Dr.WEB
для Microsoft Exchange Server

Руководство администратора

Жасағаның
دافع عن إبداعاتك
Защити созданное
Defend what you create
Protégez votre univers
Verteidige, was du erschaffen hast
Захисти створене
保护您创建的一切
Защити созданное
Proteggi ciò che crei
Защити созданное
Жасағанының қорға
Verteidige, was du erschaffen hast
Proteggi ciò che crei
Захисти створене
Defend what you create
脅威からの保護を提供します
Protégez votre univers
Proteggi ciò che crei
Захисти створене
دافع عن إبداعاتك
脅威からの保護を提供します
Defend what you create
Жасағанының қорға
دافع عن إبداعاتك
دافع عن إبداعاتك
Protégez votre univers
保护您创建的一切
Защити созданное
脅威からの保護を提供します
Захисти створене
Verteidige, was du erschaffen hast

Dr.Web для Microsoft Exchange Server
Версия 11.0
Руководство администратора
12.10.2017

«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

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. Введение

Благодарим вас за приобретение Dr.Web для Microsoft Exchange Server (далее – Dr.Web). Он надежную защищает компьютеры и информацию внутри корпоративной сети от угроз, распространяемых посредством электронной почты.

Настоящее 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.

2.1. Назначение Dr.Web

Dr.Web – это антивирусное приложение, созданное с целью защитить корпоративную почтовую систему от вирусов и спама. Оно надежно интегрируется в систему и проверяет все письма и вложения, поступающие серверу для обработки. Все сообщения проверяются до того, как они передаются клиенту.

Dr.Web может выполнять следующие функции:

- сканирование всех входящих и исходящих сообщений в реальном времени;
- фильтрация и блокировка спама, а также создание белых и черных списков адресов;
- изоляция инфицированных и подозрительных объектов в карантине;
- фильтрация электронных писем по различным критериям;
- распределение пользователей по группам для упрощения администрирования;
- отправка уведомлений о вирусных событиях в журнал событий операционной системы и ведение внутренней базы событий cmstracedb;
- сбор статистики;
- поддержка единых настроек приложения на распределенной системе почтовых серверов, в том числе, объединенных в кластер;
- автоматическое обновление вирусных баз и компонентов программы.

Для упрощения работы с приложением были реализованы полностью автоматический запуск (при запуске системы) и удобный механизм обновлений посредством добавления задания на обновление в расписание Планировщика Задач Windows.

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.

Приложение функционирует на платформе Dr.Web CMS (Central Management Service), поддерживающей централизованное управление настройками приложения и его

компонентов с возможностью удаленного администрирования через браузер по защищенному протоколу HTTPS. Платформа Dr.Web CMS имеет встроенный веб-сервер Dr.Web CMS Web Console с аутентификацией клиента, что обеспечивает доступ к управлению приложением только авторизованным администраторам.

В рамках платформы интерфейсы взаимодействия и управления компонентами приложения реализованы посредством внутренних служебных протоколов, работающих поверх TCP. Упомянутые служебные протоколы позволяют управляющему сервису Dr.Web CMS выполнять его основную задачу: предоставлять компонентам приложения канал связи с управляющей базой данных cmsdb и базой событий приложения cmstracedb, находящихся в папке установки приложения и реализованных встраиваемой реляционной базой SQLite.

Взаимодействие компонентов приложения с платформой Dr.Web CMS осуществляются следующим образом:

1. Компонент приложения при запуске (если компонент является сервисом) или загрузке (если компонент является библиотекой) подключаются к сервису Dr.Web CMS посредством служебного протокола поверх TCP.
2. Dr.Web CMS регистрирует подключение приложения и создает в базе cmsdb структуру данных, отвечающих подключившемуся компоненту приложения.
3. Dr.Web CMS контролирует работу компонента приложения, отслеживая состояние TCP-сессии и обмен служебными сообщениями с компонентом приложения.
4. В случае изменения состояния компонента приложения Dr.Web CMS изменяет переменные в базе cmsdb, отражающие состояние приложения.

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

2.2. Проверяемые объекты

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.

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

2.3. 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. Лицензирование

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

3.1. 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.

3.2. 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.

Если на компьютере установлен Dr.Web Agent, при установке Dr.Web можно выбрать вариант получения ключевого файла с сервера централизованной защиты.

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 http://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/.

3.3. 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, добавьте новый ключевой файл в папке установки программы.
2. Перезапустите службу **Dr.Web for MSP Scanning Service**.

3. 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/.

4. Принципы работы Dr.Web

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

Антивирусное и антиспам-решение Dr.Web интегрирует технологии Dr.Web в процесс обработки и хранения почты на серверах Exchange.

Продукт имеет удобный графический интерфейс пользователя для управления настройками сканирования и отслеживания результатов проверки сообщений на сервере.

4.1. Этапы проверки на вирусы и спам

После получения уведомления о приходе сообщения на сервер поступившее сообщение проходит через следующие этапы проверки:

1. **Применение правил фильтрации** (настраиваются в разделе Фильтрация).
   - Правила антидистрибуции (ограничение списков рассылки). Можно задать правила, задающие максимальное число адресов получателей сообщения (или сообщения с вложениями) и применяющиеся к адресатам-отправителям. Для этих отправителей допускается отправка только тех сообщений, в которых число адресов получателей не превышает указанного максимального значения.
   - Правила фильтрации вложенных файлов. Можно задать правила удаления вложенных файлов: по расширению, по маске имени файла, по максимальному размеру файла.

   При условии выполнения одного из заданных правил сообщение (или вложение) удаляется и об этом оповещается администратор или другие заинтересованные лица (при наличии соответствующих настроек в разделе Уведомления). В случае удаления вложенного файла к письму прикрепляется текстовый файл с сообщением об удалении приложения. Шаблон сообщения об удалении вложения и имя файла такого сообщения задаются также в разделе Фильтрация.
2. **Проверка на спам** (выполняется только в случае лицензии «Антивирус + Антиспам» и только для писем принимаемых сервером по протоколу SMTP, настраивается в разделе Антиспам).

   В первую очередь анализируются адреса получателей и отправителей на принадлежность черным и белым спискам, которые задаются в разделе Антиспам. Затем антиспам-фильтр Vade Retro проверяет текст сообщения и выдает заключение, на основе которого определяется степень вероятности того, что данное сообщение является спамом. Если письмо является спамом, то об этом оповещается администратор или другие заинтересованные лица, прописанные в соответствующих

настройках раздела Уведомления, и к письму применяется действие, установленное администратором для данной категории спама в разделе Антиспам.

3. **Проверка на вирусы** (настраивается в разделе Сканирование).

   Сообщения, успешно прошедшие предыдущие этапы проверки (или пропущенные в соответствии с настройками приложения Dr.Web), передаются далее для проверки на наличие вредоносного кода. Если объект (вложение или тело письма) содержит вредоносный код, антивирус предпринимает попытку вылечить объект. Если в настройках включено использование эвристического анализатора, становится возможным определение объектов, содержащих модифицированный или неизвестный вредоносный код, таким объектам присваивается категория **Подозрительные**.

   По результатам сканирования объектам присваиваются определенные статусы (например, **Невылеченные**, **Подозрительные**, **Поврежденные**, **Вылеченные**), и на основе такого заключения выполняются дальнейшие действия над этими объектами. К письмам с зараженными объектами прикрепляется текстовый файл с сообщением об обнаруженной инфекции и выполненными над этими объектами действиями программы.

   Вылеченные и незараженные объекты передаются серверу с соответствующей пометкой. Невылеченные, поврежденные и подозрительные объекты проходят обработку в соответствии с настройками, указанными в разделе Сканирование.

   Администратор может получать оповещения о всех типах вирусных событий при наличии соответствующих настроек в разделе Уведомления.

4.2. Карантин

Для невылеченных, поврежденных и подозрительных объектов можно установить действие **Поместить 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.

4.3. Мониторинг вирусных событий

Для предоставления администратору, а также другим заинтересованным пользователям структурированной информации о событиях, отслеживаемых Dr.Web, администратору необходимо настроить систему оповещения о событиях, которая включает в себя следующие возможности:

- Журнал событий. Возможно занесение в журнал событий записей о приходе на сервер писем с объектами, которые были вылечены, не вылечены, отфильтрованы или определены как поврежденные или спам (устанавливается на выбор). Просмотр этих событий осуществляется с помощью стандартной утилиты Windows **Просмотр Событий** -> **Приложение** (**Event Viewer** -> **Application**);

- Статистика. Предоставляется возможность ознакомиться с информацией о количестве проверенных объектов с момента установки Dr.Web, либо с момента очистки данных статистики;
- События. Возможен просмотр списка писем, обработанных Dr.Web, в которых обнаружены вирусы или спам, а также отфильтрованных писем.

5. Установка и удаление

Dr.Web поставляется в виде папки, помещенной в ZIP-архив и содержащей установочные файлы **drweb-[version]-av-exchange-windows-x64.exe** и **drweb-[version]-av-exchange-windows-x86.exe**, где **[version]** - номер текущей версии Dr.Web.

Извлеките файл установки на локальный диск компьютера, на котором установлен Microsoft Exchange Server.

Для установки и удаления Dr.Web пользователь должен обладать правами локального администратора на том компьютере, где установлен Microsoft Exchange Server, а также входить в группу Domain Users.

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

5.1. Системные требования

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

Характеристика	Требование
RAM	Не менее 512 Мбайт
Свободное пространство на диске	Не менее 1 Гбайт

ОС	**32-разрядные ОС**
	Для Microsoft Exchange Server 2003:
	• Microsoft® Windows Server® 2003x86 с установленными:
	  ▫ MSXML 4.0 Service Pack 3 (Microsoft XML Core Services);
	  ▫ SP1 или выше.

	64-разрядные ОС Для Microsoft Exchange Server 2007/2010: • Microsoft® Windows Server® 2008 x64; • Microsoft® Windows Server® 2008 R2. Для Microsoft Exchange Server 2013: • Microsoft® Windows Server® 2008 R2; • Microsoft® Windows Server® 2012;

Характеристика	Требование

	• Microsoft® Windows Server® 2012 R2:
	  ▫ Требуется SP1 (или более поздней версии) для Exchange Server 2013.
	Для Microsoft Exchange Server 2016:
	• Microsoft® Windows Server® 2012;
	• Microsoft® Windows Server® 2012 R2;
	• Microsoft® Windows Server® 2016:
	  ▫ Для Exchange Server 2016 требуется Cumulative Update 3 (или более поздняя версия).

Версия Microsoft Exchange Server	• Microsoft® Exchange Server 2003; • Microsoft® Exchange Server 2007 x64 с установленным SP1; • Microsoft® Exchange Server 2010 x64; • Microsoft® Exchange Server 2013; • Microsoft® Exchange Server 2013 с установленным SP1 (дополнительно требуется установка Cumulative Update 5 или запуск скрипта Exchange2013-KB2938053-Fixit); • Microsoft® Exchange Server 2016.

5.2. Совместимость

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

1. Dr.Web для Microsoft Exchange Server версии 11.0 совместим только с продуктами Dr.Web версии 11.
2. Dr.Web для Microsoft Exchange Server 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.
3. Dr.Web для Microsoft Exchange Server версии 11 не совместим с Dr.Web для Microsoft ISA Server и Forefront TMG версии 11.

Для корректной работы сервера Microsoft Exchange при включенном компоненте SpIDer Guard рекомендуется исключить из проверки SpIDer Guard папки и процессы Microsoft Exchange Server (список рекомендуемых исключений можно найти в документации Microsoft).

5.3. 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.

Если вы используете Microsoft Exchange Server 2013 с установленным пакетом обновлений SP1, но не устанавливали Cumulative Update 5, рекомендуется перед установкой программы запустить скрипт **Exchange2013-KB2938053-Fixit**, доступный на сайте компании Microsoft по ссылке http://support.microsoft.com/kb/2938053, во избежание ошибок при регистрации транспортных агентов во время установки.

Чтобы установить Dr.Web:

1. Запустите установочный файл программы **drweb-[version]-av-exchange-windows-x64.exe**, если вы используете Microsoft Exchange Server 2007/2010/2013/2016 или **drweb-[version]-av-exchange-windows-x86.exe** для более ранних версий сервера Exchange. Откроется окно **Мастера установки**.
2. Для продолжения установки необходимо прочитать и принять условия Лицензионного соглашения, выбрав пункт **Я принимаю условия лицензионного соглашения**.

   Нажмите **Далее**.
3. Остановите службу Microsoft Exchange Transport (при использовании Microsoft Exchange Server 2007/2010/2013/2016).

   Для этого щелкните по ссылке **Открыть список сервисов**, далее щелкните правой кнопкой мыши по названию службы в списке и выберите **Остановить**. После остановки службы нажмите **Далее**.

Остановка службы Microsoft Exchange Transport вручную связана с необходимостью избежать нарушения целостности установки на сервере, работающем под нагрузкой.

В некоторых случаях остановка службы Microsoft Exchange Transport может занять продолжительное время!

4. Выберите вариант лицензирования. Вы можете зарегистрировать лицензию после установки, указать путь к действующему ключевому файлу или использовать ключевой файл с сервера централизованной защиты, если на компьютере установлен Dr.Web Agent. Нажмите **Далее**.

Для корректной работы приложения необходимо указать путь к лицензионному ключевому файлу drweb32.key.

Для регистрации лицензии после установки или при ее обновлении достаточно поместить действующий лицензионный ключевой файл в папку установки программы и перезапустить службу Dr.Web for MSP Scanning Service.

5. Перед началом установки щелкните по ссылке **Параметры установки**, чтобы настроить следующие параметры установки:

   - **Установить транспортные агенты** – позволяет установить транспортные агенты (по умолчанию данный параметр выбран). Для Microsoft Exchange Server 2007/2010/2013/2016 включение данной опции приведет к регистрации библиотеки DRWTransportAgent.dll и разрешению поставляемых библиотекой транспортных агентов (антивирусного и антиспама) в службе Microsoft Exchange Transport. Для Microsoft Exchange Server более ранних версий выбор данной опции приведет к регистрации библиотеки DrWebSink.dll и подключению агента антиспама в Microsoft Internet Information Services (IIS).
   - **Установить модуль VSAPI** – позволяет установить модуль DrWebVSAPI.dll для проверки посредством интерфейса антивирусного сканирования VSAPI (данный интерфейс не поддерживается Microsoft Exchange Server 2013), предоставляемого сервисом Microsoft Exchange Information Store. Если данный параметр выбран, вы можете дополнительно настроить режим проверки: включить сканирование исходящих сообщений, упреждающее и фоновое сканирование.

   Кроме того, вы можете включить мониторинг процесса установки и регистрации транспортных агентов, установив флажок **Контролировать процесс подключения транспортных агентов**. В процессе установки регистрация транспортных агентов для Microsoft Exchange Server 2007/2010/2013/2016 в системе SMTP-транспорта будет произведена посредством Exchange PowerShell. В этом случае консоль PowerShell не закроется автоматически, и для завершения установки потребуется ручной ввод команды `exit` для ее закрытия.

   Нажмите **OK**.

Во избежание ошибок при регистрации транспортных агентов во время установки рекомендуется убедиться, что на сервере Microsoft Exchange Server установлен скрипт RemoteExchange.ps1 (по умолчанию, находится в папке C:\Program Files\Microsoft \Exchange Server\V14\bin\ для Microsoft Exchange Server 2010 и в папке C:\Program Files \Microsoft\Exchange Server\V15\bin\ для Microsoft Exchange Server 2013).

