Dr.WEB®

для MIMEsweeper

Защити созданное

Руководство администратора

Dr.Web для MIMEsweeper
Версия 6.0.1
Руководство администратора
07.02.2013

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

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

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

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Глава 1. Введение

Благодарим вас за приобретение программы **Dr.Web для MIMEsweeper**. Данный антивирусный продукт представляет собой приложение, подключаемое к системе контентной фильтрации ClearSwift MIMEsweeper в качестве одной из политик проверки содержимого почтовых сообщений.

В программе применены наиболее передовые разработки и технологии **«Доктор Веб»**, которые позволяют обнаруживать и обезвреживать вредоносные объекты, представляющие угрозу функционированию почтовых серверов и информационной безопасности адресатов.

Программа проверяет все почтовые сообщения, получаемые контентным фильтром, на вирусы, программы дозвона, рекламные программы, потенциально опасные программы, программы взлома и программы-шутки. Если **Dr.Web для MIMEsweeper** работает с лицензией «Антивирус+Антиспам» (и соответствующим лицензионным ключевым файлом), то она также осуществляет проверку корреспонденции на спам с помощью спам-фильтра VadeRetro. При обнаружении угроз безопасности приложение классифицирует нежелательную почту согласно настройкам ClearSwift MIMEsweeper и по возможности обезвреживает обнаруженные вредоносные программы.

Основные функции программы

Dr.Web для MIMEsweeper предоставляет вам следующие преимущества:

- установку антивируса на те же компьютеры, где установлен контентный фильтр;
- подключение антивируса в качестве сценария фильтрации первого типа (классификация контентного сканера), рекомендованный компанией ClearSwift;
- проверку почтовых сообщений, и в том числе архивов во вложениях, до их обработки почтовым сервером;
- обнаружение вредоносного программного обеспечения;
- лечение зараженных объектов;
- выявление и отсеивание спама;
- высокую скорость проверки;
- регулярное автоматическое обновление антивирусных баз.

Настоящее руководство призвано помочь администраторам почтовых серверов, использующим контентный фильтр ClearSwift MIMEsweeper for SMTP, установить и настроить программу **Dr.Web для MIMEsweeper**, а также ознакомиться с ее основными функциями. Дополнительную информацию о сценариях контентных фильтров ClearSwift можно найти на официальном сайте компании по адресу http://www.clearswift.com/products/msw/smtp/eval/avscenario.aspx.

Используемые обозначения

В данном руководстве применены следующие условные обозначения (табл. 1).

Таблица 1. Условные обозначения.

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

Техническая поддержка

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

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

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

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

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

Глава 2. Лицензирование

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

Лицензионный ключевой файл

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

- период, в течение которого разрешено использование программы;
- перечень компонентов, разрешенных к использованию;
- разрешение или запрет на использование спам-фильтра VadeRetro;
- количество пользователей, защищаемых программой.

Ключевой файл программы **Dr.Web для MIMEsweeper** является действительным при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- ключ распространяется на все используемые программой модули;
- ключ разрешен к использованию на почтовых серверах;
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится недействительным, при этом программа перестает обезвреживать вредоносные программы и пропускает почтовые сообщения без изменений. Факт нарушения корректности ключевого файла записывается в журнал регистрации событий операционной системы.

Детальную информацию о регистрации событий вы можете найти в главе Регистрация событий.

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.

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 при помощи средств операционной системы или архиватора формата ZIP (например, WinZip или Pkunzip) и поместите его в каталог установки программы **Dr.Web для MIMEsweeper** (обычно %ProgramFiles%\DrWeb for MIMEsweeper).

В некоторых случаях для ознакомления с программой можно получить *демонстрационный ключевой файл*. Такие ключевые файлы обеспечивают полную функциональность основных антивирусных компонентов, но имеют ограниченный срок действия и не предполагают оказание поддержки пользователю.

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

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

Обновление лицензии

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

Замена ключевого файла

1. Чтобы обновить лицензию, выполните одно из следующих действий:
   - замените имеющийся ключевой файл в каталоге установки программы (обычно, %ProgramFiles%\DrWeb for MIMEsweeper) новым ключевым файлом;
   - при измененном пути к ключевому файлу, замените имеющийся ключевой файл в заданном каталоге хранения новым ключевым файлом.
2. Приложение автоматически переключится на использование нового ключевого файла.

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

Использование ключевого файла

При работе программы ключевой файл по умолчанию должен находиться в каталоге установки. Программа регулярно проверяет наличие и корректность ключевого файла. Во избежание порчи ключа, не модифицируйте ключевой файл.

При установке **Dr.Web для MIMEsweeper** ключевой файл копируется в каталог установки приложения (обычно, % ProgramFiles%\DrWeb for MIMEsweeper). Мастер установки автоматически регистрирует ключевой файл в реестре операционной системы. Вы можете изменить путь к ключевому файлу.

Изменение пути к ключевому файлу

Данную операцию рекомендуется выполнять только администратору или опытному пользователю системы. Неверные действия при изменении реестра могут серьезно повредить систему. Специалисты компании Microsoft рекомендуют перед изменением реестра создать резервную копию всех важных данных, имеющихся на компьютере.

1. Откройте редактор реестра операционной системы.
2. Найдите ветку HKEY_LOCAL_MACHINE\SOFTWARE\Doctor Web\DrWeb for MIMEsweeper\License.
3. В контекстном меню ключа FILE выберите **Изменить**.
4. Введите путь к файлу лицензии.
5. Нажмите кнопку **ОК** и выйдите из редактора реестра.
6. Чтобы перезагрузить **Dr.Web для MIMEsweeper**, откройте редактор политик MIMEsweeper for SMTP и на панели инструментов нажмите кнопку **Save MIMEsweeper Policy**  .

Программа **Dr.Web для MIMEsweeper** готова к использованию ключевого файла, расположенного по указанному адресу.

Определение параметров лицензирования

Лицензионный ключевой файл регулирует использование программы **Dr.Web для MIMEsweeper**.

Определение параметров лицензирования

Ключевой файл имеет формат, защищенный от редактирования. Редактирование файла делает его недействительным. Чтобы избежать порчи ключевого файла, не следует сохранять его при закрытии текстового редактора.

