия для почтовых сообщений с вложениями.
   Для сообщений вы можете выбрать одно из следующих действий:

   - **Удалить** – удалить сообщение;
   - **Добавлять префикс в тему** – пропустить сообщение, добавив в его тему префикс, заданный в поле **Префикс в теме**.

   Для вложенных файлов доступны следующие действия:

   - **Удалить** – удалить вложенный файл;
   - **Перемещать в карантин** – перемещать вложенный файл в карантин.

   В поле **Префикс в теме** вы можете изменить префикс, добавляемый в тему отфильтрованного письма. По умолчанию установлен префикс ***FILTERED***.

В поле **Суффикс имени файла** вы можете при необходимости изменить суффикс, который добавляется к имени текстового файла, прикрепляемого к отфильтрованному письму. По умолчанию указано значение **_filtered.txt**.

В поле **Содержимое файла** вы можете изменить текст, содержащийся в прикрепляемом файле. При редактировании текста содержимого файла вы можете использовать макросы из выпадающего списка **Макрос**.

4. Нажмите кнопку **Сохранить**, когда закончите изменять настройки фильтрации

Таблица условий для создания правила фильтрации

Тип условия	**Тип соответствия**	**Значение**
Тип данных	Равно Не равно	Файл Сообщение
Источник данных	Равно Не равно Включает Не включает Соответствует Не соответствует	Указывается вручную. Если выбран тип соответствия **Включает**, **Не включает**, **Соответствует** или **Не соответствует**, при вводе значения вы можете использовать подстановочные символы «*****» и «**?**» вместо любой последовательности символов или одного любого символа.
Адресат данных	Равно Не равно Включает Не включает Соответствует	Указывается вручную. Если выбран тип соответствия **Включает**, **Не включает**, **Соответствует** или **Не соответствует**, при вводе значения вы можете использовать подстановочные символы «*****» и «**?**» вместо любой последовательности символов или одного любого символа.

	Не соответствует	
Протокол	Равно Не равно	HTTP FTP POP3 SMTP
Число получателей	Равно Не равно Больше Не больше Меньше Не меньше	Указывается вручную.
Имя файла	Равно Не равно Включает Не включает Соответствует Не соответствует	Указывается вручную. Если выбран тип соответствия **Включает**, **Не включает**, **Соответствует** или **Не соответствует**, при вводе значения вы можете использовать подстановочные символы «*****» и «**?**» вместо любой последовательности символов или одного любого символа.
Размер файла	Равно Не равно Больше Не больше Меньше Не меньше	Указывается вручную (в байтах).

Тема сообщения	Равно Не равно Включает Не включает Соответствует Не соответствует	Указывается вручную. Если выбран тип соответствия **Включает**, **Не включает**, **Соответствует** или **Не соответствует**, при вводе значения вы можете использовать подстановочные символы «*****» и «**?**» вместо любой последовательности символов или одного любого символа.
Есть вложение	Равно Не равно	Ложь Истина

Пример правила фильтрации

Для фильтрации файлов, размер которых превышает 20 Мб, передаваемых по протоколу FTP, можно использовать правило (см. Рисунок 11), состоящее в одновременном выполнении следующих условий:

Тип условия	Тип соответствия	Значение
Тип данных	Равно	Файл
Протокол	Равно	FTP
Размер файла	Больше	20000

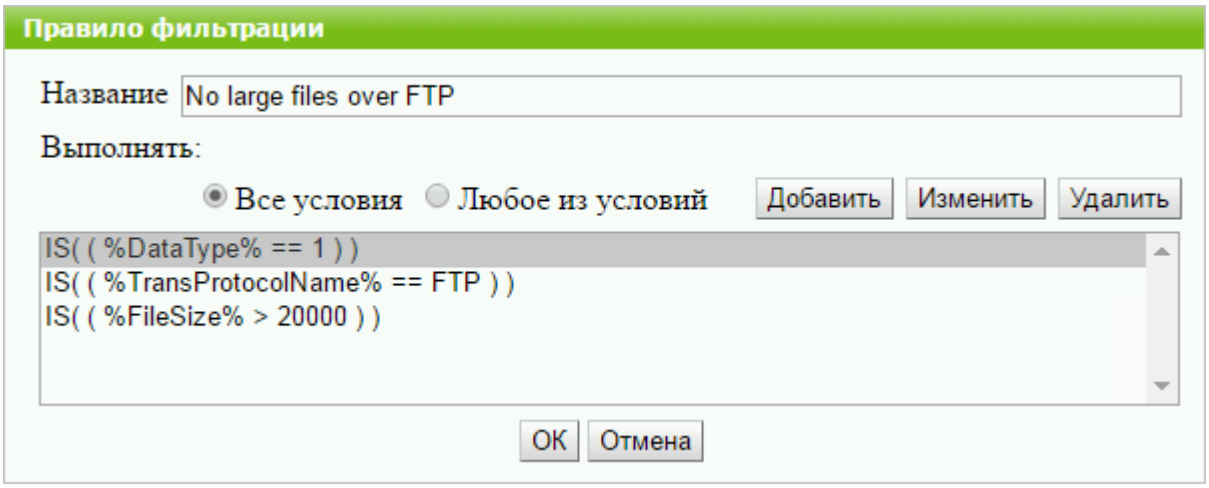

Рисунок 11. Пример правила фильтрации

7.3. Управление группами клиентов

По умолчанию Dr.Web применяет параметры стандартного профиля для всех клиентов. Если вы желаете применить параметры другого профиля для определенных клиентов (см. Создание и настройка профилей), вам необходимо объединить этих клиентов в группу и присвоить ей созданный профиль. Таким образом, вы можете разделить всех клиентов на группы, для каждой из которых будут установлены отдельные параметры защиты.

7.3.1. Создание новой группы

Для управления существующими группами и создания новых откройте область сведений раздела **Группы**. Для этого выберите пункт **Группы** в дереве административной консоли Dr.Web Administrator Web Console (см. Рисунок 12).

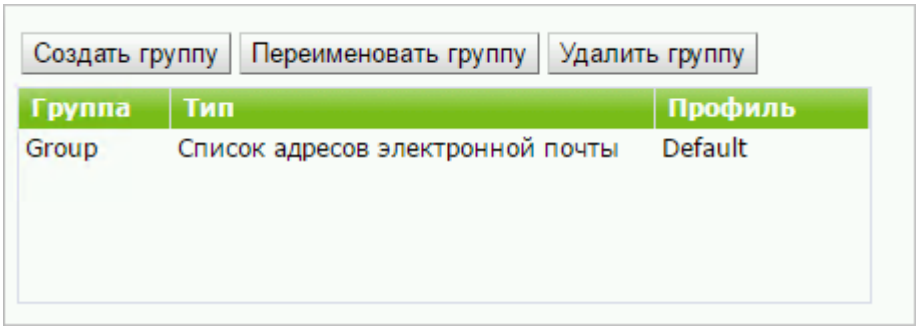

Рисунок 12. Раздел Группы

Создание новой группы

Чтобы создать новую группу:

- в области сведений раздела **Группы** нажмите кнопку **Создать группу**, расположенную над списком существующих групп;
- щелкните правой кнопкой на пункте **Группы** в дереве консоли и нажмите **Создать группу** в контекстном меню.

В окне **Создать группу** укажите имя для новой группы и нажмите **ОК**. По умолчанию, новой группе назначается профиль **Default**.

Имена групп должны быть заданы латинскими символами.

Изменение имени группы

Чтобы переименовать группу, выберите нужную группу в списке в области сведений раздела **Группы** и нажмите кнопку **Переименовать группу**.

Удаление группы

Чтобы удалить группу, выберите ее в списке в области сведений раздела **Группы** и нажмите кнопку **Удалить группу**.

Просмотр настроек группы

Чтобы открыть область сведений с настройками группы, выберите ее имя в дереве административной консоли. Вы можете изменить такие параметры, как тип группы и назначенный ей профиль (см. Настройки и формирование групп).

Когда вы закончите создание и формирование необходимых вам групп, нажмите кнопку **Сохранить**.

7.3.2. Настройки и формирование групп

В области сведений, открывающейся при щелчке по группе в дереве административной консоли (см. Рисунок 13), вы можете изменить настройки выбранной группы, в том числе определить способ ее формирования: путем задания списка почтовых адресов, IP-адресов или путем выбора из списка групп Active Directory.

Вы можете выбрать тип группы в выпадающем списке **Тип**.
Выбор типа группы зависит от протокола, с которым предполагается работа в текущем профиле. Например, при работе с протоколом SMTP вам рекомендуется выбрать тип **Список адресов электронной почты**, а при работе с протоколом FTP рекомендуется указать тип **Список IP-адресов**.