6. При повторной установке приложения вам будет предложено использовать сохраненные перед его удалением настройки (если была выбрана соответствующая опция). Вы можете использовать сохраненную конфигурацию или удалить ее и настроить работу приложения заново после его установки. Нажмите **Далее**.

   Начнется установка Dr.Web на ваш компьютер. По умолчанию файлы программы помещаются в папки %Program Files%\DrWeb for Exchange и %Program Files%\Common

Files\Doctor Web. Журналы регистрации событий и вспомогательные компоненты приложения помещаются в папку %Program Data%\Doctor Web.

7. Если вы установили флажок Контролировать процесс подключения транспортных агентов при настройке параметров установки, вам потребуется завершить мониторинг после того, как транспортные агенты будут установлены и подключены. Сообщения «**Dr.Web AntiVirus Agent enabled**» и «**Dr.Web AntiSpam Agent enabled**» в консоли PowerShell указывают на успешное подключение агентов приложения к службе Microsoft Exchange Transport. В консоли PowerShell введите команду `exit`.
8. По завершении установки нажмите кнопку **Готово**.

В случае установки из файла **drweb-[version]-av-exchange-windows-x86.exe** вам будет предложено перезагрузить сервер. При установке из файла **drweb-[version]-av-exchange-windows-x64.exe** перезагрузка не требуется: служба Microsoft Exchange Transport будет запущена автоматически, и после ее запуска сервер придет в рабочее состояние. Однако, если на сервере запущены службы поддержки протоколов POP3 и IMAP4, перезагрузка Microsoft Exchange Transport может разорвать их соединение с транспортной системой сервера. В этом случае дождитесь окончательного запуска службы Microsoft Exchange Transport и служб установленного приложения, после чего перезапустите службы Microsoft Exchange POP3 или Microsoft Exchange IMAP4 вручную (или же перезагрузите сервер).

Чтобы переустановить Dr.Web:

1. Удалите Dr.Web.

Файл настроек приложения cmsdb не удаляется автоматически при удалении приложения. Таким образом, все пользовательские настройки сохраняются и могут быть использованы при повторной установке. Однако при установке новой версии приложения может оказаться, что набор настроек базовой конфигурации расширился или изменился. В результате использование сохраненного файла становится невозможным, поскольку может привести к сбоям в работе приложения.

Если вы хотите использовать сохраненные настройки приложения, обратитесь в техническую поддержку компании «Доктор Веб» для уточнения совместимости настроек платформы Dr.Web CMS разных версий приложения. Если в более поздней версии появились новые параметры, в общем случае достаточно добавить в существующую базу настроек недостающие переменные, правильно указав их тип и значения по умолчанию.

2. Удалите вручную файлы cmsdb и cmstracedb из папки %ProgramFiles%\DrWeb for Exchange.
3. Выполните установку Dr.Web, следуя описанным выше инструкциям.

5.4. Удаление Dr.Web

Чтобы удалить Dr.Web:

1. Запустите установочный файл программы **drweb-[version]-av-exchange-windows-x64.exe** или **drweb-[version]-av-exchange-windows-x86.exe** в зависимости от используемой версии Microsoft Exchange Server. Откроется окно **Мастера установки**.

   

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

2. Остановите службу Microsoft Exchange Transport (при использовании Microsoft Exchange Server 2007/2010/2013/2016). Для этого щелкните по ссылке **Открыть список сервисов**, далее щелкните правой кнопкой мыши по названию службы в списке и выберите **Остановить**. После остановки службы нажмите **Далее**.
3. Если вы хотите сохранить текущие настройки программы для их дальнейшего использования, например, после переустановки программы, установите флажок **Сохранить настройки**. Нажмите кнопку **Удалить**.
4. В ходе удаления приложения будут также удалены транспортные агенты для Microsoft Exchange Server 2007/2010/2013/2016 в системе SMTP-транспорта. Удаление транспортных агентов осуществляется посредством Exchange PowerShell. Подтвердите удаление транспортных агентов, набрав `Yes` (или `Y`) в консоли Exchange PowerShell. По завершении удаления введите команду `exit`, чтобы закрыть консоль.
5. Для завершения удаления приложения необходимо перезагрузить компьютер. Нажмите кнопку **Перезагрузить сейчас** или кнопку **Позже**.

6. Антивирусное сканирование и проверка на спам для Microsoft Exchange Server

Dr.Web для версий Exchange Server 2003/2007/2010 поддерживает интерфейс VSAPI (программный интерфейс приложений вирусного сканирования, разработанный Microsoft для серверов Exchange).

Кроме того, программа поддерживает серверные роли для версий Exchange Server 2007/2010/2013 SP1/2016 и может быть установлена на серверах с разными ролями.

В программе также реализована поддержка транспортных агентов (антивирусных агентов и агентов антиспама) для версий Exchange Server 2007/2010/2013/2016.

Версия Microsoft Exchange Server	Доступные модули антивирусного сканирования и фильтрации почты	Доступные модули проверки на спам и фильтрация почты
2003	DrWebVSAPI.dll (Backend)	DrWebSink.dll (IIS)
2007	DRWTransportAgent.dll (Hub, Edge) DrWebVSAPI.dll (Mailbox)	DRWTransportAgent.dll (Hub, Edge)
2010	DRWTransportAgent.dll (Hub, Edge) DrWebVSAPI.dll (Mailbox)	DRWTransportAgent.dll (Hub, Edge)
2013	DRWTransportAgent.dll (Frontend, Backend)	DRWTransportAgent.dll (Frontend, Backend)
2013 SP1	DRWTransportAgent.dll (Edge, MailBox)	DRWTransportAgent.dll (Edge, MailBox, CAS)
2016	DRWTransportAgent.dll (Edge, MailBox)	DRWTransportAgent.dll (Edge, MailBox)

Если вам необходимо установить на сервер почтовых ящиков (Mailbox) агенты антиспама, поставляемые вместе с Microsoft Exchange Server уже после установки Dr.Web, вам нужно понизить приоритет агентов Dr.Web. Таким образом проверка почты будет осуществляться сначала агентами Microsoft Exchange Server, а затем агентами Dr.Web.

6.1. Поддержка VSAPI

Антивирусные решения для серверов Exchange, работающие на основе VSAPI, проверяют все почтовые сообщения, поступающие на сервер, до отправки клиенту. Проверка осуществляется в трех режимах:

- упреждающем (proactive);
- по запросу (on-demand);
- фоновом (background).

Если адрес отправителя письма присутствует в списке значений переменной TrustedEmails, письмо сразу выводится из цикла проверки на вирусы и признается чистым.

Упреждающее сканирование

Все электронные сообщения, поступающие на сервер Exchange, помещаются в общую очередь на проверку антивирусным приложением. Сообщениям в очереди присваивается одинаковый низкий приоритет. Если приоритет сообщений не меняется, то проверка осуществляется по принципу «first in, first out» (FIFO), то есть в порядке поступления сообщений.

Сканирование по запросу

Если приоритет какого-либо сообщения повышается, что происходит при его запросе почтовым клиентом, то проверка этого сообщения будет выполнена досрочно, поскольку очередь на проверку обслуживается несколькими потоками. Изначально низкий приоритет вновь поступающих сообщений гарантирует, что их проверка не будет мешать проверке сообщений с высоким приоритетом.

Процессы упреждающего сканирования и сканирования по запросу обеспечивают проверку всех писем, проходящих через сервер. При этом система приоритетов позволяет оптимизировать нагрузку на сервер и время ожидания сообщения клиентом.

Фоновое сканирование

В режиме фонового сканирования производится проверка сообщений, уже находящихся в хранилище, что позволяет обнаруживать вирусы, попавшие в хранилище до установки Dr.Web, а также ранее неизвестные вирусы в сообщениях, проверенных до последнего обновления вирусных баз. Данный режим сканирования запускается администратором Exchange с помощью набора ключей реестра и управляется с помощью задачи **Doctor Web For Exchange Start Background Scanning Task** в планировщике задач Windows. По умолчанию данная задача запускается каждый день в 01:15.

Более подробную информацию о настройках антивирусного сканирования на основе VSAPI см. в приложении Настройки антивирусного сканирования Microsoft Exchange Server.

При совместном использовании VSAPI и транспортных агентов на одном сервере необходимо отключить проверку исходящих сообщений с помощью VSAPI при их поступлении в транспортную систему из почтового хранилища. Отключить такую проверку можно, установив значение `0` для параметра **TransportExclusion** в разделе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan`.

6.2. Серверные роли

Exchange Server 2007/2010/2013 SP1/2016 может быть установлен в нескольких конфигурациях, определяющих режимы работы сервера и поддерживаемую им функциональность. Для этого при развертывании задаются роли сервера в организации Exchange.

Exchange Server 2007/2010 и 2013 SP1 позволяет создать пять ролей сервера: сервер почтовых ящиков (Mailbox), сервер клиентского доступа (CAS), транспортный сервер-концентратор (Hub), сервер единой системы обмена сообщениями (Unified Messaging) и пограничный транспортный сервер (Edge). Exchange Server 2016 позволяет создать две роли: сервер почтовых ящиков и пограничный транспортный сервер.

Приведенные ниже роли сервера поддерживают проверку на вирусы и спам:

- **Сервер почтовых ящиков (Mailbox)** – реализует основные службы, в частности, для хранения данных и поддержки клиентских папок, и позволяет проверять сообщения на вирусы через интерфейс VSAPI;
- **Транспортный сервер-концентратор (Hub)** – распределяет сообщения внутри организации, позволяет применять для сообщений политики безопасности, осуществлять антивирусную проверку и фильтрацию спама;
- **Пограничный транспортный сервер (Edge)** – данная роль присваивается автономному серверу, находящемуся в демилитаризованной зоне и не использующему внутренние ресурсы организации (за исключением односторонней синхронизацией с Active Directory для регистрации топологии серверов транспортных концентраторов), что позволяет данному серверу выступать в качестве SMTP-шлюза и осуществлять фильтрацию спама и вирусов.

Dr.Web может быть установлен на сервер, для которого задана любая из этих ролей и их комбинации.

В Microsoft Exchange Server 2013 концепция серверных ролей уже не используется и осуществлен возврат к архитектуре Frontend–Backend, поэтому проверка на вирусы и спам всегда будет осуществляться агентами на уровне SMTP-транспорта.

6.3. Транспортные агенты

Концепция организации Microsoft Exchange 2007/2010/2013/2016 использует измененную структуру SMTP-событий. Поток сообщений на разных этапах SMTP-транспортировки обрабатывается транспортными агентами разной функциональности.

При поступлении сообщения на сервер, оно перенаправляется через транспортную сеть SMTP, при этом на каждое SMTP-событие может быть зарегистрировано несколько транспортных агентов, которые получают доступ к сообщению в соответствии с их приоритетатми и могут производить над ним определенные действия. Каждый агент выполняет свою проверку, после чего сообщение передается следующему агенту. Таким образом, транспортные агенты позволяют реагировать на события, связанные с получением письма и его дальнейшим передвижением по сети.

Существует два различных типа транспортных агентов:

- **SMTP Receive Agent** – позволяет реагировать на события, возникающие при получении письма по SMTP;
- **Routing Agent** – позволяет реагировать на события, возникающие при роутинге письма.

Exchange Server 2007/2010/2013/2016 позволяет задавать приоритет агентам транспорта и тем самым управлять очередностью применения агентов к сообщениям. Таким образом, порядок следования агентов определяется не только последовательностью событий, к которым они относятся, но и заданным приоритетом в рамках одного SMTP-события.

Транспортные агенты позволяют интегрировать Dr.Web в процесс обработки электронной почты, в частности, для проверки сообщений на вирусы и спам.

При использовании транспортных агентов Dr.Web проверяет на вирусы и спам только письма, принимаемые сервером по протоколу SMTP (при наличии лицензии «Антивирус + Антиспам»).

6.3.1. Транспортные агенты антиспама

Транспортные агенты антиспама реагируют на SMTP-событие **OnEndOfData**, соответствующее окончанию процесса получения сервером содержимого письма.

Письмо сразу выводится из проверки на спам и признается чистым, если:

- домен адреса отправителя письма присутствует в списке значений переменной TrustedDomains;
- адрес отправителя присутствует в списке значений переменной SpamTrustedEmails.

В отличие от белого списка Антиспама, который формирует политику применения исключений с учетом адресов отправителей и получателей (в частности, если

отправитель и получатель находятся в одном домене и адрес отправителя находится в белом списке, то письмо все равно может быть признано спамом), переменные TrustedDomains и SpamTrustedEmails безусловно исключают письмо из проверки на спам. Поэтому прибегать к добавлению доменов и адресов в список значений данных переменных рекомендуется только в случае крайней необходимости, а в общем случае использовать белый список консоли Dr.Web Administrator Web Console.

Если домен или адрес отправителя не относится к доверенным, письмо помещается в общую очередь на проверку. В результате проверки, если письмо признано спамом, оно может быть удалено, заблокировано, перенаправлено на другой почтовый ящик, помечено, как Junk email, или в тему сообщения добавлен префикс. Все эти события фиксируются в разделе событий Веб-консоли Администратора и в журнале событий сервера.

Если письмо удаляется как спам или блокируется как несоответствующее правилам фильтрации, транспортный агент либо разрывает соединение с клиентом, либо формирует ответ **RejectMessage** следующего содержания: **Dr.Web AntiSpam Agent: Message was rejected as spam**. Выбрать, какое именно действие будет выполняться, можно при помощи Административной консоли CMS. В любом случае письмо не доходит до получателей.

Если письмо перенаправляется на другой почтовый ящик или помечается, как Junk email, к его заголовку добавляется дополнительный служебный заголовок X-header.

Для перенаправляемого письма добавляется заголовок **X-DrWeb-RedirectTo**, в значении которого указывается адрес нового получателя. Этот заголовок предназначен для антивирусного транспортного агента, который после проверки письма на вирусы и признав его чистым, удаляет весь список исходных получателей сообщения, заменив их на адрес, указанный в заголовке. При этом письмо не будет получено исходными адресатами. Письмо будет доставлено исходным получателям, если оно помечено как Junk email. В этом случае в сообщение добавляется заголовок **X-MS-Exchange-Organization-SCL**, в значении которого указывается индекс недоверия письму. Этот заголовок понимают почтовые клиенты Microsoft, а также сам почтовый сервер Microsoft Exchange Server. Если значение индекса больше 4, но меньше 7, почтовые клиенты пользователей смогут перемещать такое сообщение в папку **Junk** (если они правильно настроены). Важно отметить, что если значение индекса превышает 7, письмо может быть отклонено транспортной системой самого сервера Microsoft Exchange Server.

Добавление префикса в тему письма, признанного спамом, никак не влияет на его доставку. Получатели могут сами настроить правила обработки писем с таким префиксом для своего почтового клиента.

6.3.2. Антивирусные транспортные агенты

Антивирусные агенты реагируют на SMTP-событие **OnSubmittedMessage**, соответствующее постановке в очередь обработки транспортной системой сервера.

Никакие исключения для писем из обработки этим агентом не предусмотрены.

Если адрес отправителя письма присутствует в списке значений переменной TrustedEmails, письмо сразу выводится из цикла проверки на вирусы и спам и признается чистым.

Цикл проверки антивирусного агента подразумевает последовательную проверку на вирусы тела письма и всех его вложений. Инфицированное письмо может быть удалено, заблокировано или перемещено в Карантин (для подозрительных объектов также предусмотрена возможность пропустить их, не применяя к ним никаких действий). Все эти события фиксируются в разделе событий консоли Dr.Web Administrator Web Console и в журнале событий сервера.