1. Чтобы определить параметры лицензирования, записанные в вашем ключевой файле, откройте файл для просмотра (например, Блокнот).
2. Вы можете проверить следующие параметры лицензирования (табл. 2).

Таблица 2. Параметры ключевого файла.

Параметр	Комментарий
Группа `[Key]`, параметр `Applications`	Указывает компоненты программы, которые разрешено использовать владельцу лицензии.
Группа `[Key]`, параметр `Expires`	Указывает срок действия лицензионного ключа в формате Год-Месяц-День.
Группа `[User]`, параметр `Name`	Указывает регистрационное имя владельца лицензии.

Параметр	Комментарий
Группа [Settings], параметр MailServer	Указывает не разрешение (Yes) или запрет (No) использования ключа на почтовых серверах.
Группа [Settings], параметр SpamFilter	Указывает на разрешение (Yes) или запрет (No) использования спам-фильтра VadeRetro. Спам-фильтр доступен только для лицензии «Антивирус+Антиспам».
Группа [Settings], параметр EmailAddresses	Указывает количество пользователей, защищаемых программой.

3. Закройте файл, не сохраняя изменений.

Глава 3. Установка и удаление программы

Dr.Web для MIMEsweeper устанавливается на те же компьютеры, где установлен контентный фильтр ClearSwift MIMEsweeper for SMTP, и работает как сценарий фильтрации типа 1 (классификация контентного сканера), рекомендованный компанией ClearSwift.

Дополнительную информацию о сценариях контентных фильтров ClearSwift можно найти на официальном сайте компании по адресу http://www.clearswift.com/products/msw/smtp/eval/avscenario.aspx.

Системные требования

Компьютер, на который производится установка программы **Dr.Web для MIMEsweeper**, должен удовлетворять следующим системным требованиям (табл. 3).

Таблица 3. Системные требования.

Компонент	Требование
Место на жестком диске	Не менее 60 МБ свободного дискового пространства.
Операционная система	Одна из следующих: • Microsoft® Windows® 2000 (Professional Edition, Server, Advanced Server или Datacenter Server) с пакетом обновлений SP4 и Update Rollup 1; • Microsoft® Windows Server® 2003 (Standard Edition, Enterprise Edition или Datacenter Edition); • Microsoft® Windows Server® 2008 (Standard Edition, Enterprise Edition или Datacenter Edition);

Компонент	Требование
	• Microsoft® Windows Server® 2008 R2. Поддерживаются 32- и 64-битные версии операционных систем.
Почтовый контентный фильтр	ClearSwift MIMEsweeper for SMTP 5.2 или более поздняя версия.
Прочее	Подключение к сети Интернет для обновления антивирусных баз данных программы.

Настоящие системные требования относятся только к программе **Dr.Web для MIMEsweeper**. Требования к контентному фильтру содержатся в документации ClearSwift MIMEsweeper for SMTP. **Dr.Web для MIMEsweeper** может работать на тех же серверах, на которых установлен контентный фильтр.

Установка программы

Перед установкой программы удостоверьтесь, что компьютер удовлетворяет минимальным системным требованиям.

Для установки **Dr.Web для MIMEsweeper** необходимо иметь права администратора.

Единый сервер политик

Установка программы

1. Скопируйте следующие файлы на компьютер, где работает сервер политик контентного фильтра ClearSwift MIMEsweeper for SMTP Policy Server:
   - установочный файл программы **drweb-mimesweeper-600-windows-nt.exe.**;
   - лицензионный ключевой файл.

2. Запустите файл **drweb-mimesweeper-600-windows-nt.exe**.
3. Откроется окно мастера установки. Нажмите кнопку **Далее**.
4. На шаге **Лицензионное соглашение** прочитайте и примите лицензионное соглашение и нажмите кнопку **Далее**.
5. На шаге **Лицензионный ключевой файл** выполните одно из следующих действий:
   - введите путь к лицензионному ключевому файлу;
   - нажмите кнопку **Обзор**, чтобы открыть стандартное диалоговое окно **Открытие файла**, и затем выберите или введите имя файла с ключом.

   Установка программы невозможна без корректного лицензионного ключа. Для получения ключа с официального сайта компании **«Доктор Веб»** нажмите кнопку **Получить ключ**.

   Нажмите кнопку **Далее**.
6. При подключении к сети Интернет через прокси-сервер, на шаге **Настройка прокси** установите флажок **Использовать прокси** и введите следующую информацию:

Настройка	Комментарий
IP-адрес прокси	Введите адрес прокси-сервера в формате *<адрес>:<порт>*, где <адрес> – IP-адрес или имя прокси-сервера, <порт> – порт, на котором работает прокси-сервер.
Имя пользователя, Пароль	При необходимости, введите имя пользователя и пароль для подключения к прокси-серверу. Если прокси-сервер разрешает анонимный доступ, оставьте поля пустыми.
Подтверждение пароля	Повторно введите пароль.

8. На шаге **Готова к установке программы** нажмите кнопку **Далее.** Мастер установки регистрирует программу и среди прочего копирует лицензионный ключевой файл в каталог установки (обычно, %ProgramFiles%\DrWeb for MIMEsweeper).
9. На шаге **Перезапуск служб** выберите одну из опций перезапуска сервисов контентного фильтра.
10. На шаге **Программа InstallShield завершена** нажмите кнопку **Готово**.

Dr.Web для MIMEsweeper подключается к контентному фильтру только после перезапуска сервиса MIMEsweeper for SMTP Security Service.

Программа **Dr.Web для MIMEsweeper** установлена и готова к настройке.

Многочисленные серверы политик

Если в среде ClearSwift MIMEsweeper for SMTP используется несколько серверов политик Policy Server, необходимо установить программу **Dr.Web для MIMEsweeper** на все компьютеры, где работают серверы политик Policy Server. Сценарии контентного фильтра применяются всеми серверами политик. После создании сценария проверки почтовых сообщений с использованием **Dr.Web для MIMEsweeper** каждый сервер политик Policy Server во время проверки подключается к программе. Если приложение не установлено на компьютере, где работает сервер политик Policy Server, дальнейшая обработка почты для контентного фильтра становится невозможной.