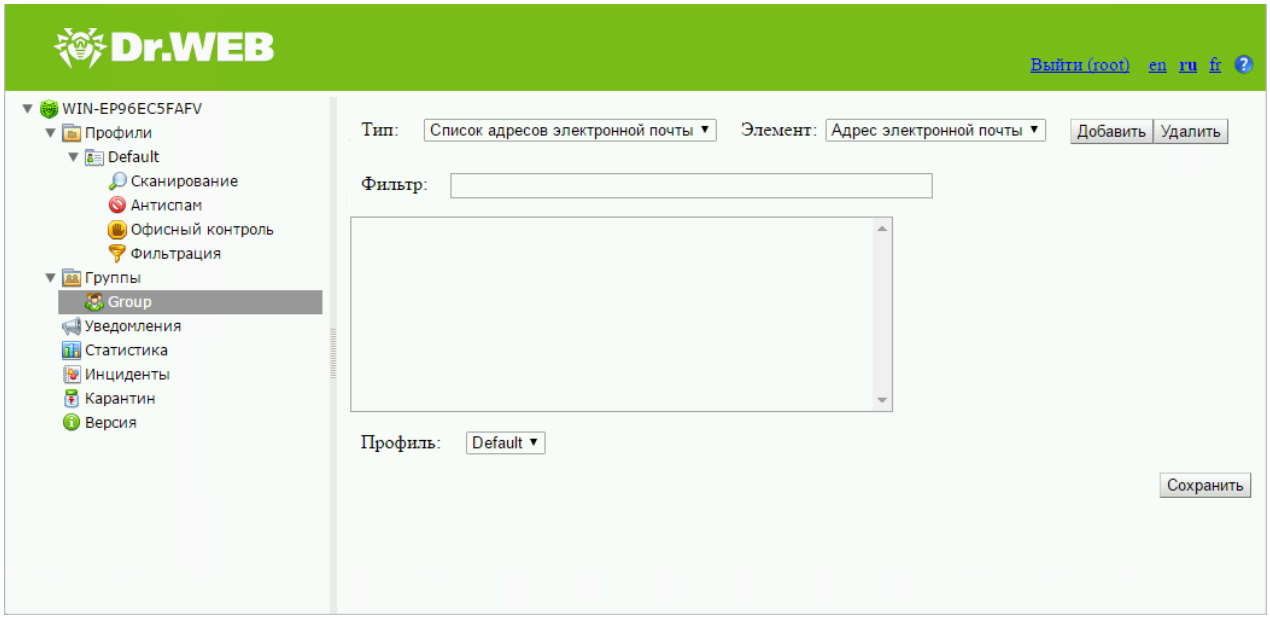

Рисунок 13. Настройки группы

Чтобы сформировать список почтовых адресов:

1. В выпадающем списке **Тип** выберите значение **Список адресов электронной почты**.
2. Чтобы добавить почтовый адрес в список, нажмите кнопку **Добавить**. В открывшемся окне введите адрес электронной почты и нажмите кнопку **OK**.
3. Чтобы удалить адрес из списка, выделите его и нажмите кнопку **Удалить**, после чего подтвердите удаление выбранного адреса.

Вы можете использовать подстановочные символы «*» и «?» вместо любой последовательности символов или одного любого символа вводимого текста соответственно.

Чтобы сформировать список IP-адресов:

1. В выпадающем списке **Тип** выберите значение **Список IP-адресов**.
2. В выпадающем списке **Элемент** выберите тип элемента списка: **IP-адрес** или **Диапазон IP-адресов**.
3. Чтобы добавить новый элемент в список, нажмите кнопку **Добавить**. В открывшемся окне в зависимости от выбранного типа элемента списка введите IP-адрес или укажите диапазон IP-адресов. Далее нажмите кнопку **OK**.
4. Чтобы удалить элемент из списка, выделите его и нажмите кнопку **Удалить**, после чего подтвердите удаление выбранного элемента списка.

Чтобы сформировать список групп Active Directory:

1. В выпадающем списке **Тип** выберите значение **Список групп Active Directory**.

2. Чтобы добавить группу в список, нажмите кнопку **Добавить**. В открывшемся окне выберите группу и нажмите кнопку **ОК**.
3. Чтобы удалить группу из списка, выделите ее и нажмите кнопку **Удалить**, после чего подтвердите удаление выбранной группы.

Формирование списка групп Active Directory возможно в том случае, если сервер включен в домен.

Если сервер не включен в домен, вы можете сформировать список групп Active Directory, используя консоль Dr.Web CMS Web Console. Для этого:

1. Откройте консоль Dr.Web CMS Web Console.
2. Для параметра **/DrWebADAccessor_1.0/Application Settings/ADAccUserName** укажите имя пользователя, имеющего доступ к Active Directory.
3. Для параметра **/DrWebADAccessor_1.0/Application Settings/ADAccPassword** укажите пароль пользователя, имеющего доступ к Active Directory.

По умолчанию значения этих параметров не проставлены.

В выпадающем списке **Профиль** выберите профиль, который вы хотите назначить данной группе.

После того, как вы закончите изменять настройки выбранной группы, нажмите кнопку **Сохранить**.

7.4. Уведомления

Уведомления заносятся в журнал операционной системы и используются для информирования администратора о различных событиях, связанных с работой Dr.Web (например, связанных с обнаружением инфицированных объектов, спама, фильтрацией сообщений и т.д.).

Чтобы настроить уведомления:

1. Выберите пункт **Уведомления** в дереве административной консоли. Откроется область сведений для настройки уведомлений (см. Рисунок 14).

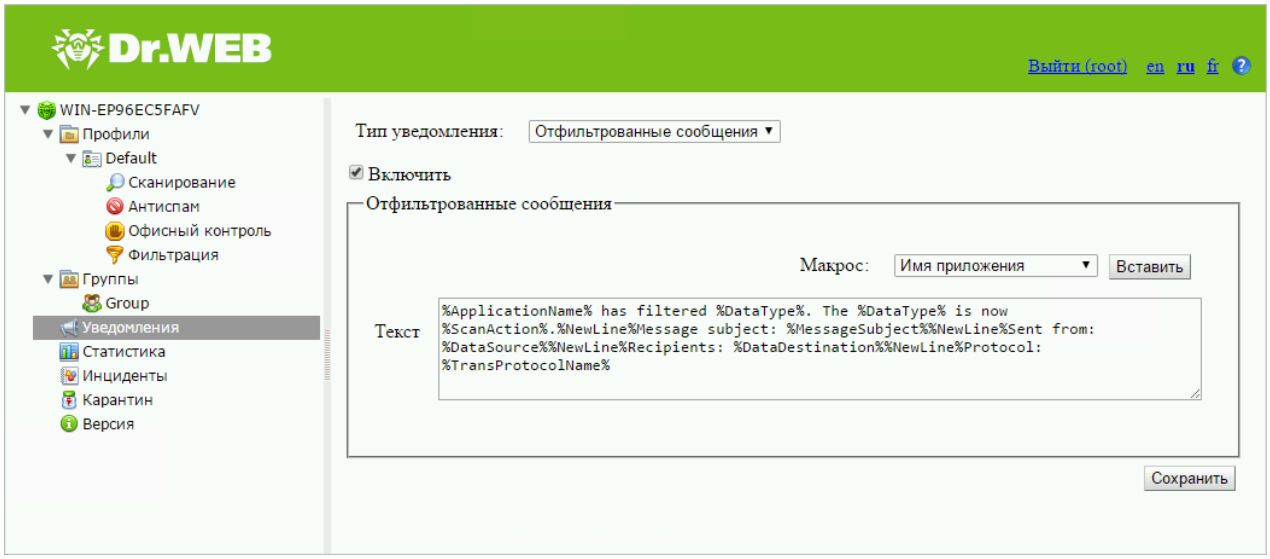

Рисунок 14. Раздел настройки уведомлений

2. В списке **Тип уведомления** выберите тип событий для отправки уведомлений:
   - **Отфильтрованные сообщения** – для отправки уведомлений о фильтрации сообщений;
   - **Отфильтрованные файлы** – для отправки уведомлений о фильтрации вложений;
   - **Зараженные** – для отправки уведомлений об обнаруженных вирусных угрозах;
   - **Спам** – для отправки уведомлений о спаме;
   - **Обновление** – для отправки уведомлений с информацией о последнем обновлении;
   - **Устаревшие базы** – для отправки уведомлении о необходимости обновить вирусные базы;
   - **Офисный контроль** – для отправки уведомлений о фильтрации сетевых ресурсов с помощью **Офисного контроля**.
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 для замены ключевых слов из выпадающего списка **Макрос**.
5. Нажмите кнопку **Сохранить**, когда закончите изменять настройки уведомлений.

7.5. Просмотр статистики

Раздел **Статистика** позволяет просмотреть общие или средние количественные данные о работе Dr.Web за определенный период времени (см. Рисунок 15).

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 Dr.Web;
   - **За день** – для просмотра статистики за последние сутки работы Dr.Web;
   - **За час** – для просмотра статистики за последний час работы Dr.Web;
   - **За минуту** – для просмотра статистики за последнюю минуту работы Dr.Web;
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 (в том числе, отфильтрованных, спам-писем, подозрительных и т.д.).
- **Действия над проверенными объектами**. Данный подраздел содержит статистическую информацию о действиях, которые были применены Dr.Web к обнаруженным вредоносным объектам.
- **Типы угроз**. В данном подразделе содержится информация о различных типах угроз, обнаруженных Dr.Web за выбранный период времени.
- **Категории сайтов**. В данном подразделе отображается статистика работы Офисного контроля, а также количество заблокированных ресурсов по категориям.