Если для инфицированных объектов настроено удаление, после обнаружения первого инфицированного объекта цикл сканирования вложений прерывается, и в транспортную систему сервера посылается событие на удаление письма. События удаления фиксируются в разделе событий консоли Dr.Web Administrator Web Console и в журнале событий сервера, но ни отправители, ни получатели не уведомляются об удалении письма. Это наиболее быстрый способ реакции на инфекции, однако, более безопасным способом обработки с точки зрения возможной потери данных является перемещение зараженных объектов в Карантин. Кроме того, если на сервере поддерживается протокол EWS (Exchange Web Services), существует возможность с помощью консоли Dr.Web Administrator Web Console или консоли Dr.Web CMS Web Console настроить отправку уведомлений на определенный почтовый адрес для каждого случая удаления инфицированных писем.

Если вложение блокируется, как несоответствующее правилам фильтрации, и для инфицированных объектов настроено перемещение в Карантин, все инфицированные или заблокированные вложения в исходном сообщении заменяются вложенными текстовыми файлами, описывающими причину удаления вложения. Далее, в очищенном письме проверяется наличие заголовка **X-DrWeb-RedirectTo**, поставленного транспортным агентом антиспама, и если такой заголовок не найден, письмо доставляется получателям. Если же письмо должно быть перенаправлено, каждому получателю письма отправляется уведомление **SmtpResponce** следующего содержания: «**Dr.Web AntiVirus Agent: Message was redirected as spam.**». При этом, письмо без инфицированных вложений отправляется по адресу, указанному в значении заголовка **X-DrWeb-RedirectTo**.

6.4. Службы Dr.Web

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

- **Dr.Web CMS** – поддерживает распределенную систему управления компонентами приложения, реализуя основной функционал по контролю работоспособности отдельных модулей и их функциональную диагностику. Сервис поддерживает базу данных настроек компонентов приложения, базу событий и отслеживает статистику рабочих параметров компонентов.
- **Dr.Web CMS Web Console** – содержит встроенный веб-сервер, предоставляющий возможность запуска административных консолей приложения в браузере.
- **Dr.Web for MSP Component Host** – инстанцирует в себе все запрашиваемые в процессе работы вспомогательные компоненты приложения.
- **Dr.Web for MSP Scanning Service** – подготавливает объекты, перехваченные фильтрами приложения, к процессу антивирусного сканирования, а также обрабатывает полученные результаты
- **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 работу приложений, работающих на платформе CMS, и отвечает за перезапуск основных служб.

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

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

7. Консоль Dr.Web Administrator Web Console

Работа Dr.Web может быть настроена с помощью консоли Dr.Web Administrator Web Console (см. Рисунок 1).

Запуск консоли консоли Dr.Web Administrator Web Console

Для корректной работы консоли Dr.Web Administrator Web Console необходимо использовать следующие браузеры:

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

Кроме того, для корректной работы 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 Enchanced 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 консоли Dr.Web Administrator Web Console откройте в браузере следующую страницу:

`https://<Exchange Server address>:2080/exchange`,

где <*Exchange Server address*> – это IP-адрес сервера Exchange.

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

При первом запуске консоли Dr.Web Administrator Web Console используйте данные учетной записи по умолчанию: имя пользователя **root** и пароль **drweb**.

Если не удается открыть Dr.Web Administrator Web Console на удаленном компьютере, убедитесь, что для брандмауэра Windows созданы необходимые разрешающие правила.

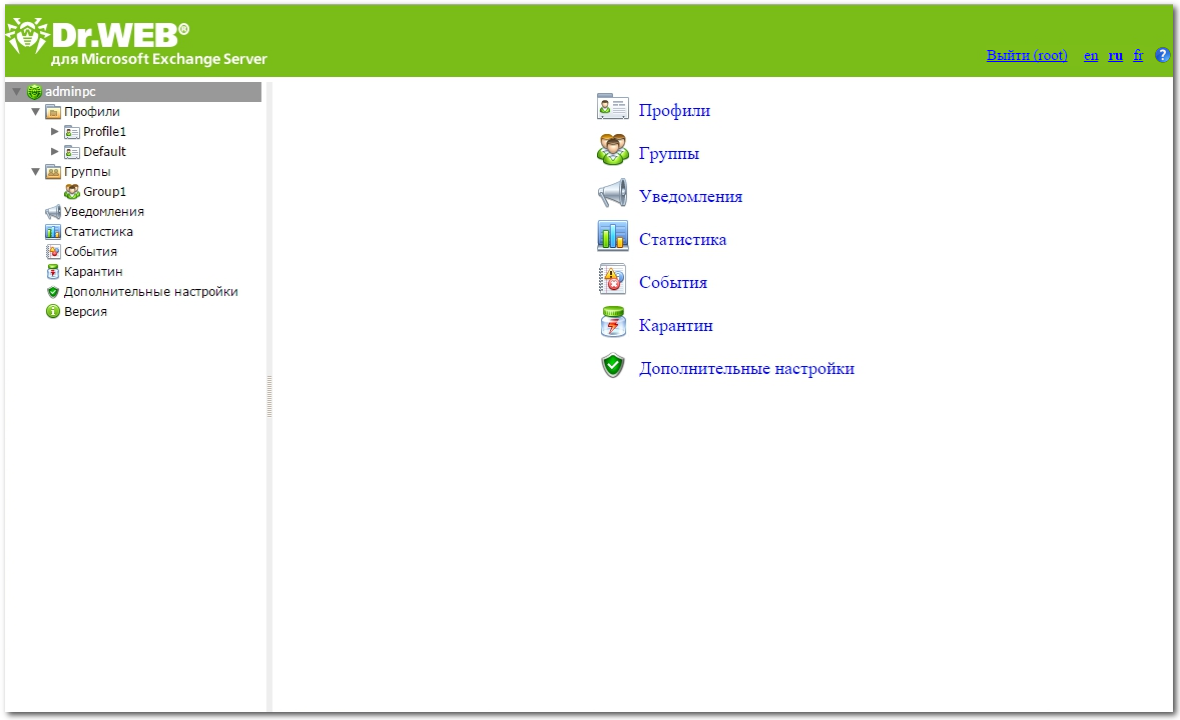

Рисунок 1. Dr.Web Administrator Web Console

Интерфейс

Dr.Web Administrator Web Console состоит из двух частей:

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

Администрирование

Предусмотрены следующие уровни доступа к консоли Dr.Web Administrator Web Console:

- с возможностью изменения настроек;
- без возможности изменения настроек.

Установить уровень доступа можно при добавлении новой учетной записи администратора.

7.1. Группы и профили

Для упрощения организации антивирусной защиты среды Exchange в Dr.Web реализована возможность создания групп клиентов и присвоения им определенных профилей. Профиль представляет собой набор настраиваемых параметров обработки сообщений, от которых зависит то, как именно будет осуществляться защита среды Exchange. Настройки профиля находятся в разделе дерева консоли Dr.Web Administrator Web Console **Профили**, который разделен на следующие подразделы:

- Сканирование – в данном разделе вы можете настроить работу вашего основного компонента обнаружения вирусов;
- Антиспам – в данном разделе вы можете настроить работу Антиспама (настройки в данном разделе доступны только при наличии версии «Антивирус + Антиспам», т.е. в том случае, если у вас есть соответствующий ключевой файл (см. Лицензионный ключевой файл);
- Фильтрация – в данном разделе вы можете создать правила для фильтрации электронных писем.

Любой профиль можно назначить группе клиентов. Эти группы формируются в разделе дерева консоли **Группы**.

7.1.1. Создание и настройка профилей

В процессе установки Dr.Web автоматически создает стандартный профиль **Default**, который нельзя удалить или переименовать. Этот профиль будет применяться ко всем письмам, пока вы не создадите другой профиль и не назначите его определенной группе клиентов. При создании нового профиля его параметры принимают текущие значения настроек стандартного профиля.

Для управления существующими профилями и создания новых перейдите к области сведений раздела **Профили**, выбрав пункт **Профили** в дереве консоли Dr.Web Administrator Web Console (см. Рисунок 2).

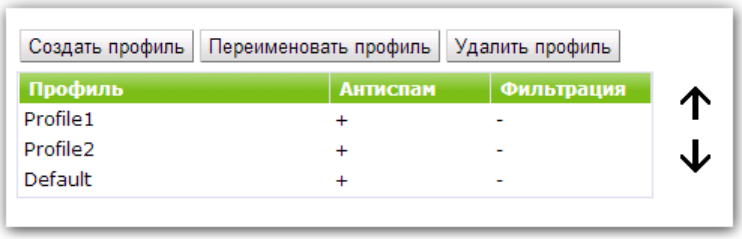

Рисунок 2. Раздел Профили

Для каждого профиля в списке содержится также информация о его настройках, а приоритет профиля определяется в зависимости от его положения в таблице.

Чтобы создать новый профиль:

1. Нажмите кнопку **Создать профиль**, расположенную над списком существующих профилей.

   

   Либо, для создания нового профиля щелкните правой кнопкой на пункте **Профили** в дереве консоли и выберите **Создать профиль** в появившемся контекстном меню.

2. В открывшемся окне введите имя профиля. Новый профиль появится в дереве консоли под пунктом **Профили**. Если профиль с таким же именем уже существует, профиль создан не будет.

Чтобы изменить имя профиля:

Выберите нужный профиль в списке, расположенном в области сведений раздела **Профили**, и нажмите кнопку **Переименовать профиль**;

Чтобы удалить профиль:

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

Либо, чтобы удалить или переименовать профиль, щелкните правой кнопкой на имени этого профиля в дереве консоли и выберите соответствующий пункт в появившемся контекстном меню.

По умолчанию настройки созданного профиля будут такими же, как настройки стандартного профиля.

Чтобы изменить настройки профиля:

Выберите имя профиля в дереве консоли Dr.Web Administrator Web Console и перейдите к желаемому разделу: Сканирование, Антиспам или Фильтрация.

7.1.1.1. 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 сообщений, получаемых или отправляемых этим клиентом, будет использован профиль с наибольшим 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, и его нельзя переместить выше нижней строки в списке профилей.

7.1.1.2. Сканирование

Процесс сканирования настраивается в разделе настроек **Сканирование**. Изменение параметров в этом разделе влияет на типы проверяемых объектов, а следовательно, на уровень надежности антивирусной защиты. 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 консоли Dr.Web Administrator Web Console. Откроется область сведений для настройки сканирования (см. Рисунок 3).

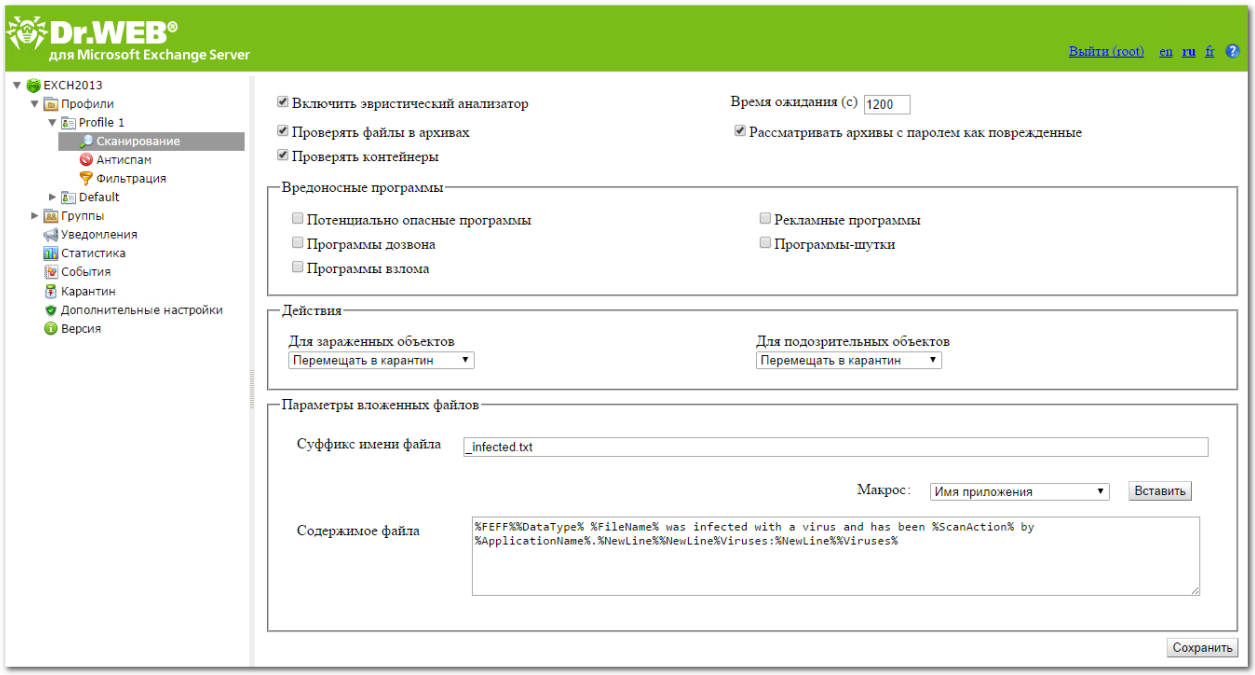

Рисунок 3. Раздел настроек сканирования

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

Отключать эвристический анализатор и проверку файлов в прикрепленных архивах не рекомендуется, так как это приведет к существенному снижению уровня надежности антивирусной защиты.

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

Флажок **Рассматривать архивы с паролем как поврежденные** определяет, будет ли программа игнорировать такие архивы или применять к ним действия, заданные для зараженных объектов. Типы объектов, которые будут рассматриваться как поврежденные, можно указать при помощи консоли CMS.

3. В группе настроек **Вредоносные программы** вы можете указать типы вредоносных объектов, которые следует искать в письмах. Для этого установите соответствующие флажки. К выбранным программам будет применяться действие, установленное для зараженных объектов.
4. 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**. Тело письма будет пропущено, а вложенный файл отправлен в карантин (см. Работа с карантином).
   - **Удалить**. Объект будет удален.
   - **Пропустить**. Письмо будет пропущено и направлено получателю (действие доступно только для подозрительных объектов).
   - **Архивировать**. Зараженный вложенный файл будет переименован в **inf*.tmp**, где * – произвольный набор символов, и запакован в zip-архив. При этом копия файла будет перемещена в карантин. Пароль для данного архива, а также максимальный допустимый размер архивируемого файла, можно указать в разделе Дополнительные настройки.

   По умолчанию для всех типов объектов выбрано действие **Перемещать в карантин**.
5. В группе настроек **Параметры вложенных файлов** вы можете изменить суффикс имени файла, который прилагается к письму после того, как программа совершит над ним выбранное действие. В поле **Содержимое файла** 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.

7.1.1.3. Антиспам

Перед началом проверки сообщения на спам анализируются адреса получателей и отправителей на принадлежность к черным и белым спискам, которые задаются в разделе **Антиспам**. Затем осуществляется проверка текста сообщения при помощи компонента Антиспам.

Антиспам анализирует содержимое электронных сообщений и делает заключение о том, являются ли они спамом, на основе подсчета различных параметров, характерных для спама. В зависимости от результатов анализа, каждому письму присваивается целое число (*score*). Чем больше это число, тем больше вероятность того, что письмо является спамом. Изменять пороговое значение для определения принадлежности письма к спаму можно при помощи консоли Dr.Web CMS Web Console.

Письма с ложными срабатываниями Антиспама следует пересылать на адрес vrnonspam@drweb.com, а письма с пропущенным спамом – на адрес vrspam@drweb.com.