Установка программы для нескольких серверов политик

1. Для каждого компьютера, где работает сервер политик Policy Server, выполните установку **Dr.Web для MIMEsweeper** согласно инструкции для среды, в которой работает единый сервер политик.
2. Повторите шаг 1 для всех компьютеров, где работают сервера политик Policy Server.

Программа **Dr.Web для MIMEsweeper** установлена и готова к настройке.

Удаление программы

Для удаления **Dr.Web для MIMEsweeper** необходимо иметь права администратора.

Удаление программы

1. Откройте редактор политик MIMEsweeper for SMTP и в списке сценариев (рис. 1) выберите сценарий, созданный для программы **Dr.Web для MIMEsweeper**.
2. В контекстном меню сценария выберите **Delete**.
3. Откроется окно подтверждения удаления. Нажмите кнопку **Да**.
4. На панели инструментов редактора политик MIMEsweeper for SMTP нажмите кнопку **Save MIMEsweeper Policy**  .
5. Закройте редактор политик MIMEsweeper for SMTP.

6. Для удаления **Dr.Web для MIMEsweeper** воспользуйтесь одним из следующих способов вызова мастера удаления программы:
   - на **Панели управления** откройте компонент **Установка и удаление программ**, в окне **Установка и удаление программ** выберите программу **Dr.Web for MIMEsweeper** и нажмите кнопку **Удалить**;
   - В меню **Пуск** выберите пункт **Все программы**, а затем выберите пункт **Удалить Dr.Web for MIMEsweeper** в меню группы **Dr.Web for MIMEsweeper**.
7. Откроется окно подтверждения удаления. Нажмите кнопку **Да**. Мастер удаляет компоненты программы и задание на обновление антивирусных баз.

Лицензионный файл и журнал регистрации событий программы не удаляются по умолчанию. Вы можете удалить оставшиеся файлы вручную из следующих папок:

- лицензионный ключевой файл хранится в каталоге установки программы (обычно, %ProgramFiles%\DrWeb for MIMEsweeper) или в указанном пользователем каталоге;
- файлы журналов регистрации событий программы хранятся в каталоге хранения журналов (обычно, % AllUserProfile%\Local Settings\Application Data\Doctor Web\Logs).

Настройка подключения через прокси

Если компьютер, на котором установлена программа **Dr.Web для MIMEsweeper**, подключен к сети Интернет через прокси-сервер, необходимо дополнительно настроить модуль обновления программы для подключения к прокси-серверу.

Настройка подключения к прокси-серверу

1. Чтобы настроить параметры соединения с прокси-сервером, запустите на исполнение файл UpdaterProxySetup.exe, хранящийся в папке установки программы (обычно, %ProgramFiles%\DrWeb for MIMEsweeper).
2. В открывшемся окне установите флажок **Использовать прокси**.
3. В поле **Прокси** введите адрес прокси-сервера в формате <*адрес*>**:**<*порт*>, где <*адрес*> – IP-адрес или имя прокси-сервера, <*порт*> – порт, на котором работает прокси-сервер.
4. При необходимости, в поле **Имя** пользователя введите имя пользователя, а в поле **Пароль** – пароль указанного пользователя, и затем повторно введите пароль в поле **Подтверждение пароля**. Если прокси-сервер разрешает анонимный доступ, оставьте поля пустыми.

   Модуль обновления программы **Dr.Web для MIMEsweeper** использует указанную учетную запись для подключения к прокси-серверу.

5. Нажмите кнопку **ОК**.

Глава 4. Интеграция с контентным фильтром

Dr.Web для MIMEsweeper устанавливается на те же компьютеры, где установлен контентный фильтр ClearSwift MIMEsweeper for SMTP, и работает как сценарий фильтрации типа 1 (классификация ClearSwift). Это наиболее современные сценарии проверки сообщений, создание которых максимально автоматизировано контентным фильтром.

Настройка контентного фильтра для работы с программой

1. Чтобы настроить контентный фильтр ClearSwift MIMEsweeper for SMTP для работы с программой **Dr.Web для MIMEsweeper**, откройте редактор политик ClearSwift MIMEsweeper for SMTP.
2. Создайте сценарий проверки почтовых сообщений с помощью **Dr.Web для MIMEsweeper**.
3. Настройте созданный сценарий.
4. При желании, вы также можете отключить проверку на спам.

Дополнительную информацию о сценариях контентных фильтров ClearSwift можно найти на официальном сайте компании по адресу http://www.clearswift.com/products/msw/smtp/eval/avscenario.aspx.

Создание сценария проверки

Контентный фильтр ClearSwift MIMEsweeper for SMTP использует сценарии типа Content Scanner для проверки содержимого писем с помощью антивирусов.

Создание сценария проверки сообщений

1. Откройте редактор политик MIMEsweeper for SMTP.
2. В иерархическом дереве в левой части окна раскройте узел **MIMEsweeper for SMTP**, а затем узел **Policies**.
3. В контекстном меню узла **Scenarios** выберите пункт **Создать**, а затем пункт **Content Scanner**.

   Откроется окно мастера создания сценариев.

4. На шаге **Welcome to the Content Scanner Wizard** проверьте, что флажок **I want to create new items without using wizard** снят и нажмите кнопку **Далее**.
5. На шаге **Initial Scenario State**, проверьте, что установлены следующие флажки:
   - **Enabled** – указывает на то, что сценарий должен выполняться для всех полученных сообщений;
   - **Overridable** – указывает на то, что сценарий допускает изменение настроек для подкаталогов узла Scenarios (например, переопределение параметров сценария для входящих или исходящих писем отдельно).

   Нажмите кнопку **Далее**.

6. На шаге **Scanner** в списке антивирусов выберите **Dr.Web for MIMEsweeper** и нажмите кнопку **Далее**.
7. На шаге **Cleaning** установите или снимите следующие флажки:
   - чтобы вылечить с помощью программы **Dr.Web для MIMEsweeper** зараженные сообщения, установите флажок **Clean the detected item**;
   - чтобы добавить в текст вылеченного письма сообщение о лечении, установите флажок **Annotate the associated message**.