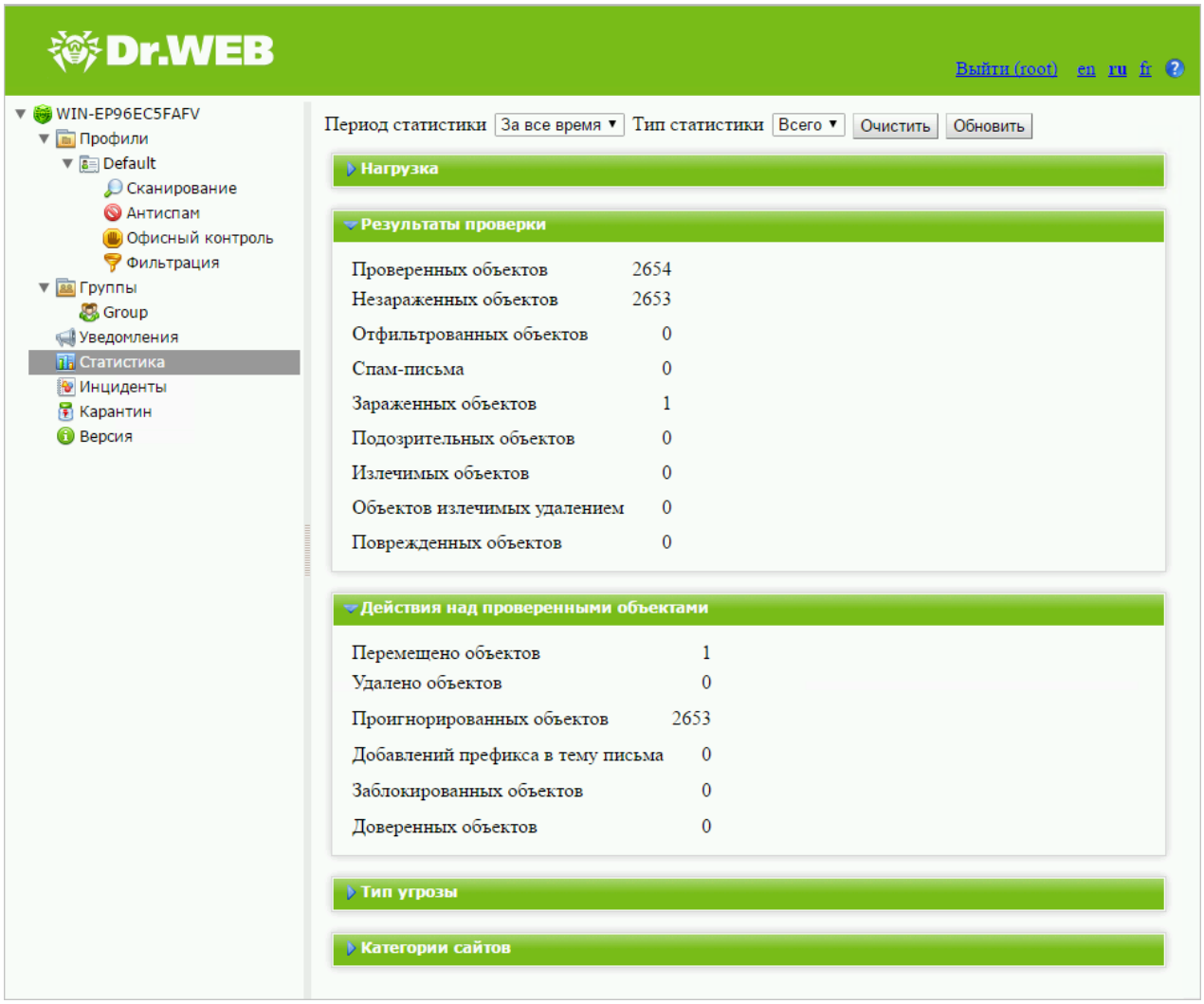

Рисунок 15. Раздел статистики

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

7.6. Просмотр списка инцидентов

Раздел **Инциденты** позволяет просмотреть список событий, связанных со срабатыванием антивирусной защиты и Антиспама за указанный промежуток времени, и информацию об этих событиях (см. Рисунок 16).

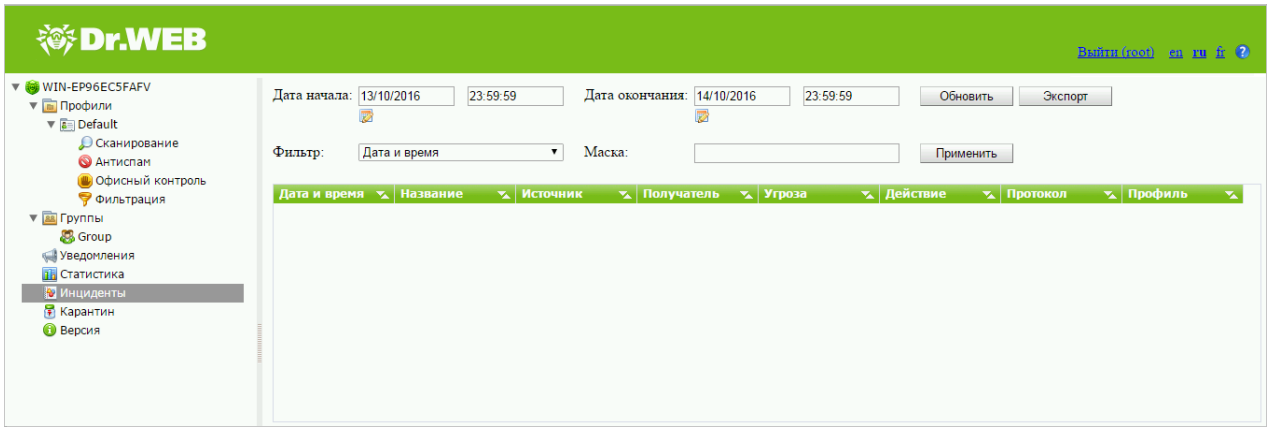

Рисунок 16. Инциденты

Информация о событиях

Для каждого инцидента в списке отображается следующая информация:

- дата и время;
- название объекта, с которым связан инцидент;
- источник и получатель;
- тип угрозы;
- действие, которое было применено к угрозе;
- протокол передачи;
- название примененного профиля.

Вы можете задать параметры отображения информации в списке инцидентов:

1. Щелкните правой кнопкой мыши по заголовку списка и выберите в контекстном меню пункт **Выбрать столбцы**.
2. Выберите типы информации, которые вы хотите включить в просмотр.

Действия над списком инцидентов

1. Вы можете настроить просмотр инцидентов за определенный период времени. Для этого укажите дату и время начала и окончания интересующего интервала и нажмите кнопку **Обновить**.
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**.

Вы можете использовать подстановочные символы «*» и «?» вместо любой последовательности символов или одного любого символа вводимого текста соответственно.

3. Вы можете сохранить список инцидентов в виде текстового файла. Для этого нажмите кнопку **Экспорт**. В открывшемся окне выберите формат файла для сохранения и нажмите кнопку **ОК**. Список инцидентов может быть сохранен в виде HTML-документа или в формате TSV (Tab Separated Values).
4. Для того чтобы отсортировать записи в списке по тому или иному критерию, нажмите на соответствующий заголовок колонки.
5. Для обновления списка инцидентов нажмите кнопку **Обновить**. Список обновляется при каждом запуске административной консоли Dr.Web Administrator Web Console и переходе в раздел **Инциденты**. Обновление может занять некоторое время. Если вы хотите отменить ход обновления, например, при ошибочно указанных параметрах фильтрации, нажмите кнопку **Отмена**.

7.7. Работа с карантином

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

В разделе Карантин административной консоли Dr.Web Administrator Web Console выводится информация о текущем состоянии Карантина.

Кроме того, для просмотра и редактирования содержимого **Карантина** вы можете использовать утилиту Менеджер Карантина.

7.7.1. Просмотр карантина с Dr.Web Administrator Web Console

Вкладка **Карантин** (см. Рисунок 17) административной консоли Dr.Web Administrator Web Console используется для просмотра списка изолированных объектов и краткой информации об этих объектах.

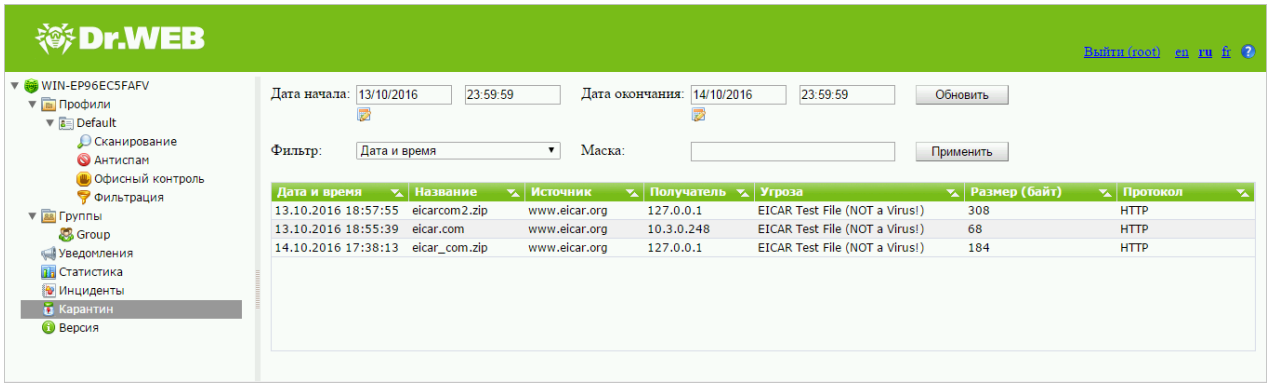

Рисунок 17. Список объектов в Карантине

Просмотр информации об объектах в карантине

Для каждого события в списке отображается следующая информация:

- дата и время перемещения в карантин;
- имя инфицированного файла;
- источник и получатель;
- название угрозы;
- размер файла (в байтах);
- протокол передачи.