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 должна быть включена по умолчанию (т.е. должен быть установлен флажок **Включить антиспам** в верхней части области сведений раздела **Антиспам**).

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

Чтобы проверить, поддерживается ли компонент Антиспам вашей лицензией, откройте ваш ключевой файл (файл drweb32.key, расположенный в папке %ProgramFiles%\DrWeb for Exchange\) в текстовом редакторе и найдите в нем значение параметра SpamFilter. Если SpamFilter=Yes, то это означает, что ваша лицензия поддерживает использование компонента Антиспам, если SpamFilter=No, компонент Антиспам не поддерживается.

Любое редактирование ключевого файла делает его недействительным! Поэтому не сохраняйте ключевой файл при закрытии текстового редактора.

Чтобы настроить работу Антиспама:

1. Выберите пункт **Антиспам** для настраиваемого профиля в дереве консоли Dr.Web Administrator Web Console. Откроется область сведений раздела **Антиспам** (см. Рисунок 4).

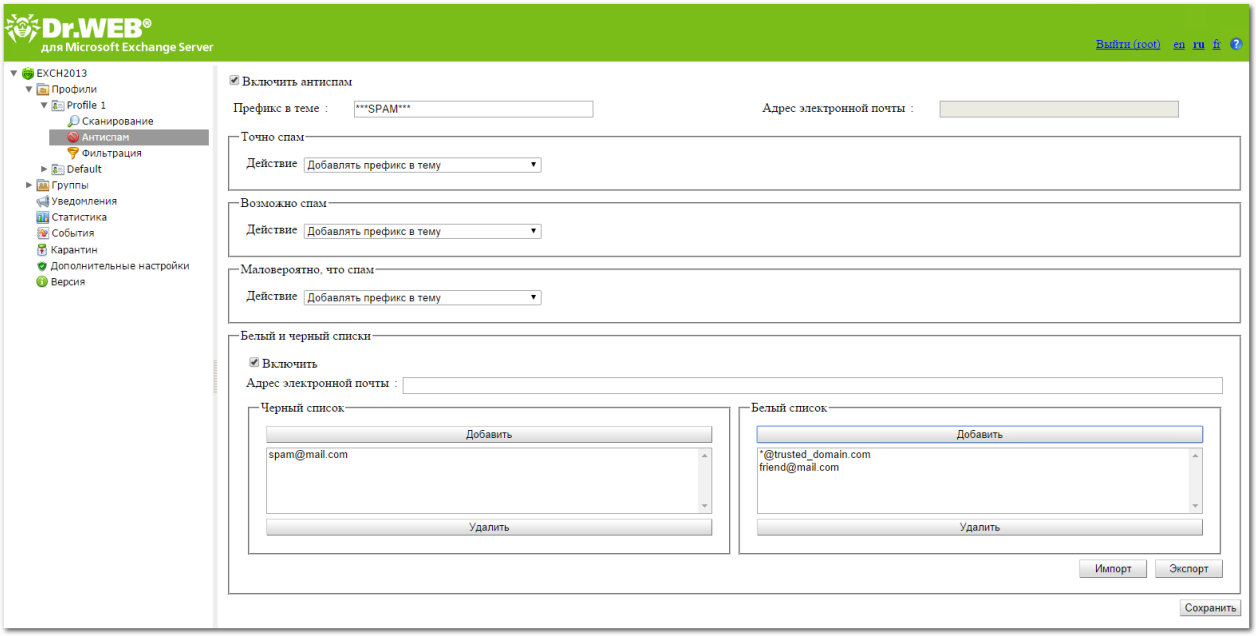

Рисунок 4. Раздел настроек Антиспама

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 поле **Адрес электронной почты** вы можете задать адрес электронной почты, на который будут перенаправлены письма, являющиеся спамом.
5. 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:
   - **Добавлять префикс в тему**. К теме письма будет добавлен префикс, указанный в поле **Префикс в теме**;
   - **Пропустить**. Письмо будет пропущено и доставлено получателю;
   - **Перемещать в папку нежелательной почты**. Для сообщения добавляется служебный заголовок **X-MS-Exchange-Organization-SCL**, в значении которого указывается индекс недоверия к письму. Если значение индекса больше 4, но меньше 7, почтовые клиенты, для которых установлены необходимые настройки, смогут перемещать такое сообщение в папку нежелательной почты.

- **Перенаправлять**. Письмо будет перенаправлено по адресу, указанному в поле **Адрес электронной почты**;
- **Блокировать**. Передача письма будет заблокирована.

6. 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 адреса, которым вы доверяете, в белый список. Письма с данных адресов не будут проходить проверку на спам. Если вы добавите адрес в черный список, то всем письмам с этого адреса будет присваиваться статус **Точно спам**;
   - чтобы добавить адрес, введите его в поле **Адрес электронной почты**, затем нажмите кнопку **Добавить в белый список** или **Добавить в черный список** для добавления в нужный список;
   - чтобы удалить адрес из списка, выберите его в нужном списке и нажмите кнопку **Удалить из белого списка** или **Удалить из черного списка**;
   - с помощью кнопок **Экспорт** и **Импорт** 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. В данном случае электронные адреса должны указываться с префиксом **«+»** (для добавления адреса в белый список) или **«-»** (для добавления адреса в черный список), например **+trusted_address@mail.com** и **-distrusted_address@mail.com**, а сам текстовый файл должен быть сохранен с расширением **.lst** в формате Unicode.

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

В некоторых случаях добавление домена в белый список выше указанным способом может не сработать. Чтобы исключить такой домен из проверки на спам, необходимо добавить его в список значений переменной TrustedDomains.

7. Нажмите кнопку **Сохранить**, когда закончите изменять настройки Антиспама.

7.1.1.4. Фильтрация

Dr.Web позволяет использовать специальную систему фильтрации для снижения нагрузки на почтовый сервер. Например, в случае спам-атаки, лишние письма выводятся из транспортной системы сервера до начала их проверки на спам или вирусы. Для эффективной работы фильтров необходимо задать оптимальный набор правил фильтрации, не содержащий противоречивых и лишних правил.

Перед выполнением фильтрации определяется группа, к которой принадлежит отправитель письма. Если отправитель принадлежит к одной из созданных групп, к нему будут применены правила фильтрации, заданные в профиле соответствующей группы. Если отправитель письма не принадлежит ни к одной из групп, для письма будут применены настройки профиля **Default**. Таким образом, если необходимо, чтобы

правило фильтрации применялось ко всем письмам от отправителей, не входящих в группы, создайте его настройках фильтрации стандартного профиля **Default**.

Если профиль отправителя не содержит каких-либо ограничений, и письмо проходит дальше, определяется профиль, который следует применять для его дальнейшей обработки в зависимости от адресов получателей. Каждый адрес из списка получателей будет соотнесен со своей группой (будь то группа AD или список адресов), и для каждой из них будет определен соответствующий профиль настроек. Для применения фильтрации будет выбран профиль с наибольшим приоритетом. Таким образом, если необходимо, чтобы определенные ограничения распространялись на созданную группу получателей, то не создавайте правила фильтрации для нее в стандартном профиле **Default**, а создайте для этой группы отдельный профиль.

Если необходимо создать специальные группы получателей, для которых не будут действовать никакие ограничения, не создавайте никаких правил фильтрации в стандартном профиле **Default**, поскольку письмо, отфильтрованное в соответствии с правилами профиля отправителя, будет исключено из дальнейшей обработки по профилям получателей.

В первую очередь каждое письмо обрабатывается транспортным агентом антиспама. На данном этапе применяются правила фильтрации к письму как к целому объекту. Фильтрация осуществляется по количеству отправителей, получателей, теме, числу вложений и т.д. После выполнения фильтрации осуществляется дальнейшая проверка неотфильтрованных писем на спам (см. Схему 1).

Вторым транспортным агентом на пути письма является антивирусный агент. На данном этапе применяются правила фильтрации к письму как к набору файлов, при этом тело письма само рассматривается как файл. Фильтрация осуществляется по размеру файлов, их именам, расширениям и т.д. После выполнения фильтрации осуществляется дальнейшая проверка неотфильтрованных писем на вирусы (см. Схему 1).

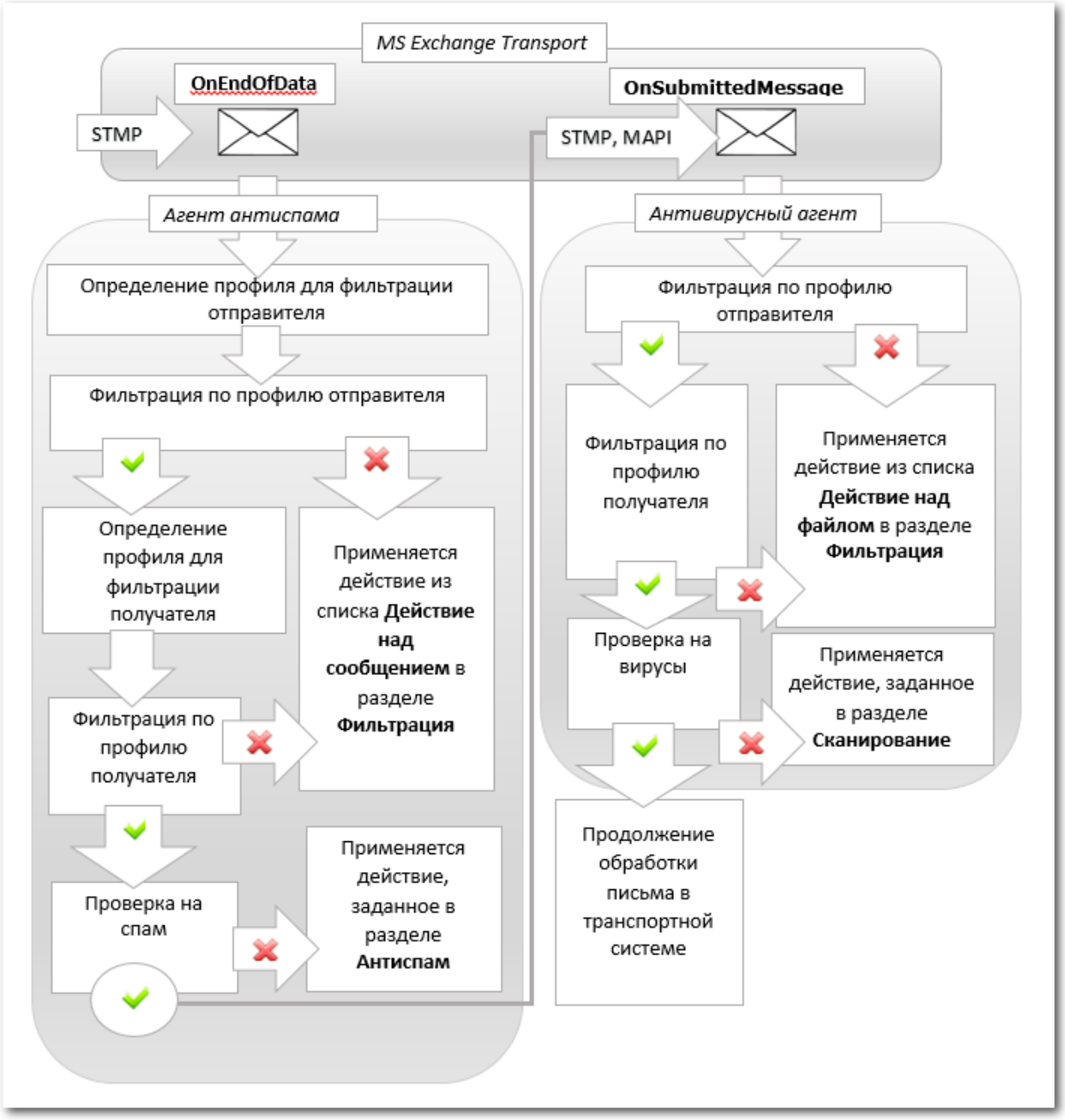

Схема 1. Фильтрация писем в транспортной системе

Фильтрация трафика настраивается в разделе настроек профиля **Фильтрация** (см. Рисунок 5). Работа фильтров определяется набором правил, которые может добавлять администратор. Правила задают условия для фильтрации по основным свойствам сообщений и их вложений.

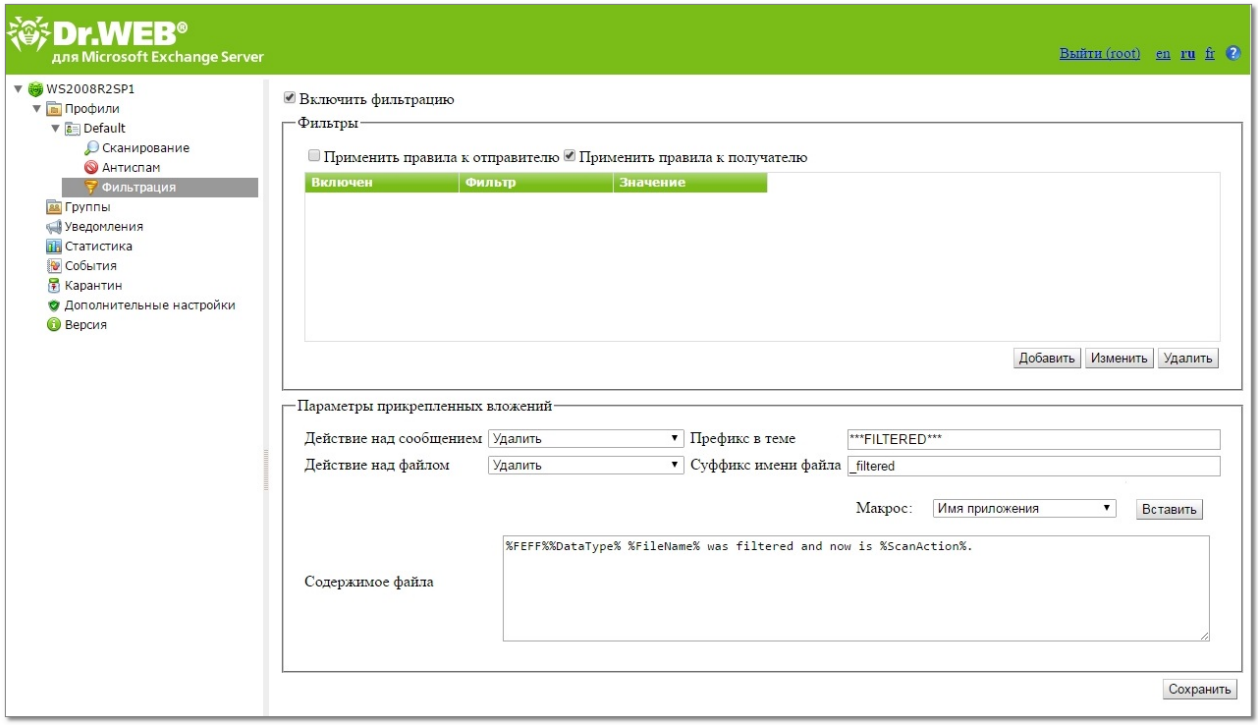

Рисунок 5. Раздел настройки фильтрации

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

Чтобы настроить фильтрацию сообщений:

1. Включите фильтрацию, установив флажок **Включить фильтрацию** в верхней части области сведений раздела **Фильтрация**. При этом, настройки в данном разделе станут доступными.

   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. Включите использование одного или нескольких фильтров из списка, установив соответствующие флажки. Если в списке еще нет фильтров, вы можете их создать.

3. В разделе **Параметры вложенных файлов** 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:

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

   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 вы можете использовать макросы из выпадающего списка **Макрос**.