   Нажмите кнопку **Далее**.

8. На шаге **Stripping** установите или снимите следующие флажки:
   - чтобы удалить обнаруженные вредоносные программы, если лечение не возможно, установите флажок **Strip the detected item**;
   - чтобы добавить в текст обезвреженного письма сообщение о нейтрализованной угрозе, установите флажок **Annotate the associated message**.

Если опции лечения и удаления выбраны одновременно, то программа сначала предпринимает попытку вылечить объект и только в случае неудачи – удаляет его.

Нажмите кнопку **Далее**.

9. На шаге **Classifications**, выберите, как классифицировать письма с обнаруженными объектами. Рекомендуется относить письма с нейтрализованным вирусом к категории Cleaned, а письма с вирусом, который не удалось вылечить, к категории Virus. Для этого выполните следующие действия:
   - для опции **On detected items cleaned** выберите значение **Cleaned**;
   - для опции **On detected items stripped** выберите значение **Cleaned**;
   - для опции **On threat cannot be removed** выберите значение **Virus**.

   Нажмите кнопку **Далее**.

10. На шаге **Scenario Name** введите следующую информацию:
    - **Name** – имя сценария;
    - **Notes** – краткое описание сценария.

    Нажмите кнопку **Далее**.

11. На шаге **Completing the Content Scanner Wizard** прочитайте описание сценария и нажмите кнопку **Готово**.

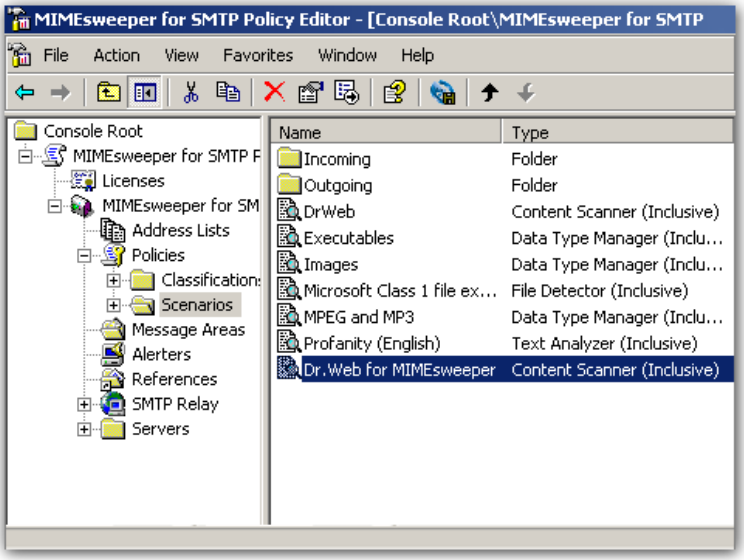

Рисунок 1. Список сценариев контентного фильтра.

Сценарий проверки почтовых сообщений при помощи **Dr.Web для MIMEsweeper** появляется в списке сценариев контентного фильтра ClearSwift MIMEsweeper for SMTP (рис. 1).

Настройка сценария проверки

После создания сценария необходимо указать типы данных, подлежащих проверке программой **Dr.Web для MIMEsweeper**.

Настройка сценария проверки сообщений

1. Чтобы настроить сценарий проверки сообщений, откройте редактор политик MIMEsweeper for SMTP и в списке сценариев (рис. 1) выберите созданный сценарий для программы **Dr.Web для MIMEsweeper**.
2. В контекстном меню сценария выберите пункт **Свойства**.

3. На вкладке **Data Types** (рис. 2) выполните любые из следующих действий:
   - для проверки писем на вирусы и спам, выберите опцию **Include all data types**;
   - для проверки писем только на вирусы, выберите опцию **Exclude selected data types**, в списке типов данных раскройте узел **Containers** и установите флажок **SMTP message**;
   - для проверки писем только на спам, выберите опцию **Include selected data types**, в списке типов данных раскройте узел **Containers** и установите флажок **SMTP message**.

Для раздельной классификации инфицированных и спам-сообщений вы можете использовать отдельные сценарии для проверки писем либо только на вирусы, либо только на спам.

4. Если на шаге **Cleaning** создания сценария вы выбрали опцию **Annotate the associated message**, на вкладке **Cleaned Annotation** задайте параметры строки оповещения, добавляемой к вылеченным письмам.
5. Если на шаге **Stripping** создания сценария вы выбрали опцию **Annotate the associated message**, на вкладке **Stripped Annotation** задайте параметры строки оповещения, добавляемой к письмам, из которых были удалены инфицированные объекты.
6. Нажмите кнопку **OK**.
7. В списке сценариев проверки выберите сценарий для программы **Dr.Web для MIMEsweeper** и воспользуйтесь стрелочками  на панели инструментов, чтобы поместить сценарий на первое место в списке. Контентный фильтр выполняет сценарии в том, порядке в котором сценарии упорядочены в списке. Для обеспечения безопасности и корректной работы сценарий антивирусной проверки должен выполняться первым.
8. На панели инструментов редактора политик MIMEsweeper for SMTP нажмите кнопку **Save MIMEsweeper Policy**  .

Программа **Dr.Web для MIMEsweeper** подключена к системе контентной фильтрации ClearSwift MIMEsweeper for SMTP и готова к проверке почтовых сообщений в соответствии с созданным сценарием.