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

- Для просмотра объектов, перемещенных в карантин в течение определенного периода времени, укажите даты и время начала и окончания интересующего вас интервала и нажмите кнопку **Обновить**.
- 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**.

  Вы можете использовать подстановочные символы «*****» и «**?**» вместо любой последовательности символов или одного любого символа вводимого текста соответственно.

- Чтобы отсортировать записи в списке по тому или иному критерию, нажмите на соответствующий заголовок колонки.
- Для обновления списка событий нажмите кнопку **Обновить**. Список объектов в карантине обновляется при каждом запуске административной консоли Dr.Web Administrator Web Console и переходе в раздел **Карантин**. Обновление может занять некоторое время. Если вы хотите отменить ход обновления, например, при ошибочно указанных параметрах фильтрации, нажмите кнопку **Отмена**.

Действия над объектами в карантине

1. Чтобы удалить объект из списка, щелкните правой кнопкой мыши по объекту и выберите **Удалить** в контекстном меню (для выбора нескольких объектов удерживайте нажатой клавишу SHIFT или CTRL на клавиатуре).
2. Чтобы восстановить объект, щелкните правой кнопкой мыши по объекту и выберите **Восстановить** в контекстном меню.

Чтобы настроить параметры карантина, используйте утилиту Менеджер карантина.

7.7.2. Менеджер карантина

Менеджер карантина – это дополнительная утилита, входящая в состав Dr.Web. Она служит для настройки параметров карантина и работы с изолированными файлами.

Для запуска **Менеджера Карантина** (см. Рисунок 18) воспользуйтесь ссылкой **Dr.Web Quarantine** на Рабочем столе.

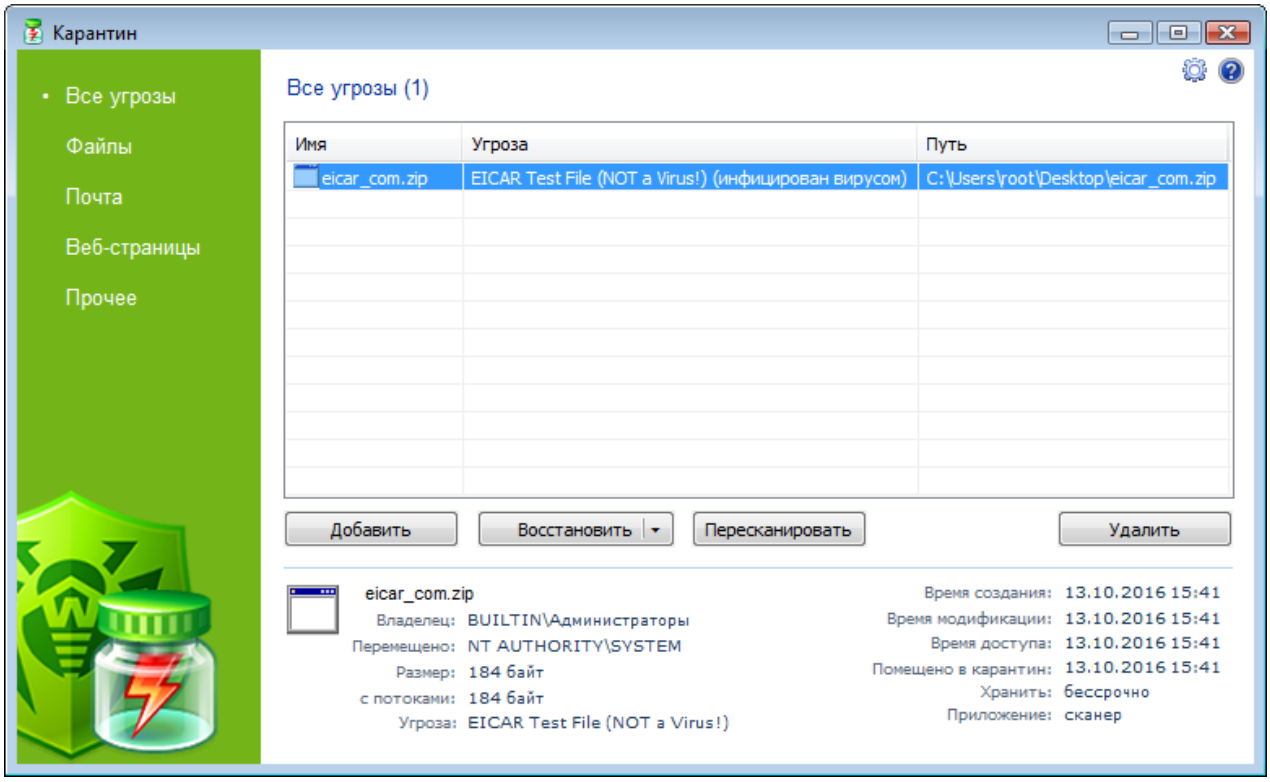

Рисунок 18. Главное окно утилиты Dr.Web Quarantine

Окно **Менеджера карантина** состоит из нескольких частей:

1. Боковая панель слева служит для фильтрации отображаемых объектов карантина. При нажатии на соответствующий пункт, в центральной части окна будут показаны все объекты карантина или только заданные группы объектов:
   - файлы;
   - почтовые объекты;
   - веб-страницы;
   - все остальные объекты, не попадающие в предыдущие категории.
2. 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 Dr.Web при автоматическом перемещении объекта в карантин;
   - **Путь** – полный путь, по которому находился объект до перемещения в Карантин.
3. В нижней части окна карантина отображается подробная информация о выделенных объектах карантина.

Вы можете включить отображение столбцов с подробной информацией об объекте.

Чтобы настроить отображение столбцов:

1. Чтобы задать параметры отображения информации в таблице **Менеджера 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 или 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**.

   Чтобы закрыть окно без сохранения изменений нажмите кнопку **Отменить**.

7.7.2.1. Управление карантином с помощью Менеджера карантина

В окне **Менеджера карантина** доступны следующие кнопки управления:

- **Добавить** – добавить файл в карантин. В окне выбора файлов укажите нужный файл;
- **Восстановить** – переместить файл из карантина и восстановить первоначальное местоположение файла. Путь для восстановления файла указан в колонке **Путь** на Рисунке 18. 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.

7.7.2.2. Настройка свойств карантина

С помощью **Менеджер карантина** можно задать параметры карантина. Для этого:

1. Нажмите на кнопку **Настройки** в окне **Менеджер 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, для которых были применено удаление либо лечение. Резервные копии создаются автоматически при удалении файлов либо лечении. Резервные копии сохраняются временно.
3. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений. Нажмите **Отмена**, чтобы закрыть окно настроек без сохранения изменений.

8. Обновление вирусных баз

Для обнаружения вредоносных объектов Dr.Web использует специальные вирусные базы, в которых содержится информация обо всех известных вредоносных программах. Так как каждый день появляются новые вредоносные программы, эти базы требуют периодического обновления. Для этого в приложении реализована система обновления вирусных баз через Интернет. В течение срока действия лицензии модуль обновления регулярно пополняет вирусные базы информацией о новых вирусах и вредоносных программах.

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

Вы можете запустить обновление вирусных баз, щелкнув по ссылке **Запустить** в разделе **Задание на обновление**.

Параметры обновления можно изменить в файле drwupsrv.bat.

Во время установки Dr.Web создается задание по обновлению вирусных баз, в котором задан оптимальный интервал запроса обновлений с серверов обновлений «Доктор Веб». Вы можете отредактировать данное расписание при помощи планировщика заданий Windows:

1. Откройте планировщик заданий.
2. В контекстном меню задания **Doctor Web for MSP Update Task** выберите пункт **Свойства**.
3. В диалоговом окне **Doctor Web for MSP Update Task** выберите вкладку **Триггеры** (или **Расписание**, если на вашем компьютере установлена ОС Windows Server 2003) и измените период обновления. По умолчанию, обновление вирусных баз программы выполняется ежедневно каждый час.
4. Нажмите кнопку **ОК**.

8.1. Информация о версии программы и вирусных базах

В области сведений административной консоли **Версия** (см. Рисунок 19) вы можете ознакомиться с информацией о версии приложения, лицензии, вирусных базах, а также о времени и результате последнего обновления программы.