Чтобы создать правило фильтрации:

1. Нажмите кнопку **Добавить** под списком правил. Откроется окно **Правило фильтрации** (см. Рисунок 6), в котором вы можете задать имя правила и его условия.

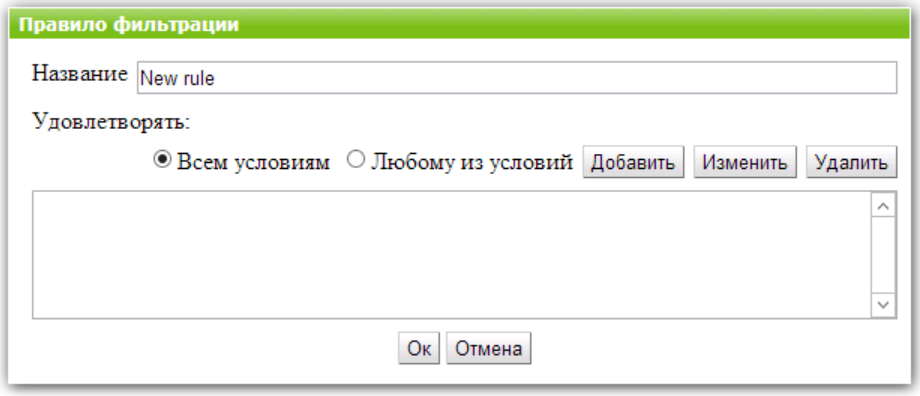

Рисунок 6. Настройка правила фильтрации

2. Вы можете добавить одно или несколько условий фильтрации и 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:

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
Адресат данных	Равно Не равно Включает Не включает Соответствует Не соответствует	Указывается вручную
Протокол	Равно Не равно	SMTP MAPI
Число получателей	Равно Не равно Больше Не больше Меньше Не меньше	Указывается вручную
Имя файла	Равно Не равно Включает Не включает	Указывается вручную

Тип условия	Тип соответствия	Значение
	Соответствует Не соответствует	
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
Есть вложение	Равно Не равно	Ложь Правда

Если для какого-либо из условий **Источник данных**, **Адресат данных**, **Имя файла** и **Тема сообщения** выбран тип соответствия **Включает**, **Не включает**, **Соответствует** или **Не соответствует**, при указании значения вы можете использовать подстановочные символы «*» и «?» вместо любой последовательности символов или одного любого символа соответственно.

3. Чтобы удалить или изменить одно из условий, выделите его в списке и нажмите кнопку **Удалить** или **Изменить** соответственно.

Пример правила фильтрации

Для фильтрации файлов, размер которых превышает 20000 байт, можно использовать правило (см. Рисунок 7), состоящее в одновременном выполнении следующих условий:

Тип условия	Тип соответствия	Значение
Тип данных	Равно	Файл

Тип условия	Тип соответствия	Значение
Размер файла	Больше	20000

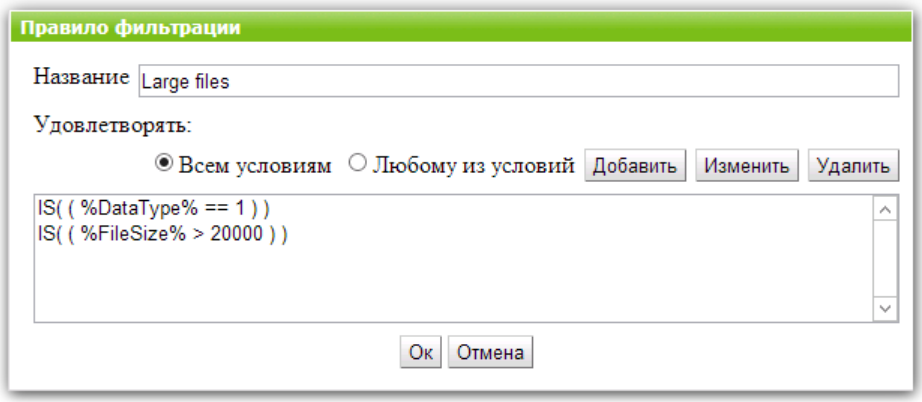

Рисунок 7. Пример правила фильтрации

Чтобы изменить или удалить существующее правило фильтрации:

Для изменения или удаления правила выделите его в списке фильтров и нажмите кнопку **Изменить** или **Удалить** под списком фильтров.

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

Поскольку в некоторых случаях применение фильтрации может повлиять на работоспособность почтовой системы, рекомендуется выполнить следующие действия:

- добавить в исключения в переменную TrustedEmails. Учетные записи для системных ящиков хранятся в Active Directory, а их названия содержат в начале текст «HealthMailbox».
- не создавать фильтров с условием удаления небольших по размерам файлов (менее 1000 байт), чтобы под такие условия не попадали уведомления. Иначе может произойти так называемое «зацикливание», когда уведомление повторно подпадает под действие фильтра.

7.1.2. 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.

При создании групп и назначении им профилей необходимо учитывать, что к пользователям групп типа Security в Active Directory всегда применяется стандартный профиль. Таким образом, чтобы объединить пользователей домена в группы для назначения им других профилей настроек, необходимо сначала создать для них дополнительные выделенные группы с типом Distribution в настройках Active Directory.

7.1.2.1. Создание новой группы

Для управления существующими группами и создания новых откройте область сведений раздела **Группы**. Для этого выберите пункт **Группы** в дереве консоли Dr.Web Administrator Web Console (см. Рисунок 8).

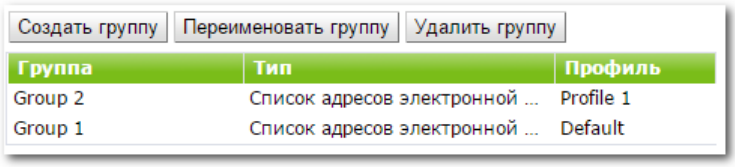

Рисунок 8. Раздел Группы

Чтобы создать новую группу:

1. В области сведений раздела **Группы** нажмите кнопку **Создать группу**, расположенную над списком существующих групп.

   Либо щелкните правой кнопкой на пункте **Группы** в дереве консоли и нажмите **Создать группу** в появившемся контекстном меню.

2. В открывшемся окне введите имя группы. Новая группа появится в дереве консоли под пунктом **Группы**. Если группа с таким же именем уже существует, новая группа создана не будет.

Чтобы изменить имя группы:

Выберите нужную группу в списке в области сведений раздела **Группы** и нажмите кнопку **Переименовать группу**.

Чтобы удалить группу:

Выберите ее в списке в области сведений раздела **Группы** и нажмите кнопку **Удалить группу**.

Либо, чтобы удалить или переименовать группу, щелкните правой кнопкой на имени этой группы в дереве консоли Dr.Web Administrator Web Console и выберите соответствующий пункт в появившемся контекстном меню.

Чтобы открыть настройки группы:

Чтобы открыть область сведений с настройками группы, выберите ее имя в дереве консоли Dr.Web Administrator Web Console.

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**.

7.1.2.2. Настройки и формирование групп

В области сведений, открывающейся при щелчке по группе в дереве консоли Dr.Web Administrator Web Console (см. Рисунок 9), вы можете изменить настройки выбранной группы, в том числе определить способ ее формирования: путем задания списка почтовых адресов или путем выбора из списка групп AD. Вы можете выбрать тип группы в выпадающем списке **Тип**.

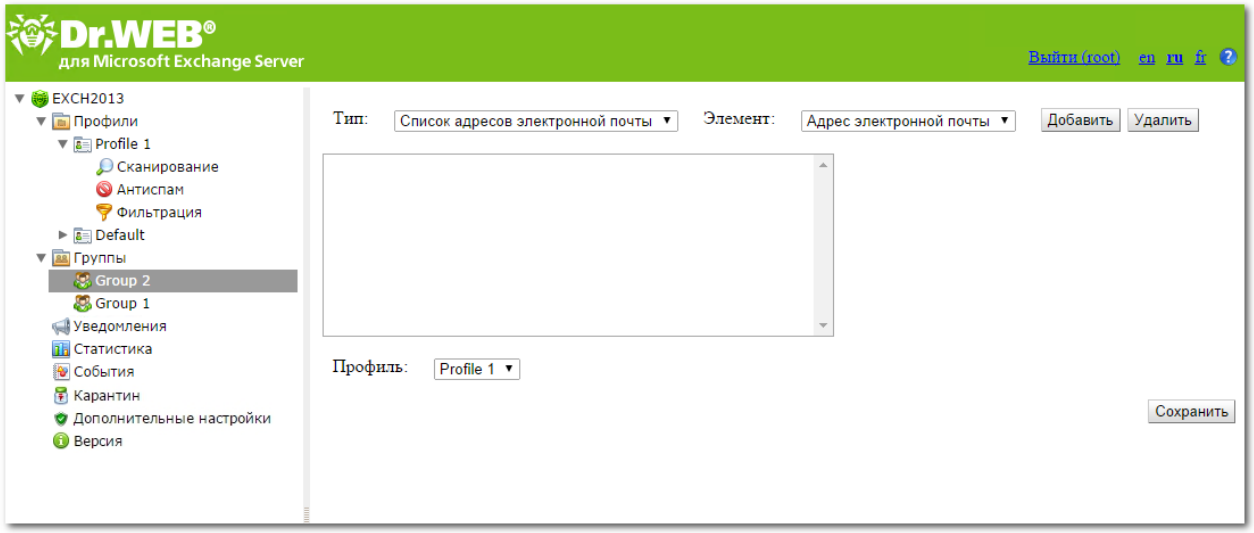

Рисунок 9. Настройки группы

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 **ОК**.
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 групп AD:

1. В выпадающем списке **Тип** выберите значение **Список групп AD**.
2. Чтобы добавить группу в список, нажмите кнопку **Добавить**. В открывшемся окне выберите группу и нажмите кнопку **Ok**.

   При добавлении группы AD убедитесь, что вы добавляете группу распределения (Distribution), а не группу безопасности (Security), в противном случае вы не сможете назначить ей профиль, отличный от стандартного.

3. Чтобы удалить группу из списка, выделите ее и нажмите кнопку **Удалить**, после чего подтвердите удаление выбранной группы.

   Формирование списка групп AD возможно только в том случае, если сервер включен в домен. В противном случае необходимо включить сервер в домен, либо указать имя и пароль пользователя, который имеет доступ к AD, в качестве значений параметров **/DrWebADAccessor_1.0/Application Settings/ADAccUserName** и **/DrWebADAccessor_1.0/Application Settings/ADAccPassword** соответственно в **Административной консоли CMS**. По умолчанию значения этих параметров – пустые.

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

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

7.2. Уведомления

Уведомления заносятся в журнал операционной системы и используются для информирования администратора и пользователей сети 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 консоли Dr.Web Administrator Web Console. Откроется область сведений для настройки уведомлений (см. Рисунок 10).

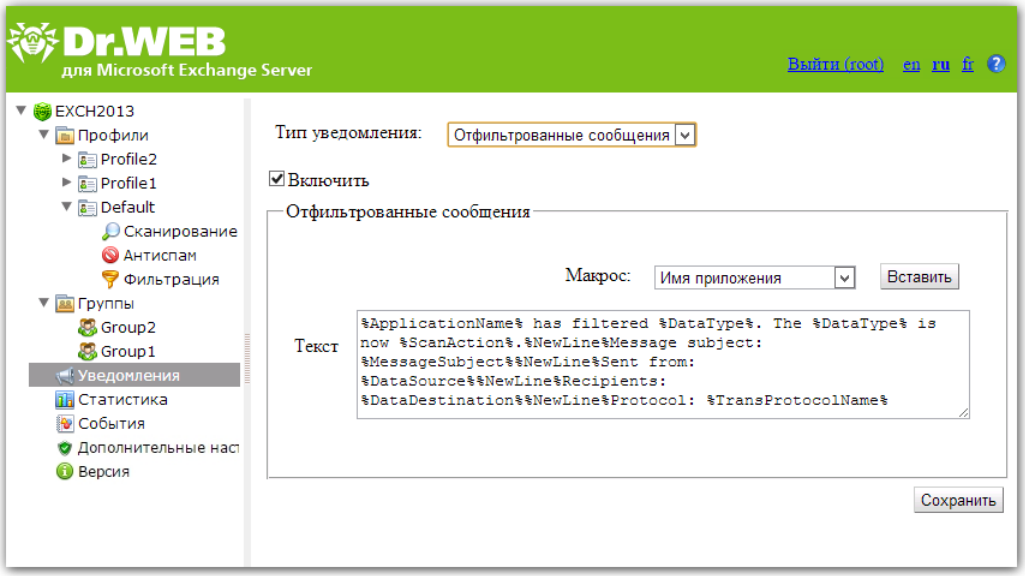

Рисунок 10. Раздел настройки уведомлений

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.
   - **Спам** – для отправки уведомлений о спаме;
   - **Зараженные** – для отправки уведомлений об обнаруженных вирусных угрозах;
   - **Обновление** – для отправки уведомлений с информацией о последнем обновлении;
   - **Устаревшие базы** – для отправки уведомлении о необходимости обновить вирусные базы.
3. Чтобы включить отправку уведомлений выбранного типа, установите флажок **Включить**.
4. В разделе настроек ниже вы можете изменить шаблон уведомления выбранного типа в поле **Текст**. При редактировании текста вы можете использовать макросы.
5. Нажмите кнопку **Сохранить**, когда закончите изменять настройки уведомлений.

7.3. Просмотр статистики

Раздел **Статистика** позволяет просмотреть общие или средние количественные данные о работе Dr.Web за определенный период времени (см. Рисунок 11).

Рисунок 11. Раздел статистики

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 момента запуска 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.

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

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**. 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.

7.4. Просмотр списка событий

Раздел **События** позволяет просмотреть все события, связанные с работой Dr.Web (см. Рисунок 12).

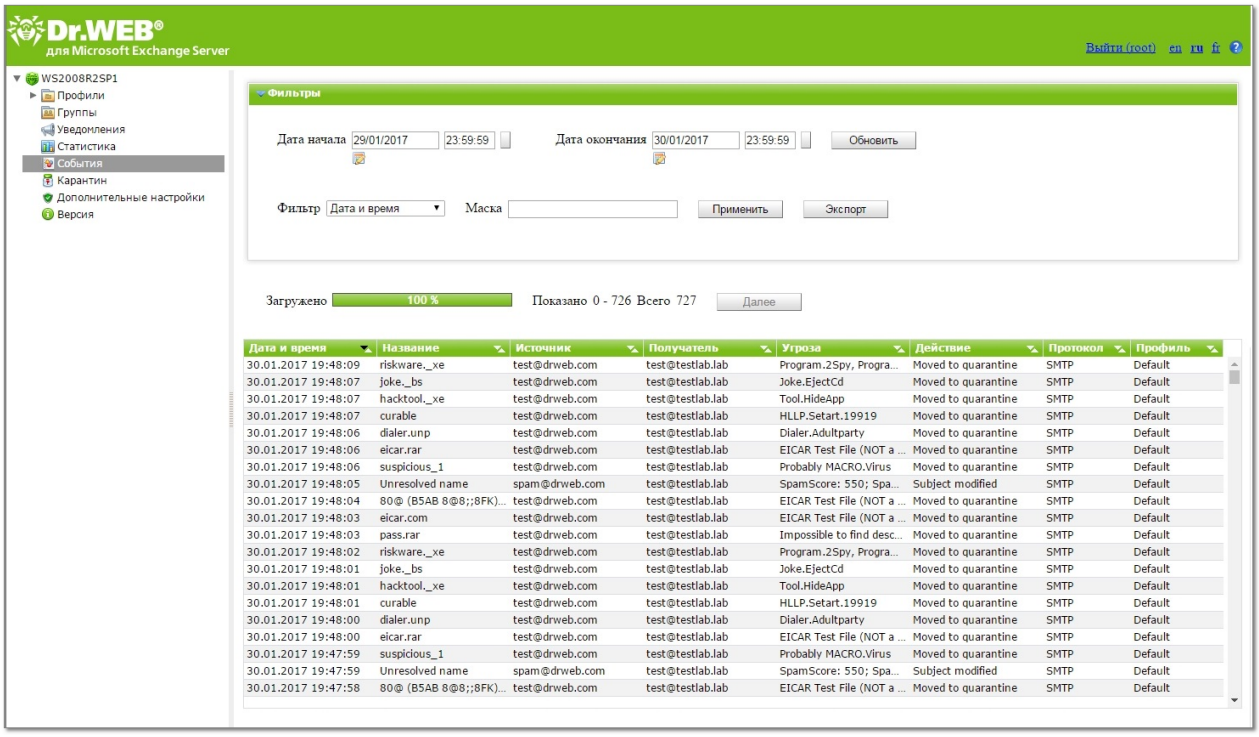

Рисунок 12. Раздел событий

Информация о событиях

Для каждого события в списке отображается следующая информация:

- дата и время события;
- название объекта, с которым связано событие;
- электронные адреса отправителя и получателей письма, содержавшего инфицированный объект;
- тип угрозы;
- действие, которое было применено к угрозе;
- протокол, по которому было передано письмо;
- название примененного профиля.