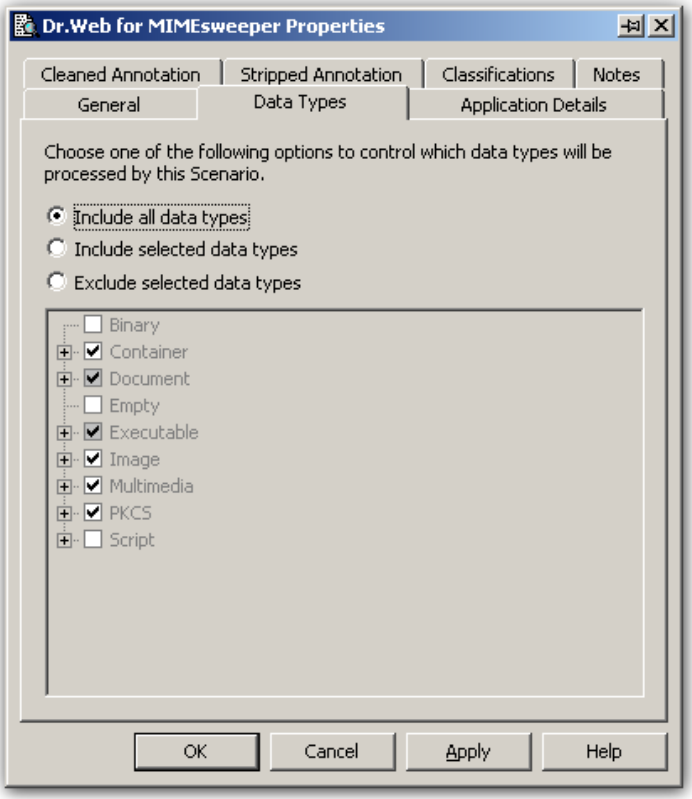

Рисунок 2. Вкладка Data Types.

Отключение проверки на спам

При желании вы можете отключить проверку почтовых сообщений на спам.

Отключение проверки на спам

1. Чтобы отключить проверку почтовых сообщений на спам, откройте редактор политик MIMEsweeper for SMTP и в списке сценариев (рис. 1) выберите сценарий, созданный для программы **Dr.Web для MIMEsweeper**.
2. В контекстном меню сценария выберите пункт **Свойства**.
3. На вкладке **Data Types** (рис. 2) выберите опцию **Exclude selected data types**, в списке типов данных раскройте узел **Containers** и снимите флажок **SMTP message**.
4. Нажмите кнопку **OK**.
5. На панели инструментов редактора политик MIMEsweeper for SMTP нажмите кнопку **Save MIMEsweeper Policy**  .

Глава 5. Проверки

После установки **Dr.Web для MIMEsweeper** проверяет на вирусы и спам все почтовые сообщения, переданные контентным фильтром ClearSwift MIMEsweeper for SMTP. Сообщения, переданные и сохраненные на сервере до установки программы, не проверяются.

Антивирусная проверка сообщений

Приложение проверяет только новые сообщения, приходящие на сервер. Сообщения, переданные и сохраненные на сервере до установки программы, не проверяются.

Dr.Web для MIMEsweeper обнаруживает и обезвреживает следующие вредоносные объекты:

- инфекции в теле письма в формате Rich-Text или HTML;
- инфицированные вложения, в том числе:
- инфицированные архивы;
- инфицированные почтовые сообщения;
- файлы-бомбы или архивы-бомбы;
- рекламные программы;
- программы взлома;
- программы дозвона;
- программы-шутки;
- потенциально опасные программы.

Приложение использует разные методы обнаружения вирусов и обрабатывает зараженные сообщения в соответствии с настройками сценария проверки (табл. 4).

Таблица 4. Настройки проверки на вирусы.

Настройка	Комментарий
Clean the detected item	При выборе данной опции на шаге Cleaning создания сценария проверки программа предпринимает попытку вылечить инфицированный объект. При этом письму присваивается классификация, заданная в параметре **On detected items cleaned** на шаге Classifications создания сценария проверки.
Strip the detected item	При выборе данной опции на шаге Stripping создания сценария проверки программа удаляет инфицированный объект. При этом если одновременно с данной выбрана опция лечения, то приложение удаляет инфицированный объект только в случае невозможности лечения. При этом письму присваивается классификация, заданная в параметре **On detected items stripped** на шаге Classifications создания сценария проверки.
Annotate the associated message	При выборе данной опции на шаге Cleaning или Stripping создания сценария проверки в тело письма после нейтрализации инфицированного объекта добавляется оповещение о выполненных действиях. Текст сообщения и его местоположение в письме зависит от выполненного действия и настроек сценария.
On threat cannot be removed	При задании данной опции на шаге Classifications создания сценария проверки почтовым сообщениям, нейтрализация которых средствами программы **Dr.Web для MIMEsweeper** невозможна, контентный фильтр присваивает указанную классификацию (по рекомендации, Virus).

При обнаружении инфицированного объекта программа пытается вылечить его или, если опция лечения не выбрана, сразу удаляет. Если к почтовому сообщению прикреплено несколько файлов или архивов, программа обезвреживает только зараженные вложения. Если вирус обнаружен в теле письма (например, в виде скрипта в письме HTML-формата), письмо перемещается в карантин. Чистые письма, файлы и архивы передаются без изменений. Письма, которые программа не может обезвредить, помечаются как вирусы и по умолчанию перемещаются в карантин. В зависимости от настроек сценария оповещение о результатах проверки и предпринятых программой действиях может добавляться не только в тело, но и в заголовок писем.

Методы обнаружения вирусов

Все антивирусы **«Доктор Веб»** одновременно используют несколько методов обнаружения вредоносных объектов, что позволяет максимально тщательно проверить подозрительные файлы и контролировать поведение программ:

1. В первую очередь применяется *сигнатурный* анализ. Он выполняется путем анализа кода подозрительных файлов на предмет соответствия сигнатурам известных вирусов (сигнатурой называется непрерывная конечная последовательность байт, необходимая и достаточная для опознания вируса). При этом сравнение проводится по контрольным суммам сигнатур, что позволяет значительно снизить размер записей в антивирусных базах данных, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения и лечения зараженных файлов. **Антивирусная база Dr.Web** составлена таким образом, что благодаря одной записи можно обнаруживать целые классы угроз.
2. После завершения сигнатурного анализа применяется уникальная технология **Origins Tracing**, которая позволяет определить новые или модифицированные вирусы, использующие известные механизмы заражения файлов. Так, например, эта технология защищает пользователей антивирусных решений **Dr.Web** от таких вирусов, как вирус-шантажист Trojan.Encoder.18 (так же известный под названием gpcode). Кроме того, именно введение **Origins Tracing** позволяет значительно снизить количество ложных срабатываний эвристического анализатора.
3. Работа эвристического анализатора основывается на неких знаниях (*эвристиках*) о характерных признаках вирусного и, наоборот, безопасного кода. Каждый признак имеет определенный вес (число, показывающее серьезность и достоверность данного признака). На основании суммарного веса, характеризующего каждый конкретный файл, эвристический анализатор вычисляет вероятность заражения файла неизвестным вирусом. Как и любая система проверки гипотез в условиях неопределенности,

эвристический анализатор может допускать ошибки как первого (пропуск неизвестных вирусов), так и второго рода (ложная тревога).