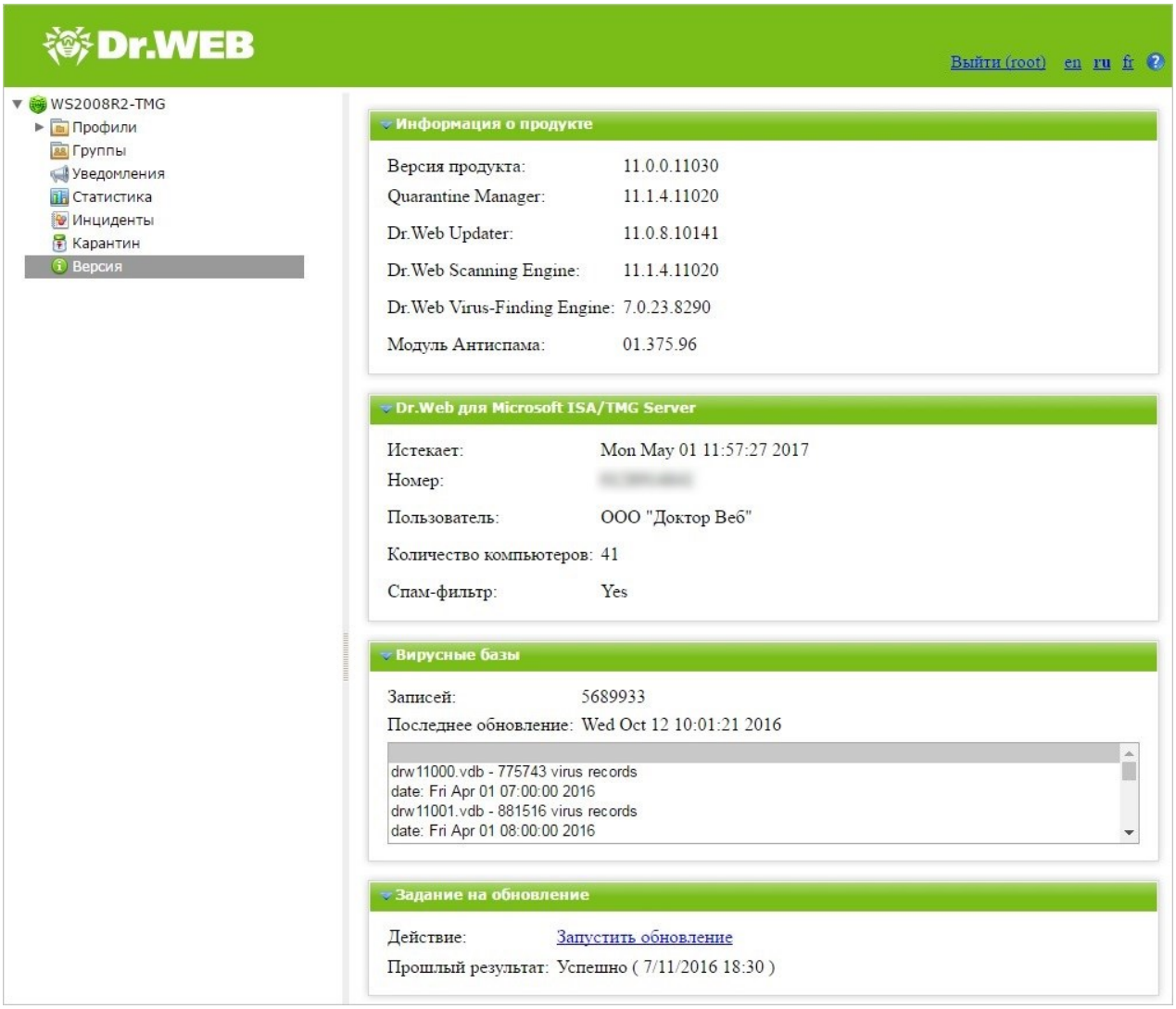

Рисунок 19. Версия

9. Веб-консоль Dr.Web CMS Web Console

Веб-консоль **Dr.Web CMS Web Console** – это дополнительная консоль, входящая в состав Dr.Web. С ее помощью можно вручную задавать значения переменных, чтобы устранить возникшие ошибки или изменить параметры работы приложения. Например, создать кластер, добавить администраторов, изменить параметры учетных записей, и т.д.

Используйте Dr.Web CMS Web Console в том случае, если вы точно знаете значения переменных, которые вы указываете вручную. Для общего управления настройками приложения используйте административную консоль Dr.Web Administrator Web Console.

Запуск консоли Dr.Web CMS Web Console

Для запуска консоли Dr.Web CMS Web Console (см. Рисунок 20) откройте в браузере следующую страницу:

`https://<ISA Server address>:2080/root`,

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

> Для доступа к странице консоли Dr.Web CMS Web Console необходимо ввести данные учетной записи администратора.
>
> При первом запуске Dr.Web CMS Web Console используйте данные учетной записи по умолчанию: имя пользователя **root** и пароль **drweb**. Далее настоятельно рекомендуется изменить пароль для данной учетной записи (подробнее в разделе Изменение пароля администратора).

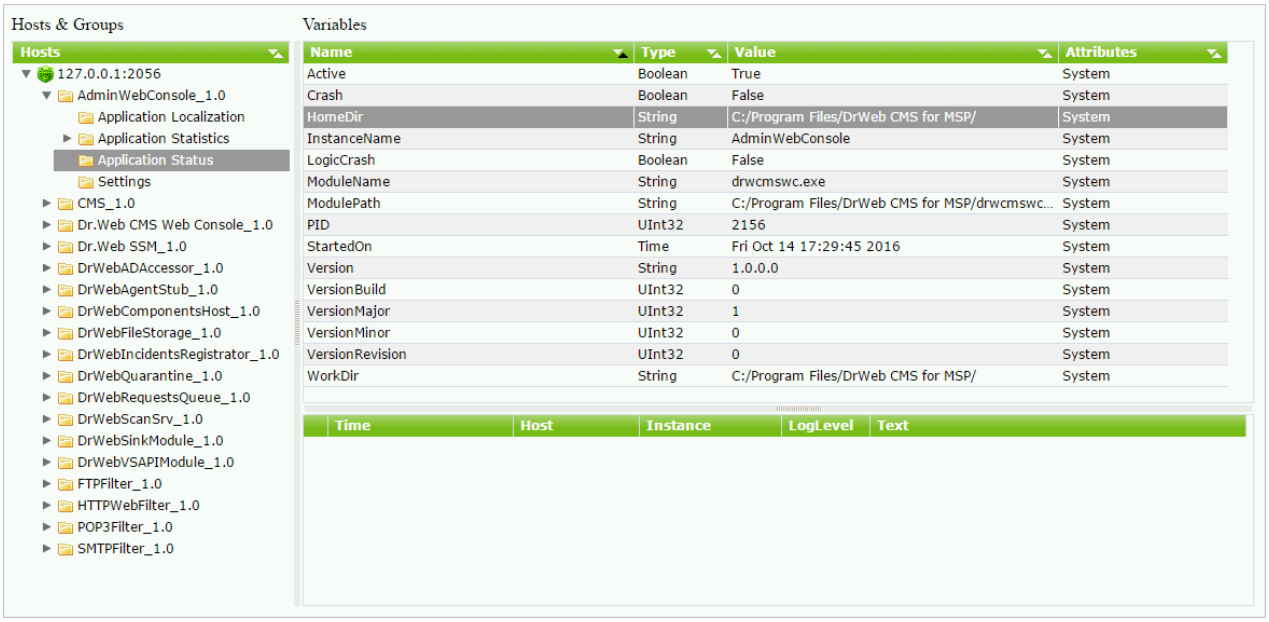

Рисунок 20. Веб-консоль Dr.Web CMS Web Console

Интерфейс

Веб-консоль Dr.Web CMS Web Console 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 адресу хоста открывается контекстное меню, в котором доступны следующие функции:

   - **Add host**. Добавить в дерево подключение к новому хосту;
   - **Remove host**. Удалить подключение к хосту из дерева;
   - **Create group**. Создать новую группу;
   - **Create variable**. Создать новую переменную;
   - **View traces**. Отображать сообщения трассировки в режиме реального времени;
   - **Debug traces**. Включить режим отладки;
   - **Load traces**. Загружать отфильтрованные сообщения трассировки за прошедшие периоды;
   - **Edit trace filter**. Изменить параметры фильтрации сообщений трассировки.

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 сообщений трассировки

   В данном окне отображаются сообщения трассировки, содержащие информацию о событиях, регистрируемых консолью Dr.Web CMS Web Console.

   Для отображения сообщений трассировки в режиме реального времени установите флажок **View traces** в контекстном меню, раскрывающемся при щелчке правой кнопкой мыши по адресу хоста.

   Каждое сообщение имеет следующие поля:

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

Чтобы отфильтровать сообщения, выводимые в окне трассировки, выберите пункт **Edit trace filter** контекстного меню, раскрывающегося при щелчке правой кнопкой мыши по адресу хоста. В открывшемся окне укажите параметры фильтрации:

- **Log level**. Степень детализации журнала событий;
- **Instances**. Источники событий;
- **Contents**. Текст, входящий в сообщение (в поле **Text**);
- **NonContents**. Текст, не входящий в сообщение (в поле **Text**).