Вы можете задать параметры отображения информации в списке событий:

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.

На страницу умещается определенное количество строк списка. Если количество строк за выбранный период превышает это ограничение, вы можете пролистать список и перейти к другим событиям при помощи кнопки **Далее**.

Действия над списком событий

1. Вы можете настроить просмотр событий за определенный период времени. Для этого укажите дату и время начала и окончания интересующего интервала 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 событий в виде текстового файла. Для этого нажмите кнопку **Экспорт**. В открывшемся окне выберите формат файла для сохранения и нажмите кнопку **ОК**. Список событий 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 событий нажмите кнопку **Обновить**. Список событий обновляется при каждом запуске консоли Dr.Web Administrator Web Console и переходе в раздел **События**. Обновление может занять некоторое время. Если вы хотите отменить ход обновления, например, при ошибочно указанных параметрах фильтрации, нажмите кнопку **Отмена**.

7.5. Работа с карантином

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

В разделе **Карантин** консоли Dr.Web Administrator Web Console выводится информация о текущем состоянии карантина. Кроме того, для просмотра и редактирования содержимого карантина вы можете использовать Менеджер карантина.

7.5.1. Управление карантином с помощью Dr.Web Administrator Web Console

Для просмотра списка объектов в карантине выберите пункт **Карантин** в дереве консоли Dr.Web Administrator Web Console. Откроется область сведений карантина (см. Рисунок 13).

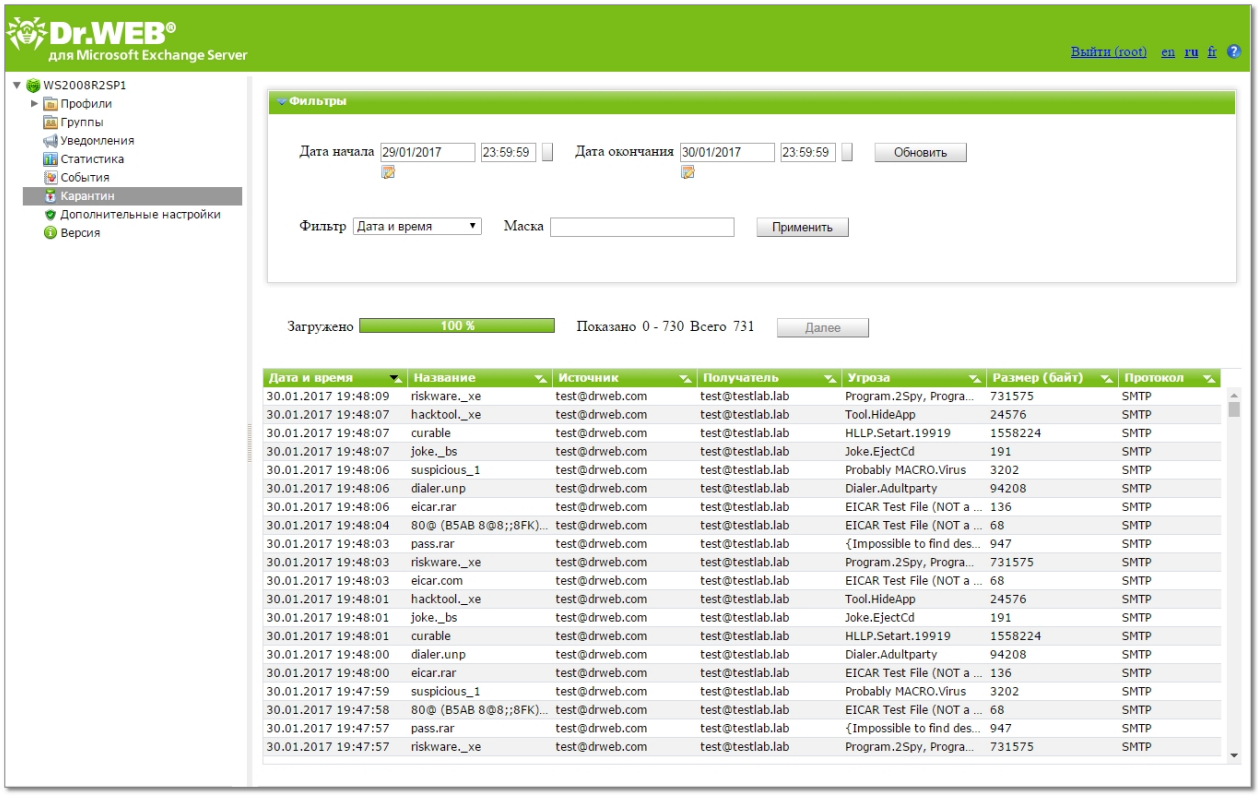

Рисунок 13. Список объектов в карантине

Просмотр информации об объектах в карантине

Для каждого объекта в списке отображается следующая информация:

- дата и время перемещения в карантин;
- имя инфицированного файла;
- адреса электронной почты отправителя и получателей письма, содержавшего инфицированный объект;
- название угрозы;
- размер файла (в байтах);
- протокол, по которому было передано письмо.

Вы можете задать параметры отображения информации в списке карантина:

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

При просмотре списка объектов в карантине доступны следующие опции:

- На страницу умещается определенное количество строк списка объектов. Если количество строк за выбранный период превышает это ограничение, вы можете пролистать список и перейти к другим объектам, перемещенным в карантин, при помощи кнопки **Далее**.
- 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 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. Затем укажите путь для восстановления файла.

7.5.2. 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 14) воспользуйтесь ссылкой **Dr.Web Quarantine** на Рабочем столе.

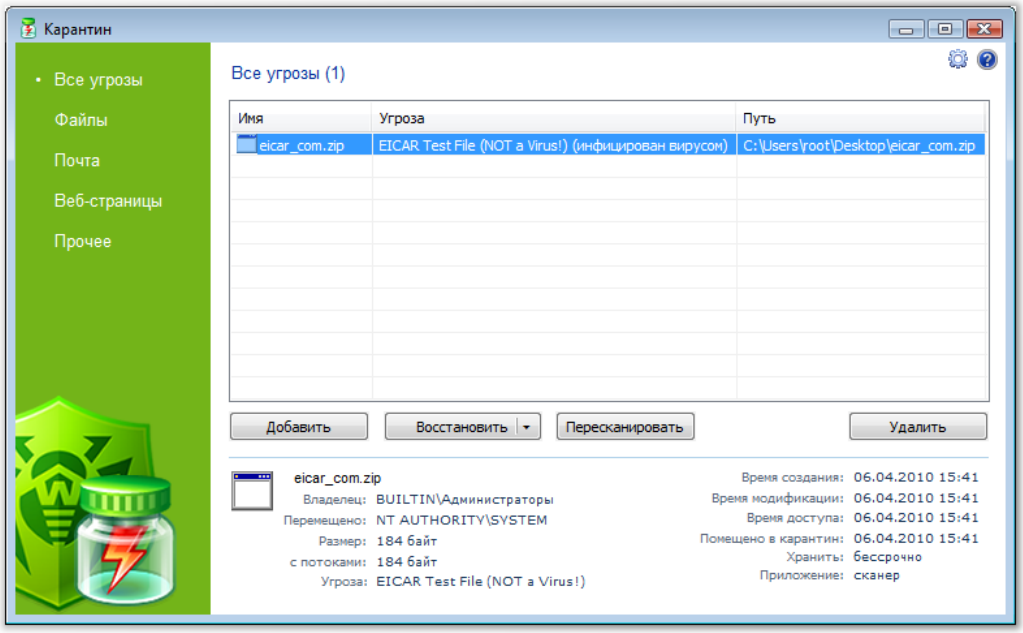

Рисунок 14. Главное окно утилиты Quarantine

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

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

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

Чтобы настроить отображение столбцов:

1. Чтобы задать параметры отображения информации в таблице карантина, щелкните правой кнопкой мыши по заголовку таблицы и выберите в контекстном меню пункт **Настроить колонки**.
2. Выберите типы информации, которые вы хотите включить в таблицу объектов. Чтобы исключить столбцы из таблицы объектов, снимите флажки напротив соответствующих пунктов. Чтобы добавить/исключить все типы информации нажмите кнопку **Отметить все/Снять отметки** соответственно.
3. Для изменения порядка следования столбцов в таблице выберите соответствующий столбец в списке и нажмите на одну из следующих кнопок:

- **Вверх** – для перемещения столбца ближе к началу таблицы (вверх по списку в настройках и левее в таблице объектов);
- **Вниз** – для перемещения столбца ближе к концу таблицы (вниз по списку в настройках и правее в таблице объектов).

4. Для сохранения изменений в настройках нажмите кнопку **ОК**, для закрытия окна без сохранения изменений – кнопку **Отменить**.

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

7.5.2.1. Управление карантином

Действия над объектами в карантине

В окне карантина доступны следующие кнопки управления:

- **Добавить** – добавить файл в карантин. В открывшемся браузере по файловой системе выберите нужный файл;
- **Восстановить** – переместить файл из карантина и восстановить первоначальное местоположение файла. Путь для восстановления файла указан в колонке **Путь** на Рисунке 14. Если путь не указан, пользователю будет предложено выбрать папку для восстановления файла;

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

  В выпадающем меню доступен вариант **Восстановить в – переместить файл** под заданным именем в папку, указанную пользователем.
- **Пересканировать** – сканировать файл из карантина повторно. Если при повторном сканировании файла обнаружится, что он не является зараженным, карантин предложит восстановить данный файл;
- **Удалить** – удалить файл из карантина и из системы.

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

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

7.5.2.2. Настройка свойств карантина

Чтобы настроить свойства Карантина:

1. Нажмите на кнопку **Настройки** в окне карантина.
2. Откроется окно **Свойства карантина**, в котором вы можете изменять следующие параметры:
   - в разделе **Задать размер карантина** вы можете управлять объемом дискового пространства, занимаемого папкой карантина в процентном соотношении относительно общего размера диска (при наличии нескольких логических дисков, данный размер будет рассчитан отдельно для каждого диска, на котором располагаются папки карантина). Значение 100% означает снятие ограничений для максимального размера папки карантина.
   - в разделе **Вид** выберите опцию **Показывать резервные копии**, чтобы отобразить в таблице объектов резервные копии файлов, находящихся в карантине. Резервные копии создаются автоматически при перемещении файлов в карантин. Даже при хранении файлов в карантине бессрочно, их резервные копии сохраняются временно.
3. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

7.6. Дополнительные настройки

Раздел **Дополнительные настройки** позволяет настроить список исключений и параметры архивации зараженных файлов (см. Рисунок 15).

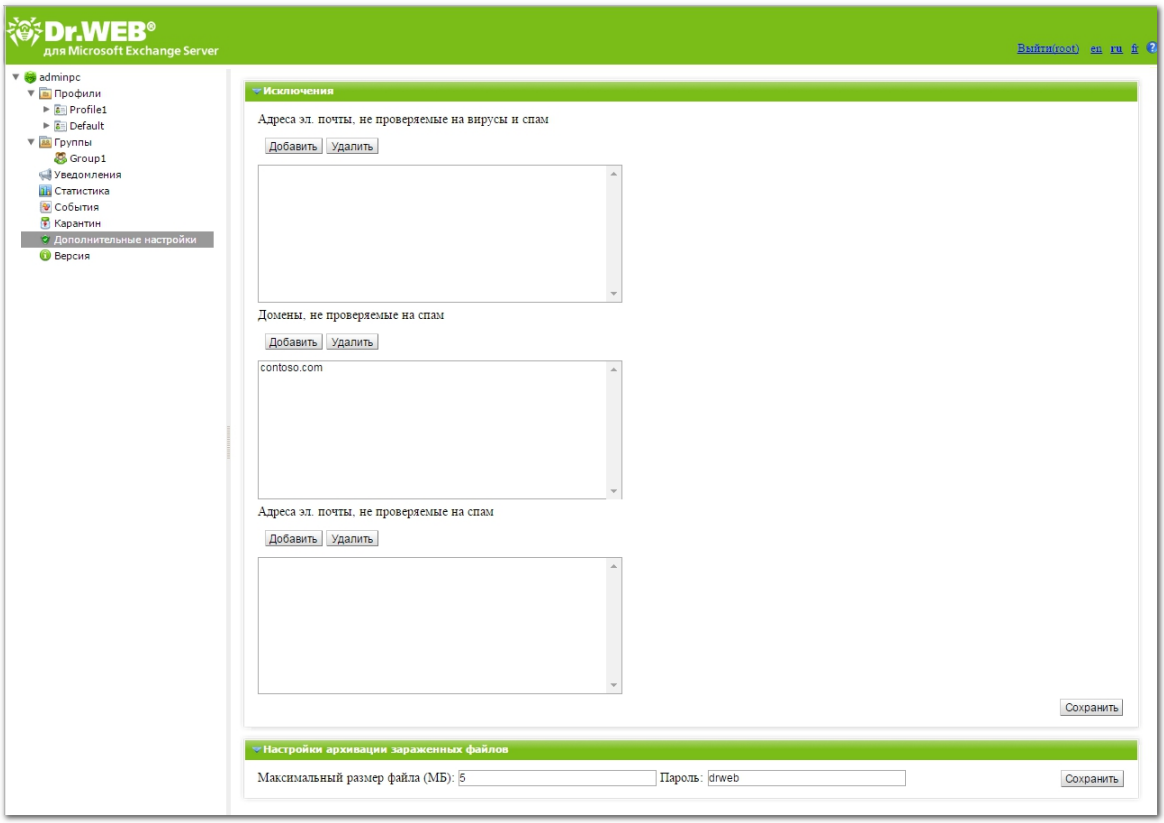

Рисунок 15. Дополнительные настройки

Исключения

Письма от доверенных отправителей можно исключить из проверки на спам и вирусы, добавив их адреса или домены в соответствующих полях раздела **Исключения**. Кроме того, вы можете задать список исключений при помощи консоли Dr.Web CMS Web Console.