Во время проверок компоненты антивирусов **Dr.Web** используют самую свежую информацию обо известных вредоносных программах. Сигнатуры вирусов, информация об их признаках и моделях поведения обновляется сразу же, как только специалисты Антивирусной Лаборатории **«Доктор Веб»** обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейший вирус проникает на компьютер, минуя резидентные средства защиты, после обновления вирусных баз он будет обнаружен в списке процессов и нейтрализован.

Добавление информации в заголовок

В зависимости от настроек сценария в заголовок и тело обезвреженных писем контентным фильтром может добавляться оповещение о результатах проверки и предпринятых приложением действиях. **Dr.Web для MIMEsweeper** помещает информацию о выполненных над письмом операциях в токен Detected (для незараженных сообщений токен остается пустым). Вы можете настроить ClearSwift MIMEsweeper for SMTP добавлять токен Detected в заголовок писем.

Рекомендуется добавлять заголовок к письмам, которые программа **Dr.Web для MIMEsweeper** не может нейтрализовать (по умолчанию им присваивается классификация Virus). Контентный фильтр MIMEsweeper for SMTP относит к данной классификации не только письма с вирусами, но и спам. Использование заголовков позволит определить причину, по которой письмо было отнесено к данной классификации.

Добавление информации в заголовок писем

1. Чтобы добавить заголовок к письмам, откройте редактор политик MIMEsweeper for SMTP.
2. В иерархическом дереве в левой части окна раскройте узел **MIMEsweeper for SMTP**, а затем раскройте узел **Policies.**

3. Выберите узел **Classifications**, а затем в правой части окна выберите классификацию, для писем которой хотите задать добавление заголовка.
4. В контекстном меню классификации выберите пункт **New**, а затем пункт **Add Header**.
5. Откроется мастер добавления заголовка. Нажмите кнопку **Next**.
6. На шаге **Header Details** выполните следующие действия:
   - введите название заголовка в поле **Header Name**;
   - введите текст заголовка, который вы хотите добавить к письмам;
   - нажмите на стрелочку на кнопке **Tokens** и выберите пункт **Detected**.

   Dr.Web для MIMEsweeper определяет значение метки **Detected** в зависимости от типа обнаруженной угрозы:

   - для спам-писем в тексте метки присутствует индикатор `SPAM`;
   - для писем, нейтрализация которых невозможна, в тексте метки присутствует индикатор `VIRUS`.

   Нажмите кнопку **Next**.
7. На шаге **Action name** по желанию измените название действия в поле **Name** и добавьте примечание в поле **Note.** Нажмите кнопку **Next**.
8. На шаге **Completing the Add Header Wizard** нажмите кнопку **Finish**.
9. В списке действий выберите добавление заголовка к письму и воспользуйтесь стрелочками  на панели инструментов, чтобы поместить добавление заголовка на первое место в списке. Контентный фильтр выполняет действия в том порядке, в котором они приведены в списке. Для корректной обработки письма перемещение его в карантин должно выполняться после добавления заголовка.
10. На панели инструментов редактора политик MIMEsweeper for SMTP нажмите кнопку **Save MIMEsweeper Policy**  .

Проверка сообщений на спам

С помощью спам-фильтра VadeRetro **Dr.Web для MIMEsweeper** проверяет на спам все почтовые сообщения, переданные контентным фильтром ClearSwift MIMEsweeper for SMTP. Фильтр VadeRetro поставляется настроенным и не требует дополнительного обучения. Фильтрация выполняется в соответствии настройками сценария проверки сообщений (табл. 5).

Таблица 5. Настройки проверки на спам.

Настройка	Комментарий
Include all data types	При выборе данной опции на вкладке Data Types свойств сценария (рис. 2) программа проверяет все полученные почтовые сообщения на спам.
Exclude selected data types, Containers | SMTP message	При установке флажка SMTP message в подгруппе Containers на вкладке Data Types свойств сценария (рис. 2) программа не проверяет полученный сообщения на спам.
On threat cannot be removed	При задании данной опции на шаге Classifications создания сценария проверки контентный фильтр присваивает указанную классификацию (по рекомендации, Virus) спам-письмам.

Контентный фильтр ClearSwift MIMEsweeper for SMTP присваивает нежелательной корреспонденции ту же классификацию, что и почтовым сообщениям, содержащим неизлечимый вирус (Virus по умолчанию). Письма с такой классификацией автоматически перемещаются в карантин. Вы можете задать добавление заголовка к письмам, отнесенным к данной классификации, и настроить фильтрацию сообщений в соответствии с причиной помещения письма в карантин.

При желании вы так же можете полностью отключить проверку на спам.

Глава 6. Обновление антивирусных баз

Модуль обновления (DrWebUpW.exe) запускается сразу после установки приложения и загружает последние версии антивирусного ядра (drweb32.dll), спам-фильтра (vrcpp.dll), а также антивирусных баз (*.vdb) и автоматически их обновляет.

Для обнаружения вредоносных объектов приложение использует специальные антивирусные 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 антивирусных баз через Интернет. В течение срока действия лицензии модуль обновления регулярно загружает и устанавливает информацию о новых вирусах и вредоносных программах, а так же обновления самой программы.

По умолчанию при установке **Dr.Web для MIMEsweeper** создается задание по обновлению антивирусных баз, в котором задан оптимальный интервал запроса обновлений с сервера Всемирной системы обновлений компании **«Доктор Веб»**. При желании вы можете отредактировать данное расписание при помощи планировщика заданий Windows. Вы также можете настроить работу модуля обновления, используя параметры командной строки (см. Приложение А).