Для удаления сообщения, выполните команду **Clear** контекстного меню, раскрывающегося при щелчке правой кнопкой мыши по сообщению.

9.1. Изменение пароля администратора

При первом запуске административной консоли Dr.Web Administrator Web Console или веб-консоли Dr.Web CMS Web Console 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.

9.2. 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**.
6. Для настройки уровня доступа щелкните по соответствующей группе в дереве хостов и групп. Выберите пункт **Create variable** в контекстном меню.
7. Откроется окно **Add new variable**. Введите имя переменной **UserLevel** и выберите **UInt32** в качестве ее типа. В качестве значения переменной установите:

   0 – полный доступ ко всем настройкам консоли;

   1 – доступ к консоли без возможности изменения настроек.

Если значение переменной **UserLevel** не задано, администратору будет предоставлен полный доступ к настройкам консоли **Dr.Web Administrator Web Console**.

9.3. Создание кластеров

Консоль **Dr.Web CMS Web Console** 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**. 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**.

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.

Список подчиненных хостов можно создать на любом уровне дерева.

При включенном брандмауэре Windows для корректной работы кластера необходимо разрешить обмен данными по протоколу TCP между управляющим и подчиненным хостами. Для этого требуется создать следующие правила брандмауэра Windows:

- входящее правило для связи управляющего сервиса **drwcms.exe** головного хоста с подчиненным хостом по протоколу TCP и любому порту;
- исходящее правило для связи управляющего сервиса **drwcms.exe** головного хоста с подчиненным хостом по протоколу TCP и порту 2056;
- входящее правило для связи подчиненного хоста с управляющим сервисом **drwcms.exe** головного хоста по протоколу TCP и порту 2056;
- исходящее правило для связи подчиненного хоста с управляющим сервисом **drwcms.exe** головного по протоколу TCP и любому порту.

Управление настройками сканирования и фильтрации для групп Active Directory

Переменные с атрибутом **Shared** профилей и групп, являющихся списками почтовых адресов, а также сами такие профили и группы свободно транслируются между базами **cmsdb** с управляющего сервера на подчиненный, так как они не зависят от Active Directory. Если управляющий и подчиненный почтовый серверы подключены к одному серверу глобального каталога GC (Global Catalog) Active Directory, при создании группы Active Directory в административной консоли **Dr.Web Administrator Web Console** на управляющем сервере, ее настройки также будут переданы на подчиненный. Однако, если объединяемые в кластер почтовые серверы не имеют общего глобального каталога, порядок создания групп AD с общим управлением настройками будет отличаться:

1. На подчиненном сервере в консоли управления Active Directory создайте новую группу распределения (Distribution).
2. С помощью консоли **Dr.Web Administrator Web Console** добавьте созданную группу в список групп приложения.
3. В консоли **Dr.Web CMS Web Console** найдите эту группу в ветке настроек **DrWebScanSrv_1.0** -> **Application Settings** ->**Groups** -> *<имя группы>*. Для переменной **ItemList**, которая задает идентификатор GUID созданной группы AD, поменяйте значение атрибута с **Shared** на **Default**.
4. В консоли управления Active Directory управляющего сервера создайте новую группу распределения (Distribution) с тем же именем, что и на подчиненном сервере.
5. С помощью административной консоли **Dr.Web Administrator Web Console** добавьте созданную группу в список групп управляющего сервера, указав для нее то же имя.
6. Группы будут сопоставлены по имени (несмотря на разные идентификаторы GUID и разные наборы пользователей), и дальнейшее назначение профилей и всех настроек сканирования и фильтрации может осуществляться с помощью административной консоли **Dr.Web Administrator Web Console** управляющего сервера и будет транслироваться сразу на оба сервера.

9.4. Выбор типов поврежденных объектов

В некоторых случаях вложения могут рассматриваться как *поврежденные*. Такие объекты не могут быть проверены на вирусы. Для поврежденных объектов применяются те же действия, что и для зараженных объектов. Чтобы определить, какие объекты будут рассматриваться как поврежденные, выполните следующие действия:

1. В дереве хостов и групп выберите группу **DrWebScanSrv_1.0** -> **Application Settings** -> **Profiles** -> **%Profile name%** -> **Scanner**.
2. Выберите переменную, которая соответствует типу объектов:
   - **ScannerTreatPswrdArchivesAsBad**. Архивы с паролем.
     Эта настройка доступна из консоли **Dr.Web Administrator Web Console**. Подробнее в разделе Сканирование.
   - **ScannerTreatIncompleteArchivesAsBad**. Неполные архивы.

- **ScannerTreatPackedArchivesAsBad**. Архивы, при запаковке которых произошла ошибка.
- **ScannerTreatRestrictedArchivesAsBad**. Архивы, доступ к которым ограничен.
- **ScannerTreatDeepArchivesAsBad**. Архивы с большим уровнем вложенности.
- **ScannerTreatBigArchivesAsBad**. Архивы слишком большого размера.

3. Для выбранной переменной в поле **Value** установите значение:

   true – объекты этого типа будут рассматриваться как поврежденные, к ним будет применено действие, выбранное для зараженных объектов в разделе Сканирование.

   false – объекты этого типа будут рассматриваться как чистые и будут проигнорированы.

9.5. Фильтрация файлов в архиве по их расширениям

Если вам необходимо отслеживать архивы, содержащие файлы с определенными расширениями, и применять к этим архивам действия, установленные для подозрительных объектов, вы можете использовать переменную **SuspiciousTypesInsideContainer**:

1. В дереве хостов и групп выберите группу **DrWebScanSrv_1.0** -> **Application Settings**.
2. Установите в качестве значения для переменной **SuspiciousTypesInsideContainer** расширения файлов в следующем формате: `exe;vbs;scr`.

В первую очередь архив будет проверен на наличие зараженных файлов. Если они будут найдены, к архиву будет применено действие, выбранное для зараженных объектов, иначе архив будет проверен на наличие файлов с указанными расширениями. Если будет обнаружен хотя бы один файл с таким расширением, к архиву будет применено действие, установленное для подозрительных объектов.

10. Регистрация событий

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

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

Информация об обновлениях заносится в отдельный текстовый журнал **dwupdater.log** (см. главу Проверка модуля обновления), расположенный в каталоге:

- **%ALLUSERSPROFILE%\Application Data\Doctor Web\Logs** при работе с Windows Server 2003;
- **%PROGRAMDATA%\Doctor Web\Logs** при работе с Windows Server 2008.

10.1. Журнал операционной системы

В журнал регистрации операционной системы (Event Log) заносится следующая информация:

- сообщения о запуске и остановке программы;
- параметры лицензионного ключевого файла: действительность или недействительность лицензии, срок действия лицензии;
- 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 и спаме (см. раздел Уведомления). Сюда относятся следующие типы событий, о которых вы можете настроить уведомления:
  - **Отфильтрованные сообщения** – уведомления о фильтрации сообщений;
  - **Отфильтрованные файлы** – уведомления о фильтрации вложений;
  - **Зараженные** – уведомления об обнаруженных вирусных угрозах;
  - **Спам** – уведомления о спаме;
  - **Зараженные** – уведомления о фильтрации зараженных объектов;
  - **Обновление** – уведомления о последнем обновлении;
  - **Устаревшие базы** – уведомления о необходимости обновить вирусные базы;
  - **Офисный контроль** – уведомления о фильтрации сетевых ресурсов с помощью **Офисного контроля**.

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 **Doctor Web**. Откроется список событий, зарегистрированных в журнале пользовательскими приложениями. Источниками сообщений Dr.Web являются приложения **Dr.Web Scanning Engine**, **Dr.Web CMS**, **Dr.Web CMS Web Console**, **Dr.Web for MSP Scanning Service**, **Dr.Web for MSP Component Host** и **Dr.Web for MSP Requests Queue**.

Перенаправление событий Dr.Web

Чтобы перенаправить события Dr.Web в определенный журнал событий операционной системы:

1. В Веб-консоли Dr.Web CMS Web Console выберите группу **DrWebScanSrv_1.0** -> **Application Settings**.
2. В качестве значения переменной **EventLog** задайте имя журнала, в который будут перенаправляться события Dr.Web, например, **Doctor Web**.

   

   Если переменная **EventLog** отсутствует или ее значение не задано, события Dr.Web записываются в журнал Doctor Web.

3. Перезапустите службу Dr.Web for MSP Scanning Service.
4. Удалите источник событий **Dr.Web CMS for MSP** из раздела реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Doctor Web\Dr.Web for Microsoft Server Products`.
5. Перезагрузите операционную систему.

10.2. 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 **isa-tmg-setup.log** создается в каталоге:

- **%ALLUSERSPROFILE%\Application Data\Doctor Web\Logs** при работе с Windows Server 2003;
- **%PROGRAMDATA%\Doctor Web\Logs** при работе с Windows Server 2008.

10.3. Журнал событий Dr.Web

Список событий сохраняется управляющим сервисом Dr.Web CMS в базу данных **cmstracedb**, которая находится в папке установки **%ProgramFiles%\DrWeb CMS for MSP**.

Управляющий сервис регистрирует различные типы событий и позволяет выбрать степень детализации для каждого приложения-подписчика службы Dr.Web CMS.