Настройки архивации зараженных файлов

Данные настройки распространяются на ZIP-архивы, в которые упаковываются зараженные и подозрительные файлы, если в разделе Сканер для обработки таких файлов было выбрано действие **Архивировать**. В соответствующих полях можно указать максимальный размер файла, который может быть упакован в архив, и пароль для архива.

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, то эти базы требуют периодического обновления. Для этого в приложении реализована система обновления вирусных баз через Интернет. В течение срока действия лицензии модуль обновления регулярно скачивает и устанавливает информацию о новых вирусах и вредоносных программах, а также обновления.

Информация о версии приложения, лицензии, вирусных базах, а также о дате, времени и результате последнего обновления программы находится в области сведений консоли Dr.Web Administrator Web Console **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 Exchange Update Task** выберите пункт **Свойства**.
3. В диалоговом окне **Doctor Web for Exchange 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**.

9. Консоль Dr.Web CMS Web Console

Консоль Dr.Web CMS Web Console (см. Рисунок 16) поддерживается отдельным сервисом Dr.Web CMS Web Console, который, в свою очередь, контролируется управляющим сервисом Dr.Web CMS.

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

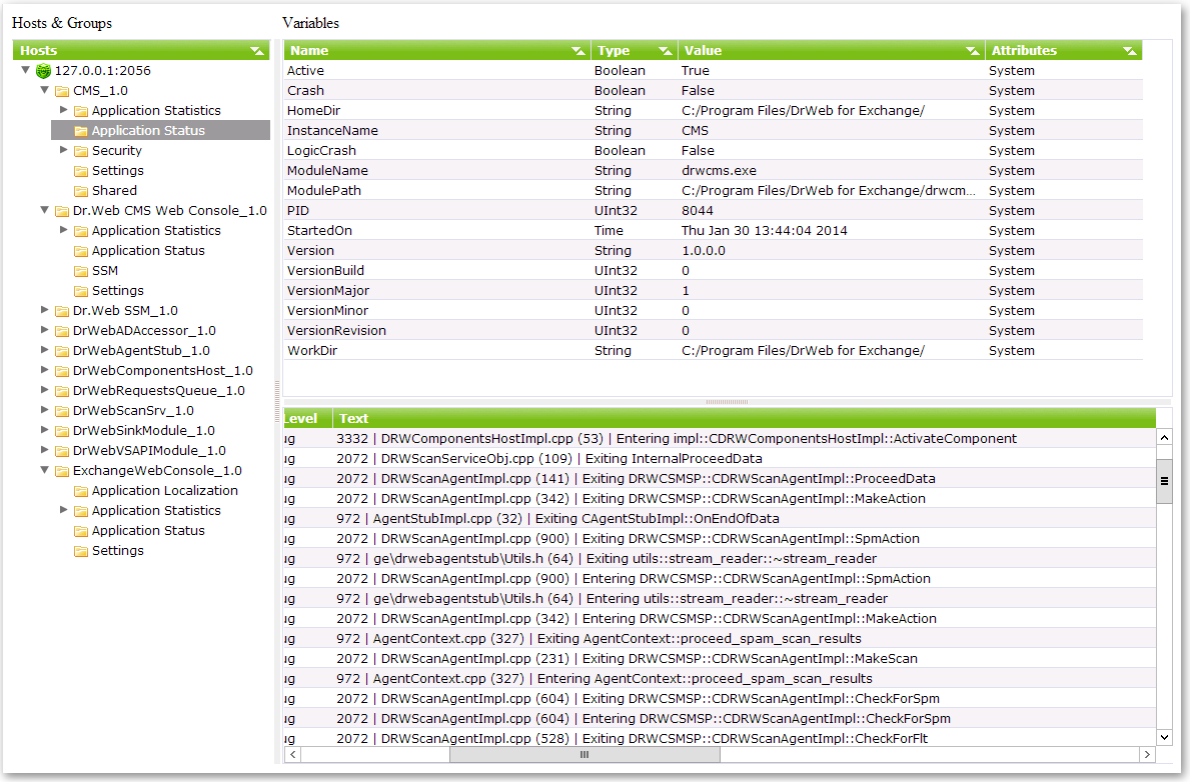

Рисунок 16. Dr.Web CMS Web Console

Запуск Dr.Web CMS Web Console

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

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

где *<Exchange Server address>* – это IP-адрес сервера Exchange.

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

При первом запуске Dr.Web CMS Web Console используйте данные учетной записи по умолчанию: имя пользователя **root**, пароль **drweb**.

Интерфейс

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 трассировку 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 консоли Dr.Web Administrator Web Console или 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 Dr.Web Administrator Web Console;

   1 – доступ к консоли Dr.Web Administrator Web Console без возможности изменения настроек.

Если значение переменной **UserLevel** не задано, администратору будет предоставлен полный доступ к настройкам 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 с кодом возврата **MB_RC_SKIPPED**.

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 AD

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 AD в 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 Административной консоли CMS 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 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 Dr.Web Administrator Web Console управляющего сервера и будет транслироваться сразу на оба сервера.

9.4. Настройка уведомлений об удалении писем с помощью Exchange Web Services

В случае работы в режиме с удалением писем при антивирусной проверке или фильтрации антивирусным агентом получателю не поступает никаких данных о письме, кроме соответствующей записи в журналах событий сервера. Для такого режима работы можно дополнительно настроить отправку через протокол EWS (Exchange Web Services) почтовых уведомлений на адрес, заданный параметром **OWSNotificationEmail**. Данные уведомления содержат информацию об отправителях, списке получателей и темах удаленных писем, но в них отсутствуют данные о теле писем и вложениях.

EWS (Exchange Web Services) размещается на серверах, имеющих роль Client Access (CAS), и выступает посредником между клиентскими запросами и внутренней структурой сервера Exchange.

Настройка уведомлений об удалении писем с помощью Exchange Web Services осуществляется в ветке настроек **DrWebAgentStub_1.0** -> **Application Settings** Административной консоли CMS путем задания следующих переменных:

- **OWSUrl**. Задает сервер, на котором расположен EWS. По умолчанию установлено значение localhost, но в общем случае в качестве значения данного параметра может быть указан IP-адрес любого другого сервера с EWS.
- **OWSAdministrator**, **OWSPassword**, **OWSDomain**. Задают параметры доступа (имя пользователя с правами доступа к EWS, его пароль и имя домена) к почтовому ящику, задаваемому параметром **OWSOutgoingEmail**.
- **OWSNotificationEmail**. Электронный адрес, на который будут приходить уведомления об удалении писем.
- **OWSOutgoingEmail**. Электронный адрес, от имени которого будут приходить уведомления об удалении писем.

Заданные настройки передаются антивирусному агенту один раз при запуске службы транспорта, и отправка уведомлений с помощью EWS не включается, если хотя бы одна из настроек будет пустой строкой.

При каждом удалении письма антивирусный транспортный агент будет пытаться установить соединение с сервером, заданным параметром **OWSUrl**. В случае, если соединение установить не удалось, в журнале событий операционной системы (Event Log) фиксируется предупреждение **444** с указанием причины невозможности отправки уведомления.

9.5. Действия агента антиспама при удалении или блокировке письма

Если письмо удаляется как спам или блокируется как несоответствующее правилам фильтрации, транспортный агент антиспама может либо разорвать соединение с клиентом, либо сформировать ответ **RejectMessage**.

Чтобы определить, какое действие будет выполняться при удалении или блокировке письма:

1. В дереве хостов и групп выберите группу **AgentStub** ->**Application Settings**.
2. В поле **Value** установите значение для переменной **Disconnect**:
   - **false**. Отправитель получит в ответ **RejectMessage** следующего содержания: **Dr.Web AntiSpam Agent: Message was rejected as spam**. Данное действие выполняется по умолчанию.
   - **true**. SMTP-соединение с клиентом будет разорвано.

9.6. Изменение режима лицензирования

Изменение способа лицензирования необходимо при переходе к работе в режиме централизованной защиты или при выходе из этого режима.

Для изменения режима лицензирования

1. В дереве хостов и групп выберите группу **DrWebScanSrv_1.0** -> **Application Settings**.
2. В поле **Value** установите значение для переменной **LicenseMode**:

   0 – для работы Dr.Web необходимо получить ключевой файл (по умолчанию);

   1 – для работы Dr.Web используется ключевой файл с сервера централизованной защиты.
3. После переключения режима перезапустите службу Dr.Web for MSP Scanning Service.

9.7. 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.
   - **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 пропущены.

9.8. Определение принадлежности письма к спаму

Компонент Антиспам присваивает каждому письму целое число (*score*). Данная величина позволяет определить, является ли проверяемое письмо спамом.

Чтобы изменить пороговые значения для определения принадлежности письма к той или иной группе (**Точно спам**, **Возможно спам** или **Маловероятно, что спам**), выполните следующие действия:

1. В дереве хостов и групп выберите группу **DrWebScanSrv_1.0** -> **Application Settings** -> **Profiles** -> **%Profile name%** -> **Antispam**.
2. Установите значения для следующих переменных:

Для корректной работы Антиспама не рекомендуется изменять значения по умолчанию для переменных **AntispamDefaultScoreMin** и **AntispamExactlyScoreMax**.

- **AntispamDefaultScoreMin**. Наименьшее значение величины *score*, которое определяет принадлежность письма к группе **Маловероятно, что спам**. Значение по умолчанию: 1.
- **AntispamDefaultScoreMax**. Наибольшее значение величины *score*, которое определяет принадлежность письма к группе **Маловероятно, что спам**. Значение по умолчанию: 199.
- **AntispamProbablyScoreMin**. Наименьшее значение величины *score*, которое определяет принадлежность письма к группе **Возможно спам**. Значение по умолчанию: 200.
- **AntispamProbablyScoreMax**. Наибольшее значение величины *score*, которое определяет принадлежность письма к группе **Возможно спам**. Значение по умолчанию: 4999.
- **AntispamExactlyScoreMin**. Наименьшее значение величины *score*, которое определяет принадлежность письма к группе **Точно спам**. Значение по умолчанию: 5000.
- **AntispamExactlyScoreMax**. Наибольшее значение величины *score*, которое определяет принадлежность письма к группе **Точно спам**. Значение по умолчанию: 2147483647.

9.9. Исключение писем из проверки

Письма от доверенных отправителей можно исключить из проверки на спам и вирусы, указав их адреса или домены в соответствующих переменных.

1. В дереве хостов и групп выберите группу **DrWebAgentStub_1.0** -> **Application Settings**.
2. Установите значения для следующих переменных:

Значения переменных устанавливаются через «;» без пробела. Пример: **example1@mail.com;example2@mail.com**.

Список исключений можно также настроить в разделе Дополнительные настройки консоли Dr.Web Administrator Web Console.

- **TrustedDomains**. Список доменов, которые будут исключены из проверки на спам. В название домена должна входить только часть адреса электронной почты, указанная после знака @. Пример: **domain.org;mail.com;drweb.com**.
- **SpamTrustedEmails**. Список адресов электронной почты, которые будут исключены из проверки на спам.
- **TrustedEmails**. Список адресов электронной почты, которые будут исключены из проверки на спам и вирусы. Эти же адреса необходимо прописать в переменной **TrustedEmails** из группы **DrWebVSAPIModule_1.0** -> **Application Settings**.

9.10. 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 CMS.

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

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).

  События Dr.Web записываются в журналы **Приложение** и **Doctor Web**.

Просмотр журнала регистрации операционной системы

1. Чтобы просмотреть журнал регистрации событий операционной системы, откройте **Панель управления** операционной системы.
2. Выберите **Администрирование**, а затем выберите **Просмотр Событий**.
3. В левой части окна **Просмотр Событий** выберите **Приложение** (или **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 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 **Приложение**.

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

10.2. Текстовый журнал программы установки

Файлы регистрации событий установки **setup-starter.log** и **exchange-setup.log** могут быть найдены по переменной окружения %ProgramData% (при ее вызове в консоли запуска программ **Пуск** -> **Выполнить**) в папке %ProgramData%\Doctor Web\Logs.

10.3. Журнал событий CMS

Список событий сохраняется управляющим сервисом Dr.Web CMS в отдельную базу данных cmstracedb, находящуюся в папке установки приложения %Program Files%\DrWeb for Exchange. Управляющий сервис регистрирует различные типы событий и позволяет выбрать степень детализации для каждого приложения-подписчиков службы Dr.Web CMS.

При необходимости, вы можете удалить базу данных cmstracedb.

Список событий отображается в окне сообщений трассировки консоли Dr.Web CMS Web Console.

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.

Список событий сохраняется управляющим сервисом в отдельную базу данных.

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

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 %Program Files%\DrWeb for Exchange:

1. Перед удалением базы данных рекомендуется снять нагрузку с сервера одним из следующих способов:
   - остановите службу транспорта, в которую установлены транспортные агенты, и службу Microsoft Exchange Information Store, если установлен модуль VSAPI;
   - если по каким-либо причинам остановка сервера не допускается, отключите транспортные агенты и перезапустите службу транспорта. Если же установлен модуль VSAPI, установите значение **0** для параметра **Enabled**, указанное в разделе реестра `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan]`, и перезапустите службу Microsoft Exchange Information Store.
2. Запустите командную консоль (cmd) от имени администратора.
3. 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"
   ```
4. Удалите файл **cmstracedb**, находящийся в папке установки приложения %Program Files %\DrWeb for Exchange.
5. Запустите службы приложения в указанном порядке:

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

`net start "Dr.Web SSM"`

6. 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:

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

11.1. Проверка установки

При работе с Windows Server 2003 Dr.Web должен быть установлен в папки:

- C:\Documents and Settings\All Users\Application Data\Doctor Web;
- C:\Program Files\Common Files\Doctor Web;
- C:\Program Files\DrWeb for Exchange.

При работе с Windows Server 2008 и выше Dr.Web должен быть установлен в папки:

- C:\ProgramData\Doctor Web;
- C:\Program Files\DrWeb for Exchange;
- C:\Program Files\Common Files\Doctor Web.

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.

Убедитесь, что запущены следующие локальные сервисы:

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

Кроме того, если Dr.Web установлен корректно, вы можете увидеть в результате выполнения команды `get-transportagent` в консоли Exchange PowerShell следующие агенты:

- Dr.Web AntiSpam Agent;
- Dr.Web AntiVirus Agent.

11.2. Проверка модуля обновления

Модуль обновления **drwupsrv.exe** автоматически запускается после установки Dr.Web. Он загружает последние версии антивирусного ядра **drweb32.dll** и ядра Антиспама **vrcpp.dll**, а также обновляет вирусные базы.

Чтобы убедиться, что обновление прошло успешно:

1. В зависимости от версии операционной системы выполните команду **Tasks**, чтобы открыть папку C:\WINDOWS\Tasks или откройте **Планировщик заданий** Windows.
2. Проверьте наличие задания Dr.Web в открывшейся папке (для правильно отработавшего задания код возврата в столбце **Последний результат** должен быть **0x0**).
3. Откройте файл журнала событий модуля обновления %AllUsersProfile%\Application Data\Doctor Web\Logs\dwupdater.log 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.

Чтобы создать тестовый файл EICAR:

- Откройте Блокнот и скопируйте в него следующую строку:

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

- Сохраните файл с расширением **.com** (вы можете использовать любое имя, например, **eicar.com**), прикрепите его 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 Exchange. Имя вируса: EICAR Test File (NOT a Virus!).
  ```

Помимо этого, Dr.Web отправит уведомление с таким же текстом на адрес администратора, указанный во время установки.