Для компьютеров, не имеющих доступа к сети Интернет, вы можете настроить централизованное обновление.

При подключении к сети Интернет через прокси-сервер, необходимо настроить модуль обновления программы для подключения к прокси-серверу.

Редактирование расписания обновлений

1. Откройте **Планировщик заданий**.
2. В контекстном меню задания **DrWeb for MIMEsweeper Update**  выберите пункт **Свойства**.
3. В диалоговом окне **DrWeb for MIMEsweeper Update** выберите вкладку **Расписание** и измените период обновления. По умолчанию, обновление антивирусных баз программы выполняется ежедневно каждые 30 минут.
4. Нажмите кнопку **OK**.

Обновление без подключения к сети Интернет

1. Создайте центральный каталог для хранения обновлений антивирусных баз и модулей программы **Dr.Web для MIMEsweeper**.

Для обновления можно использовать только папки, путь к которым соответствует соглашению об универсальном назначении имен (UNC-пути):

- папки на локальном диске компьютера;
- сетевые папки общего доступа.

2. По мере появления обновлений антивирусных баз и модулей программы **Dr.Web для MIMEsweeper** на официальном сайте компании по адресу http://download.drweb.com/bases/ помещайте файлы обновлений в центральный каталог. Вы можете просмотреть список доступных к обновлению компонентов в файле drweb32.lst, расположенном в каталоге установки приложения (обычно, %ProgramFiles%\DrWeb for MIMEsweeper).
3. На локальном компьютере, где вы хотите настроить обновление через центральный каталог, откройте **Планировщик заданий**.
4. В контекстном меню задания **DrWeb for MIMEsweeper Update**  выберите пункт **Свойства**.

5. В диалоговом окне **DrWeb for MIMEsweeper Update** выберите вкладку **Задание** и добавьте следующий ключ к команде в поле **Выполнить**:

   /URL:<*сервер обновления*>, где <*сервер обновления*> – путь к каталогу, в котором хранятся файлы обновления.

6. Нажмите кнопку **OK**.

Модуль обновления программы настроен на централизованное обновление без подключения к сети Интернет.

Глава 7. Регистрация событий

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

- журнале регистрации событий операционной системы (Event Log);
- текстовом журнале регистрации событий, расположенном в каталоге хранения локальных настроек приложения.

Текстовый журнал регистрации событий находится в файле DRWMSWLog.log в каталоге %AllUserProfile%\Local Settings\Application Data\Doctor Web\Logs. Информация об обновлениях заносится в отдельный журнал drwebupw.log, расположенный в каталоге %AllUserProfile%\Application Data\Doctor Web\Logs\.

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 ее действия, наличие или отсутствие лицензии на антиспам (информация заносится при запуске программы, в процессе ее работы и при замене лицензионного ключевого файла);
- параметры модулей программы: сканера, ядра, антивирусных баз и антиспама (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).

Просмотр журнала регистрации операционной системы

1. Чтобы просмотреть журнал регистрации событий операционной системы, откройте **Панель управления** операционной системы.
2. Выберите **Администрирование**, а затем выберите **Просмотр Событий**.
3. В левой части окна **Просмотр Событий** выберите **Приложение.** Откроется список событий, зарегистрированных в журнале пользовательскими приложениями. Источником сообщений программы **Dr.Web для MIMEsweeper** является приложение Dr.Web for MIMEsweeper.

Текстовый журнал

В текстовый журнал регистрации программы (DRWMSMLog) заносится следующая информация:

- сообщения о действительности или недействительности лицензии;
- сообщения об обнаружении вирусов для каждого зараженного письма и для каждого вируса в отдельности;
- сообщения об обнаружении спама;
- сообщения об ошибках записи или чтения файлов, ошибках анализа архивов или файлов, защищенных паролем;
- сообщения об экстренных остановах ядра программы;
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 дней до окончания срока).

При достижении максимального размера (10000 КБ по умолчанию) файл журнала очищается, и журнал начинается заново.

Глава 8. Локализация программы

Приложение поддерживает английский (по умолчанию) и русский языки интерфейса. Настройки локализации применяются только для утилиты UpdaterProxySetup и сообщений в журнале регистрации событий операционной системы (Event Log).

Изменение языка пользовательского интерфейса

Данную операцию рекомендуется выполнять только администратору или опытному пользователю системы. Неверные действия при изменении реестра могут серьезно повредить систему. Специалисты компании Microsoft рекомендуют перед изменением реестра создать резервную копию всех важных данных, имеющихся на компьютере.

1. Откройте редактор реестра операционной системы.
2. Найдите ключ HKEY_LOCAL_MACHINE\SOFTWARE\DOCTOR WEB\DRWEB FOR MIMESWEEPER\LOCALE.
3. В контекстном меню параметра LANGUAGE выберите **Изменить**.
4. В диалоговом окне введите в поле **Значение** стандартный номер языка локализации:
   - для использования русского языка, введите **1049**;
   - для использования английского языка, введите **1033**.
5. Нажмите кнопку **ОК** и выйдите из редактора реестра.
6. Перезапустите программу Dr. Web.

Глава 9. Диагностика

Для проверки корректности установки и настройки **Dr.Web для MIMEsweeper** воспользуйтесь приведенными в данном разделе тестами:

- проверка корректности установки
- проверка работы модуля обновления
- проверка работы программы

Проверка установки

1. Чтобы проверить корректность установки, удостоверьтесь, что созданы следующие папки:
   - %ProgramFiles%\DrWeb for MIMEsweeper\
   - %CommonProgramFiles%\Doctor Web\
   - %AllUserProfile%\Application Data\Doctor Web\
2. Откройте Панель управления операционной системы, выберите **Администрирование**, а затем **Службы**. Проверьте, что следующие службы запущены:
   - Dr.Web Scanning Engine (DrWebEngine)
   - MIMEsweeper for SMTP Infrastructure
   - MIMEsweeper for SMTP Security Service
3. Откройте журнал регистрации событий операционной системы (Event Log) и убедитесь, что в нем нет ошибок, связанных с программой **Dr.Web для MIMEsweeper**.
4. Откройте каталог %AllUserProfile%\Local Settings\Application Data\Doctor Web\Logs и проверьте, что текстовый журнал регистрации событий DRWMSWLog.log не содержит ошибок.