Максимальный размер базы данных составляет 500 Мбайт. При достижении этого значения действующая база архивируется в папке установки приложения, в имени файла указывается отметка времени (timestamp). После этого создается новый файл для базы данных.

При необходимости, вы можете удалить базу данных **cmstracedb**.

10.3.1. Типы регистрируемых событий

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.

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.

10.3.2. Степень детализации

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 консоли **Dr.Web CMS Web Console**, 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 консоли **Dr.Web CMS Web Console**, 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.

10.3.3. Удаление базы данных cmstracedb

При необходимости вы можете удалить базу данных **cmstracedb**, находящуюся в папке установки приложения **%PROGRAMFILES%\DrWeb CMS for MSP**:

1. Запустите командную консоль (cmd) от имени администратора.
2. Остановите службы приложения в указанном порядке:

```
net stop "Dr.Web SSM"
net stop "Dr.Web for MSP Scanning Service"
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"
```

3. Удалите файл **cmstracedb**, находящийся в папке установки приложения **%PROGRAMFILES%\DrWeb for CMS for MSP**.
4. Запустите службы приложения в указанном порядке:

   `net start "Dr.Web CMS"` (необходимо дождаться запуска данной службы для продолжения)

   `net start "Dr.Web SSM"`
5. После запуска службы Dr.Web SSM убедитесь, что с ее помощью были запущены остальные службы приложения.

11. Диагностика

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

- проверка установки приложения;
- проверка модуля обновления;
- проверка детектирования вирусов;
- проверка детектирования спама.

11.1. Проверка установки

Dr.Web должен быть установлен в следующие папки:

Для Microsoft ISA Server:

- %ALLUSERSPROFILE%\Application Data\Doctor Web;
- %PROGRAMFILES%\Common Files\Doctor Web;
- %PROGRAMFILES%\DrWeb CMS for MSP;
- %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG.

Для Microsoft Forefront TMG:

- %PROGRAMDATA%\Doctor Web;
- %PROGRAMFILES%\DrWeb CMS for MSP;
- %PROGRAMFILES%\Common Files\Doctor Web;
- %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG

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 Dr.Web.

Наконец, убедитесь, что запущены следующие локальные сервисы:

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

11.2. Проверка модуля обновления

Модуль обновления **drwupsrv.exe** автоматически запускается после установки Dr.Web. Он загружает последние версии антивирусного ядра **drweb32.dll**, вирусных баз и других составляющих, кроме компонентов приложения.

Чтобы убедиться, что обновление прошло успешно:

1. В зависимости от версии операционной системы выполните команду **Tasks**, чтобы открыть папку **%WINDIR%\Tasks** или откройте **Планировщик заданий Windows**.
2. Проверьте наличие задания Dr.Web 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\dwupdater.log** при работе в Windows Server 2003 или **%PROGRAMDATA%\Doctor Web\Logs\dwupdater.log** при работе в Windows Server 2008 и убедитесь, что в нем не зафиксировано ошибок.

11.3. Проверка детектирования вирусов

Для проверки конфигурации и способности Dr.Web 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 из раздела **Download Anti-Malware Testfile** веб-сайта EICAR по адресу http://www.eicar.org или создать его самостоятельно.

Проверка детектирования вирусов при помощи тестового файла EICAR

1. Создайте файл:
   - откройте Блокнот;
   - скопируйте в него следующую строку:
     ```
     X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
     ```
2. Сохраните файл с расширением **.com**. Вы можете использовать любое имя, например, eicar.com.
3. Прикрепите созданный файл к электронному письму и отправьте на любой тестовый адрес.

   Полученное на этот адрес письмо должно содержать текстовый файл с суффиксом **_infected.txt** и следующим содержанием:

```
Инфицированный вирусом файл eicar.com был удален Dr.Web для
Microsoft ISA Server и Forefront TMG. Имя вируса: EICAR
Test File (NOT a Virus!).
```

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

11.4. Проверка детектирования спама

Компонент **Антиспам** доступен только в версии «Антивирус + Антиспам», т.е. в том случае, если у вас есть соответствующий ключевой файл (см. Лицензионный ключевой файл).

Для проверки способности компонента **Антиспам** обнаруживать спам рекомендуется использовать письма со специальной тестовой строкой: GTUBE (Generic Test for Unsolicited Bulk Email) либо со строкой для встроенной проверки.

Чтобы создать тестовое письмо GTUBE:

1. В теме письма укажите: **Test spam mail**.
2. Скопируйте следующую строку в тело нового электронного письма:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Тестовое письмо не должно содержать никаких вложений, подписей или другой информации, кроме темы письма и тестовой строки.

3. Отправьте письмо по протоколу SMTP на любой тестовый адрес.
4. Откройте стандартную утилиту Windows **Просмотр событий** -> **Doctor Web** (**Event Viewer** -> **Doctor Web**) и найдите сообщение о том, что Dr.Web обнаружил спам.

Чтобы создать тестовое письмо для встроенной проверки:

1. В теме письма укажите: **Vade Secure**.
2. Скопируйте следующую строку в тело нового электронного письма:

```
tiUS4kVZrTfBBZXZPuLrnstNpdo8vJ-Spam-high-PQQMbQu22jePzuV8TLwVdPo81QpGXNJxRI
```

Тестовое письмо не должно содержать никаких вложений, подписей или другой информации, кроме темы письма и тестовой строки.

3. Отправьте письмо по протоколу SMTP на любой тестовый адрес.
4. Откройте стандартную утилиту Windows **Просмотр событий** -> **Doctor Web** (**Event Viewer** -> **Doctor Web**) и найдите сообщение о том, что Dr.Web обнаружил спам.

12. Приложения

12.1. Приложение A. Удаление Dr.Web вручную

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

1. Остановите сервис межсетевого экрана Microsoft ISA Server или Microsoft Forefront TMG.
2. Запустите командную консоль (**cmd**) от имени администратора.
3. Удалите регистрацию фильтров:

- в случае использования Microsoft ISA Server:

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\FTPFilter.dll"

regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\POP3Filter.dll"

regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\SMTPFilter.dll"

regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\HTTPWebFilter.dll"
```

- в случае использования Microsoft Forefront TMG:

```
regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\FTPFilter.dll"

regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\POP3Filter.dll"

regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\SMTPFilter.dll"

regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\HTTPWebFilter.dll"
```

4. Остановите службы приложения в указанном порядке:

```
net stop "Dr.Web SSM"

net stop "Dr.Web for MSP Scanning Service"

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"
```

5. Удалите службы приложения:

```
sc delete "Dr.Web SSM"

sc delete "Dr.Web for MSP Scanning Service"

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 "%ALLUSERSPROFILE%\Application Data\Doctor Web"
rd /S /Q "%PROGRAMFILES%\DrWeb CMS for MSP"
rd /S /Q "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG"
```

- в случае использования Microsoft Forefront TMG:

```
rd /S /Q "%PROGRAMDATA%\Doctor Web"
rd /S /Q "%PROGRAMFILES%\DrWeb CMS for MSP"
rd /S /Q "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway
\DrWeb for ISA and TMG"
```

12.2. 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.

12.2.1. 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
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.

Физически база данных представляет собой файл cmsdb, который находится в каталоге установки продукта (%PROGRAMFILES%\DrWeb CMS for MSP\).

12.2.2. 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.

12.2.3. Подключение к серверам

Консоль Dr.Web CMS Web Console позволяет подключаться к другим серверам, на которых функционирует CMS. Для подключения выполните следующие действия:

1. Щелкните правой кнопкой мыши по значку хоста в дереве консоли и выберите пункт **Add host**.
2. В открывшемся окне введите адрес хоста, к которому производится подключение, и нажмите **OK**.
3. Введите имя пользователя и пароль для подключения к выбранному хосту. При вводе корректных данных будет произведено подключение, и в дереве консоли будет отображен новый хост.

Описанным выше способом можно подключаться с неограниченному количеству машин и управлять ими. Настройки каждого подключения сохраняются в отдельной группе в консоли **Dr.Web CMS Web Console** по пути /**Dr.Web CMS Web Console_1.0/Application Settings/Hosts**. Каждый добавленный хост представлен в виде группы с именем подключения, внутри такой группы создаются три переменные:

- **Address** содержит адрес подключения к хосту;
- **Login** содержит имя пользователя;
- **Password** содержит пароль для подключения к хосту.

Настройки подключения к каждому из добавленных хостов сервер консоли Dr.Web CMS Web Console сохраняет в своей группе в CMS по пути /**Dr.Web CMS Web Console_1.0/ Application Settings/Hosts**.

Каждый добавленный хост представлен в виде группы с именем в виде адреса подключения к добавленному хосту. Внутри группы создаются три переменные: **Address**, **Login** и **Passsword**. Переменная **Address** содержит адрес подключения к хосту. Переменная Login содержит имя пользователя для подключения. Переменная **Password** содержит пароль для подключения к хосту.

В случае изменения данных аутентификации на подключаемом хосте консоли Dr.Web CMS Web Console может быть запрещен доступ на этот хост. В этом случае требуется корректировка настроек подключения консоли Dr.Web CMS Web Console к этому хосту.

При следующем открытии консоль Dr.Web CMS Web Console автоматически подключится к добавленным хостам. Для удаления добавленного хоста следует удалить группу с

настройками подключения к данному хосту их группы настроек консоли по пути **/Dr.Web CMS Web Console_1.0/Application Settings/Hosts**.

При помощи консоли Dr.Web CMS Web Console можно так же создавать кластеры, которые позволяют задавать настройки для всех объединенных хостов.

12.3. Приложение B. Настройка параметров обновления

Для настройки обновления вирусных баз и компонентов Dr.Web доступен файл **drwupsrv.bat**. Данный файл находится в папке с установленным Dr.Web. Команды, прописанные в файле, выполняются при запуске задания **Doctor Web for MSP Update Task** в планировщике заданий Windows.

Чтобы установить настройки обновления, укажите необходимые параметры для команд **- c update** и **- c postupdate**.

Параметры команды - c update

Команда **- c update** выполняет обновление вирусных баз и компонентов Dr.Web.

Параметр	Описание
--type arg	**Пожалуйста, не меняйте этот параметр**. Тип обновления: • update-revision - обновление компонентов в пределах текущей ревизии.
--disable-postupdate	**Пожалуйста, не меняйте этот параметр**. Последующее обновление выполняться не будет. Работа модуля обновления будет завершена после выполнения обновления.
--verbosity arg	Уровень детализации журнала: • error - стандартный; • info - расширенный; • debug - отладочный.
--interactive	Если параметр указан, при выполнении некоторых команд будет задействовано большее количество ресурсов.
--param args	**Пожалуйста, не меняйте этот параметр**. Дополнительные параметры, передаваемые для скрипта. Формат: <имя>=<значение>.

Параметр	Описание
-n [--component] arg	Перечень компонентов, которые необходимо обновить: • updater - файл drwupsrv.exe; • antispam - файл vrcpp.dll; • scan-engine - файлы dwengine.exe, dwsewsc.exe, dwinctl.dll, dwarkdaemon.exe, arkdb.bin, dwqrui.exe, dwarkapi.dll; • av-engine - вирусные базы (файлы с расширением *.vdb); • isa-and-tmg-setup - файл isa-and-tmg-setup.exe.  Одновременно можно обновлять несколько элементов, например: `-n av-engine updater`
-g [--proxy] agr	Прокси-сервер для обновления в формате <адрес>: <порт>.
-u [--user] agr	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.

Пример команды - с update для обновления вирусных баз через прокси-сервер:

```
-c update --type=update-revision --disable-postupdate --verbosity=debug
--interactive --param="<plugin_name>" -n av-engine --
proxy=192.168.134.128:808 --user=qwerty --password=qwerty
```

Параметры команды - с postupdate

Команда - **с postupdate** выполняет последующее обновление вирусных баз и компонентов Dr.Web.

Параметр	Описание
--verbosity arg	Уровень детализации журнала: • error - стандартный; • info - расширенный; • debug - отладочный.
--interactive	Если параметр указан, при выполнении некоторых команд будет задействовано большее количество ресурсов.
--param arg	Дополнительные параметры, передаваемые для скрипта. Формат: <имя>=<значение>.

Пример команды - **с postupdate**:

```
-c postupdate --verbosity=debug --interactive --param="<plugin_name>"
```

Создание зеркала обновлений

Если у вас нет возможности обновлять Dr.Web через Интернет или вы хотите сократить объем внешнего трафика, вы можете создать зеркало, чтобы выполнять обновление продуктов «Доктор Веб» по локальной сети.

Для создания зеркала обновлений выполните следующие действия на сервере с доступом в Интернет:

1. Запустите файл **drwupsrv.exe** со следующими параметрами:

```
-c download --zones=<file_path> --key-dir=<folder_path> --repodir=<folder_path>
--version=90 --verbosity=debug --log-dir=C:\Repo
```

Укажите необходимые значения параметров:

zones=<file_path> — путь к файлу зоны обновлений **drwzones.xml**;

key-dir=<folder_path> — путь к папке с лицензионным ключевым файлом;

repo-dir=<folder_path> — путь к папке с обновлениями. Обратите внимание, что к папке должен быть настроен общий доступ.

Например:

```
drwupsrv.exe -c download --zones=C:\Mirror\drwzones.xml --key-dir=C:
\Mirror\ --repodir=C:\Mirror\Repo\ --version=90 --verbosity=debug --
log-dir=C:\Mirror\Repo\
```

2. На сервере с установленным Dr.Web откройте файл **drwupsrv.bat**, в строке `set upparams` добавьте следующий параметр и запустите файл:

```
--zone="file://<repo_folder_path>"
```

Например:

```
set upparams=-c update --type=update-revision --disable-postupdate --
verbosity=debug --interactive --param="plugin=<plugin_name>" --
zone="file://<repo_folder_path>"
```

Предметный указатель

D

Dr.Web 8
- Dr.Web Administrator Web Console 25
- Dr.Web CMS Web Console 55
- Dr.Web FTP Filter 16
- Dr.Web HTTP Web Filter 19
- Dr.Web POP3 Filter 17
- Dr.Web SMTP Filter 17
- администрирование 25
- группы 40
- диагностика 67
- компоненты 12
- консоль CMS 55, 57, 57, 58
- лицензия 10
- назначение 8
- обновление 53
- проверяемые объекты 9
- профили 27
- регистрация событий 62
- системные требования 21
- службы 20
- статистика работы 44
- удаление 21, 24
- удаление вручную 70
- установка 21, 23
- фильтры 12, 12, 16, 17, 17, 19
- функции 8

Dr.Web Administrator Web Console 25, 28, 30, 32, 34, 43, 44, 46, 48
- группы 26
- профили 26

Dr.Web CMS Web Console
- добавление администратора 57
- пароль администратора 57

Dr.Web FTP Filter 16

Dr.Web HTTP Web Filter 19

Dr.Web POP3 Filter 17

Dr.Web SMTP Filter 17

E

event log 62

A

администрирование
- веб-консоль 25
- группы 26, 40
- консоль CMS 55
- профили 26, 27

антивирусные фильтры 12

антиспам
- лицензия 30
- настройка 30

Б

база данных CMS 71

белый список адресов 32

В

веб-консоль CMS 55
- создание кластеров 58

веб-консоль администрирования 25, 28, 30, 32, 34, 43, 44, 46, 48

вирусные базы 53

вирусные события 46
- журнал событий 20
- мониторинг 20
- статистика 20, 44
- уведомления 20

Г

группы 26, 40
- создание 40
- типы 41
- формирование 41

Д

диагностика 67, 68, 69

добавление администратора 57

Ж

журнал отладки 64

журнал программы установки 63

журнал событий 20, 43
- журнал программы установки 63
- журнал событий Dr.Web 64
- операционной системы 62

З

зеркало обновлений 76

К

карантин 20, 48
- действия 48, 51

Предметный указатель

карантин 20, 48
- менеджер карантина 49, 51, 52
- настройка 48
- настройка свойств 52
- управление 51

ключевой файл
- действительность 10
- обновление 11
- получение 10, 11

консоль CMS
- добавление администратора 57
- пароль администратора 57

Л

лицензия
- антиспам 30
- действительность 10
- ключевой файл 10, 10
- обновление 11
- получение 10

М

менеджер карантина 49, 51, 52
модуль обновления 53, 74
- проверка 68

Н

настройка
- антиспама 30
- карантина 48
- офисного контроля 32
- сканирования 28
- уведомлений 43
- фильтрации 34

О

обновление
- вирусные базы 53
- диагностика 68
- лицензии 11
- модуль обновления 68
- параметры командной строки 74

офисный контроль
- настройка 32
- списки адресов 32

П

пароль администратора 57
платформа CMS 71
- база данных 71
- статистика приложений 72

получение ключевого файла 10
почтовые уведомления 20
правила фильтрации 34
проверка
- детектирования вирусов 68
- детектирования спама 69
- модуля обновления 68
- работоспособности 67
- установки 67
- фильтры 16, 17, 19

проверяемые объекты 9
программа установки
- регистрация событий 63
- установка программы 23

просмотр статистики 44
профили 26, 27
- настройка 27
- приоритет 28
- создание 27

Р

регистрация событий 62, 64
- журнал операционной системы 62
- журнал программы установки 63

С

сервисы 20
системные требования 21
сканирование
- действия 28
- настройка 28

службы 20
- Dr.Web CSM 55

события 46
- мониторинг 20
- статистика 44

создание кластеров 58
сокращения 6
статистика 20
- приложений 72

Предметный указатель

статистика 20
  просмотр 44
  события 44

Т

тестовое письмо GTUBE 69
тестовый файл EICAR 68
требования 21

У

уведомления
  журнал событий 43
  настройка 43
  типы 43
уведомления по почте 20
удаление Dr.Web 21, 24
условные обозначения 6
установка Dr.Web 21, 21
  проверка 67
  программа установки 23
  установочный файл 23
установочный файл 23

Ф

фильтрация
  правила 34
фильтры
  веб-фильтр 17
  приложений 12
  проверка 16, 17, 19

Ч

черный список адресов 32

Э

эвристический анализатор 28