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. Настройки антивирусного сканирования Microsoft Exchange Server

Настройки антивирусного сканирования на основе VSAPI осуществляются с помощью набора ключей реестра и могут быть разделены на следующие типы:

- общие настройки;
- настройки базы данных;
- сканирование транспорта SMTP.

Приведенные ниже настройки антивирусного сканирования доступны для Microsoft Exchange Server 2003, 2007 и 2010.

Общие настройки

Общие настройки используются по умолчанию для всех почтовых хранилищ на сервере.

Сканирование при доступе

Ключ реестра:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS
\VirusScan]
"Enabled"=dword:00000001
```

Данная настройка обеспечивает включение антивирусной проверки для всех почтовых хранилищ. Сканирование будет осуществляться всякий раз при обращении клиента к письму.

Фоновое сканирование

Ключ реестра:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS
\VirusScan]
"BackgroundScanning"=dword:00000001
```

Данная настройка отвечает за включение фонового сканирования. Фоновое сканирование подразумевает создание отдельного потока (thread), в котором происходит сканирование всех писем для данного почтового хранилища. Включение фонового сканирования может отрицательно сказаться на производительности почтового сервера.

Упреждающее сканирование

Ключ реестра:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS
\VirusScan]

"ProactiveScanning"=dword:00000001
```

Данная настройка включает упреждающее сканирование. В этом случае происходит проверка всех писем сразу после того, как они попадают в данное почтовое хранилище. При этом письма с неизмененными штампами времени (TimeStamp), прошедшие упреждающее сканирование, не проверяются повторно при поступлении запроса письма от клиента.

Отключение проверки исходящих сообщений

Ключ реестра:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS
\VirusScan

"TransportExclusion"=reg_dword:00000000
```

Данная настройка позволяет отключить/включить (при выборе значения 1 или 0 соответственно) проверку на наличие вредоносных программ исходящих сообщений при их поступлении в транспортную систему из почтового хранилища. По умолчанию такая проверка включена.

Ограничение числа потоков для интерфейса антивирусного сканирования

Число потоков для интерфейса антивирусного сканирования VSAPI 2.6 определяется по умолчанию настройками Exchange Server, однако, его можно отрегулировать вручную путем создания переменной **ScanningThreads** в указанном ниже разделе реестра.

Ключ реестра:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIS
\VirusScan

"ScanningThreads"=reg_dword
```

Данный параметр определяет максимальное число потоков, создаваемых для сканирования. Изменение данного параметра влияет на сканирование при доступе и упреждающее сканирование, но не влияет на фоновое сканирование, для которого всегда используется один поток на базу данных.

По умолчанию значение данной переменной считается равным 2 *<*количество процессоров*> + 1.

Настройки базы данных

С помощью настроек данного типа можно задать параметры сканирования для каждой почтовой базы данных, имеющейся на почтовом сервере. Настройки записываются в реестр по следующему пути:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS
\<Server-Name>\<ID Base>],
```

где *<Server-Name>* – имя сервера, *<ID Base>* – идентификатор почтовой базы, например, `Private-ae39732e-fb7f-426d-98a0-298f3f014c77`.

Параметры:

- `"VirusScanEnabled"=dword:00000001` – включение антивирусного сканирования для указанной базы данных;
- `"VirusScanBackgroundScanning"=dword:00000001` – включение фонового сканирования для указанной базы данных;
- `"VirusScanProactiveScanning"=dword:00000001` – включение упреждающего сканирования для указанной базы данных.

Сканирование транспорта SMTP

Настройки сканирования транспорта доступны только для сервера Exchange 2003.

Ключ реестра:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\TransportAVAPI\]
"Enabled"=dword:00000001
```

Транспортное сканирование по умолчанию выключено. Вы можете включить его на последнем шаге установки программы. В результате первое антивирусное сканирование письма будет выполнено на SMTP-событие **OnSubmission** постановки в очередь обработки сообщений, т.е. на уровне транспорта. Повторное сканирование будет произведено уже на уровне хранилища информации Exchange при запросе письма клиентом.

12.2. Ручная регистрация транспортных агентов

В некоторых случаях, например, при возникновении ошибок в процессе регистрации транспортных агентов во время установки Dr.Web, вам может понадобиться выполнить их регистрацию вручную. Для этого выполните следующие команды в консоли Exchange Management Shell:

```
Install-TransportAgent -Name "Dr.Web AntiSpam Agent" -
TransportAgentFactory "DRWTransportAgent.AntiSpamAgentFactory" -
AssemblyPath "C:\Program Files\DrWeb for Exchange
\DRWTransportAgent.dll"

Install-TransportAgent -Name "Dr.Web AntiVirus Agent" -
TransportAgentFactory "DRWTransportAgent.AntiVirusAgentFactory" -
AssemblyPath "C:\Program Files\DrWeb for Exchange
\DRWTransportAgent.dll"

Enable-TransportAgent "Dr.Web AntiSpam Agent"

Enable-TransportAgent "Dr.Web AntiVirus Agent"
```

При копировании данных команд из руководства обязательно удалите переносы строк.

Чтобы отменить регистрацию транспортных агентов, выполните следующие команды в консоли Exchange Management Shell:

```
Uninstall-TransportAgent "Dr.Web AntiSpam Agent"

Uninstall-TransportAgent "Dr.Web AntiVirus Agent"
```

12.3. Отключение Dr.Web от почтового сервера вручную

При возникновении сбоев при установке или во время использования Dr.Web вы можете отключить его от почтового сервера. Для этого выполните следующие действия:

- Если установлены транспортные агенты:

  
  Транспортные агенты доступны для Microsoft Exchange Sever 2007, 2010, 2013 и 2016.

  - В консоли Exchange Management Shell выполните команду `Get-Transportagent` (если агенты были дополнительно установлены в транспортные службы, в параметре `-TransportService` необходимо уточнить службу). Подробную информацию о данной команде см. по ссылке: http://technet.microsoft.com/ru-ru/library/bb123536(v=exchg.150).aspx.
  - В консоли Exchange Management Shell будет выведен список агентов, зарегистрированных в указанной службе транспорта. Найдите среди них те, что относятся к Dr.Web (т.е. содержат префикс **Dr.Web** в имени), и для каждого из них скопируйте название в команду `Disable-TransportAgent` <*имя агента*> (при необходимости, укажите дополнительно параметр `-TransportService`). Подробную информацию о данной команде см. по ссылке: http://technet.microsoft.com/ru-RU/library/aa997880(v=exchg.150).aspx.
  - Перезапустите службу транспорта Microsoft Exchange Transport (а также Microsoft Exchange Frontend Transport, если требуется). Транспортные агенты будут отключены от служб транспорта.
  - Повторно выполните команду `Get-Transportagent` и убедитесь, что указанные агенты получили статус **Disable**.

  Таким образом, приложение будет отключено от транспортного конвейера.

- Если установлен модуль VSAPI:

  
  Модуль VSAPI доступен для Microsoft Exchange Sever 2003, 2007 и 2010.

  - Проверьте значение параметра `Enabled`, указанное в разделе реестра `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan]`: если `"Enabled"=dword:00000001`, необходимо обнулить его: `"Enabled"=dword:00000000`. Если такого раздела реестра нет, или в нем уже установлено нулевое значение для указанного параметра, модуль VSAPI уже выключен.
  - Перезапустите службу Microsoft Exchange Information Store. Модуль антивирусного сканирования будет отключен от указанной службы.

  Теперь приложение отключено от менеджера почтовых хранилищ.

- Если установлен модуль DrWebSink:

Модуль DrWebSink доступен для Microsoft Exchange Sever 2003.

- Запустите командную консоль (cmd) от имени администратора и выполните следующую команду:

```
regsvr32 /u "C:\Program Files\DrWeb for Exchange\DrWebSink.dll"
```

- Перезапустите Microsoft Internet Information Services (IIS).

Будучи отключенным от почтового сервера, приложение никак не влияет на его работу.

12.4. Удаление Dr.Web вручную

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

1. Отключите Dr.Web от почтового сервера.
2. Удалите регистрацию транспортных агентов, выполнив следующие команды в консоли Exchange Management Shell:

```
Uninstall-TransportAgent "Dr.Web AntiSpam Agent"
Uninstall-TransportAgent "Dr.Web AntiVirus Agent"
```

3. Запустите командную консоль (cmd) от имени администратора.
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"
```

Для удаления службы Dr.Web Scanning Engine потребуется утилита **drw_remover.exe**, которую вы можете получить, обратившись в службу технической поддержки компании «Доктор Веб».

6. Удалите следующие папки:

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

12.5. 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.

12.5.1. 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

Тип данных	Комментарий
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.

12.5.2. Контроль приложений

Для контроля приложения с помощью CMS происходит регистрация его имени и версии в базе управляющего сервиса. Сервис Dr.Web CMS присваивает приложению уникальное имя, состоящее из имени приложения и версии. После этого сервис создает в базе данных группу с именем зарегистрированного приложения. По умолчанию в этой группе создаются служебные подгруппы с именами **Application Status** и **Settings**. Во время работы приложения управляющий сервис ведет сбор статистики по протоколам взаимодействия. Статистика ведется в группе **Application Statistics/ Connections**, в ее подгруппах **MB** и **MS** ведется статистика взаимодействия по протоколам. Используя данные статистики, можно оценить степень нагрузки на эти сервисы и приложения.

Группа Application Status

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

Переменная (в скобках указан тип переменной)	Комментарий
Active (Boolean)	Обозначает, запущено ли сейчас приложение. Значение **true** означает, что приложение запущено.

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

Группа Settings

Данная группа содержит базовые настройки зарегистрированного приложения.

12.5.3. 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.

12.5.4. Администрирование

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

Изменение значений переменных

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

Сброс статистики

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

Ограничения при работе с переменными

При работе с переменными вводятся следующие ограничения:

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

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

Безопасность

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

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

12.5.5. Подключение к серверам

Административная консоль CMS 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 Административной консоли 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 такой группы создаются три переменные:

- **Address** содержит адрес подключения к хосту;
- **Login** содержит имя пользователя;

- **Password** содержит пароль для подключения к хосту.

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

При последующих запусках Административная консоль CMS автоматически подключается к добавленным хостам. Для удаления добавленного хоста следует удалить группу с настройками подключения к данному хосту из группы настроек Административной консоли CMS по пути **/Dr.Web CMS Web Console_1.0/Application Settings/Hosts**.

12.6. Служба Dr.Web SSM

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

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

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

Переменная (в скобках указан тип переменной)	Комментарий
Enabled (Boolean)	Обозначает, запущено ли включение/выключение SSM-контроля.
Run (Boolean)	Позволяет запустить/остановить приложение
KeepAlive (Int32)	Обозначает тип поддержания активности приложения: • 0 – приложение отключено; • 1 – приложение включено; • 2 – форсированное, т.е. приложение будет включено даже в случае его корректной остановки.
StartType (Int32)	Обозначает способ запуска приложения: • 0 – как сервис Windows; • 1 – как приложение CService; • 2 – запуск с помощью скрипта.
StartScript (String)	Содержит скрипт для запуска приложения
StopScript (String)	Содержит скрипт для остановки приложения
Restart (Boolean)	Выполняет перезапуск приложения
Timeout (UInt32)	Обозначает время ожидания реакции приложения (в секундах). По умолчанию установлено значение 10 сек.

Переменная (в скобках указан тип переменной)	Комментарий
ServiceName (String)	Обозначает имя сервиса в Windows Service Manager. По умолчанию используется значение переменной "/Application Status/InstanceName".

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

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

12.7. 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 Exchange 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	Тип обновления: • update-revision - обновление компонентов в пределах текущей ревизии.
--disable-postupdate	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	Дополнительные параметры, передаваемые для скрипта.

Параметр	Описание
	Формат: <имя>=<значение>. По умолчанию установлено значение "plugin=exchange".
-n [--component] arg	Перечень компонентов, которые необходимо обновить: • updater - файл drwupsrv.exe; • antispam - файл vrcpp.dll; • scan-engine - файлы dwengine.exe, ccsdk.dll, dwsewsc.exe, dwinctl.dll, dwarkdaemon.exe, arkdb.bin, dwqrui.exe, dwarkapi.dll; • av-engine - вирусные базы (файлы с расширением *.vdb); • exchange-plugin-setup - файл exchange-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=exchange" -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.

Параметр	Описание
	Формат: <имя>=<значение>. По умолчанию установлено значение "plugin=exchange".

Пример команды - **с postupdate**:

```
-c postupdate --verbosity=debug --interactive --
param="plugin=exchange"
```

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

12.8. Работа в режиме централизованной защиты

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

Взаимодействие компонентов антивирусной сети

Решения компании «Доктор Веб» по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (см. Рисунок 17).

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

Обновление и конфигурация локальных компонентов производится через *центральный сервер*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты. Объем трафика между защищенными компьютерами и антивирусным сервером может быть весьма значительным, поэтому предусматривается возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.

Рисунок 17. Логическая структура антивирусной сети

Все необходимые обновления загружаются на сервер централизованной защиты с серверов обновлений Dr.Web.

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

Работа Dr.Web в режиме централизованной защиты

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

Dr.Web версии 11.0 несовместим с Dr.Web Agent версии 6.

Если Dr.Web Agent был установлен после установки Dr.Web, выполните следующее:

1. В планировщике заданий Windows отключите задачу **Doctor Web for Exchange Update Task**.
2. В Административной консоли CMS измените режим лицензирования: выберите вариант использования лицензии с сервера централизованной защиты (см. Изменение режима лицензирования).

Далее запустите обновление из консоли на сервере централизованной защиты и убедитесь, что обновление прошло успешно.

Лицензирование

В режиме централизованной защиты используется лицензионный ключевой файл Dr.Web, зарегистрированный для данной станции в антивирусной сети. Если на этапе установки был выбран вариант использования лицензии с сервера централизованной защиты, то при запуске Microsoft Exchange Server с установленным Dr.Web будет предпринята попытка использовать лицензионный ключ для данной станции в антивирусной сети. Если ключ недействителен, то антивирусная проверка производиться не будет. Если при установке был выбран другой вариант получения лицензии, необходимо изменить режим лицензирования при помощи консоли CMS (1).

Обновление

Обновление вирусных баз и антивирусного ядра осуществляется из репозитория Центра Управления Dr.Web. Это позволяет отключить стандартный модуль обновления Dr.Web Updater, запускаемый по расписанию. В этом случае обновление компонентов будет выполняться согласно расписанию Центра Управления Dr.Web и из его репозитория.

Действия после удаления Dr.Web Agent

Если Dr.Web Agent был удален, для дальнейшей корректной работы Dr.Web выполните следующие действия:

1. В планировщике заданий Windows добавьте задание на обновление Dr.Web. Для этого:
   - Откройте планировщик заданий Windows.

- Создайте задачу с наименованием **Doctor Web for Exchange Update Task**.
- На вкладке **Общие** мастера создания задачи установите переключатель **Выполнять для всех пользователей** и флажок **Выполнить с наивысшими правами**. В списке **Настроить для** выберите вариант Windows Server 2003, Windows XP или Windows 2000.
- На вкладке **Тригеры** установите временной интервал выполнения задачи.
- На вкладке **Действия** создайте действие **Запуск программы** и выберите программу ***<путь до папки установки Dr.Web>*\drwupsrv.bat**.
- Снимите все установленные по умолчанию флажки на вкладке **Условия**.

2. Измените режим лицензирования. Необходимо выбрать вариант лицензирования путем получения ключевого файла (0).

Предметный указатель

Предметный указатель

Предметный указатель

Т

У

Ф

Ц

Э