Проверка модуля обновления

1. Чтобы проверить работоспособность модуля обновления, откройте Панель управления операционной системы, выберите **Назначенные Задания** и проверьте, что задание DrWeb for MIMEsweeper Update  создано.

2. Проверьте корректность обновления. Приложение и антивирусные базы обновляются сразу же после установки. При корректном обновлении, переменная ERRORLEVEL окружения операционной системы устанавливается в 0. Другие значения свидетельствуют об ошибке.
3. Откройте журнал регистрации обновлений программы DRWebUpw.log, расположенный в каталоге %AllUserProfile %\Application Data\Doctor Web\Logs\ и убедитесь, что он не содержит ошибок.

Проверка подключения программы

1. Чтобы проверить подключение **Dr.Web для MIMEsweeper** к системе контентной фильтрации, отправьте письмо с тестовым зараженным файлом EICAR-Test-File во вложении на адрес, который обслуживается защищаемым почтовым сервером. Информацию о тестовом вирусе EICAR можно найти по адресу http://en.wikipedia.org/wiki/EICAR_test_file.
2. Проверьте полученное письмо. Тестовый вирус EICAR неизлечим, поэтому, при условии настройки контентного фильтра в соответствии с настоящим руководством, инфицированный файл должен быть удален из письма. Тело и заголовок письма могут содержать оповещение о действиях, выполненных программой.
3. На адрес, который обслуживается защищаемым почтовым сервером, отправьте по протоколу SMTP тестовое спам-сообщение со следующим текстом:

   ```
   Start enjoying the benefits of Generic Medic1ne. Order quickly and easily, and save a ton of money. Try them out, they're 100% m0ney back guarantee.
   ```

4. Проверьте входящие письма. При условии настройки контентного фильтра в соответствии с настоящим руководством письмо должно быть помещено в карантин и не должно доставляться адресату.

Приложения

Приложение А. Параметры командной строки для модуля обновления

Модуль обновления допускает работу в режиме командной строки.

Параметры командной строки в Планировщике заданий

1. Чтобы настроить выполнение задания по обновлению **Dr. Web для MIMEsweeper**, откройте Планировщик Заданий.
2. В контекстном меню задания DrWeb for MIMEsweeper Update  выберите Свойства.
3. К тексту команды в поле **Выполнить** добавьте выбранные параметры командной строки.

Допустимые параметры

Вы можете использовать следующие параметры запуска, чтобы настроить работу модуля:

Параметр	Комментарий
/DBG	Включает детальный режим ведения журнала регистрации (%AllUserProfile%\Application Data\Doctor Web\Logs\ drwebupw.log).
/URL:<*url*>	Указывает сервер обновлений. Допускаются только пути в формате UNC.
/USER: <*имя*>	Указывает имя пользователя для подключения к серверу обновлений.
/PASS: <*пароль*>	Указывает пароль для подключения к серверу обновлений.

Параметр	Комментарий
/UPM: *<режим>*	Включает режим использования прокси-сервера при подключении к сети Интернет. Параметр *<режим>* может принимать следующие значения: • **direct** – не использовать прокси-сервер; • **ieproxy** – использовать системные настройки прокси-сервера; • **userproxy** – использовать настройки, заданные пользователем.
/PURL: *<адрес>*	Указывает адрес прокси-сервера.
/PUSER: *<имя>*	Указывает имя пользователя для подключения к прокси-серверу.
/PPASS: *<пароль>*	Указывает пароль для подключения к прокси-серверу.
/UA	Включает режим полного обновления, при котором загружаются обновления для всех файлов, указанных в списке обновления, независимо от используемой операционной системы и установленных компонентов продукта. Режим предназначен для получения полной локальной копии серверной области обновления Dr.Web. Этот режим нельзя использовать для обновления антивируса, установленного на компьютере.
/ST	Включает режим невидимого обновления, при котором модуль обновления запускается в невидимом окне (stealth mode).
/LNG: *<файл>*	Указывает имя файла языковых ресурсов. По умолчанию используется английский язык.
/GO	Включает пакетный режим работы, при котором не выводятся диалоговые окна.

Параметр	Комментарий
/QU	Включает режим принудительного закрытия модуля обновления по завершении обновления вне зависимости от результата. Код результата записывается в переменную ERRORLEVEL окружения операционной системы: • нулевое значение указывает на успех, • ненулевое значение указывает на неудачу.
/DIR: *<каталог>*	Указывает каталога для установки файлов обновления. По умолчанию используется каталог, из которого запущен модуль обновления.
/URM: *<режим>*	Включает режим перезагрузки компьютера после обновления. Параметр *<режим>* может принимать следующие значения: • **prompt** – перезагрузка по окончании обновления после разрешения пользователя; • **noprompt** – принудительная перезагрузка по окончании обновления при необходимости; • **force** – принудительная перезагрузка всегда вне зависимости от необходимости; • **disable** – запрет перезагрузки.
/REG	Включает режим регистрации продукта и получения регистрационного ключа.
/UPD	Включает режим обычного обновления. Используйте этот режим вместе с режимом **/REG** для загрузки обновлений сразу же после регистрации продукта.
/UVB	Включает режим обновления только антивирусных баз и ядра drweb32.dll. Этот параметр отменяет действие ключа **/UA**.

Параметр	Комментарий
/RP*<файл>* или **/RP+** *<файл>*	Включает запись отчет о работе программы в указанный файл. По умолчанию используется файл %AllUserProfile% \Application Data\Doctor Web\Logs\ drwebupw.log. Используйте параметр **/RP+** для включения режима добавления в существующий файл. Используйте параметр **/RP** для включения режима перезаписи существующего файла.
/INI: *<путь>*	Указывает альтернативный конфигурационный файл.
/NI	Запрещает использование параметров, записанных в конфигурационном файле drweb32.ini.
/NR	Запрещает создание журнала регистрации обновлений.
/SO	Включает звуковое оповещение об ошибках.

Предметный указатель

Предметный указатель

Предметный указатель