



Dr.WEB®

для Kerio MailServer

Защити созданное

Руководство администратора

© 2003-2010 «Доктор Веб». Все права защищены.

Материалы, приведенные в данном документе, являются собственностью «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

ТОВАРНЫЕ ЗНАКИ

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt! и логотипы Dr.WEB и Dr.WEB INSIDE являются зарегистрированными товарными знаками «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

Ни при каких обстоятельствах «Доктор Веб» и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

**Dr.Web для Kerio MailServer
Версия 6.00.1
Руководство администратора
12.11.2010**

«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

1. Введение	6
Используемые обозначения	7
Техническая поддержка	8
2. Лицензирование	9
Лицензионный ключевой файл	9
Получение ключевого файла	10
Обновление лицензии	11
Использование ключевого файла	12
Определение параметров лицензирования	13
3. Установка и удаление программы	15
Системные требования	17
Компоненты программы	18
Установка программы	19
Удаление программы	22
4. Настройка компонентов программы	25
Запуск и настройка демона	25
Запуск и настройка компонента Dr.Web Monitor	26
Настройка прокси	27
5. Подключение программы	28
Настройка параметров антивируса	29
6. Проверка на вирусы	32
Методы обнаружения вирусов	33
Карантин	35



7. Обновление антивирусных баз	36
8. Регистрация событий	40
Журнал операционной системы	40
Журнал отладки	41
9. Диагностика	42
Проверка установки	42
Проверка работоспособности	43
10. Приложения	44
Приложение А. Интеграция с Dr.Web Enterprise Suite	44
Предметный указатель	46



1. Введение

Благодарим вас за приобретение программы **Dr.Web для Kerio MailServer**. Данный антивирусный продукт обеспечивает надежную защиту корпоративной почтовой системы от вирусных угроз. Приложение подключается к почтовому серверу Kerio и осуществляет проверку файловых вложений электронных сообщений, поступающих на сервер.

В программе применены наиболее передовые разработки и технологии компании «**Доктор Веб**», которые позволяют обнаруживать различные типы вредоносных объектов, представляющих угрозу почтовой системе и информационной безопасности пользователей.

Dr.Web для Kerio MailServer проверяет почтовый трафик на вирусы, программы дозвона, рекламные программы, потенциально опасные программы, программы взлома и программы-шутки. При обнаружении угроз безопасности к ним применяются действия согласно настройкам почтового сервера.

Основные функции программы

Dr.Web для Kerio MailServer выполняет следующие функции:

- антивирусную проверку вложенных файлов почтовых сообщений в соответствии с правилами почтового сервера Kerio;
- обнаружение вредоносного программного обеспечения;
- изоляцию инфицированных файлов в карантине Dr.Web;
- использование эвристического анализатора для дополнительной защиты от неизвестных вирусов;
- регулярное автоматическое обновление антивирусных баз.

Настоящее руководство призвано помочь администраторам корпоративных сетей, использующих почтовый сервер Kerio, установить и настроить программу **Dr.Web для Kerio MailServer**, а также ознакомиться с ее основными функциями.




Дополнительную информацию о возможностях антивирусной проверки электронной почты в рамках почтового сервера Kerio можно найти на официальном сайте компании по адресу http://www.kerio.ru/kms_home.html.

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, которые вам необходимо ввести именно так, как они приведены в руководстве.
Зеленый полужирный	Названия продуктов компании « Доктор Веб » и их компонентов.
<u>Зеленое подчеркивание</u>	Ссылки на разделы документа и веб-сайты.
Моноширинный	Примеры программного кода, вводимый пользователем и выводимый программой текст
<i>Курсив</i>	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>.



2. Лицензирование

Права пользователя на использование программы **Dr.Web для Kerio MailServer** 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;
- возможность использования ключа на почтовых серверах;
- количество пользователей, защищаемых приложением.

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

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

При нарушении любого из условий ключевой файл становится *недействительным*, при этом программа **Dr.Web для Kerio MailServer** перестает обнаруживать вредоносные программы.

Если ключевой файл стал недействительным в процессе работы (например, истек срок его действия), то почтовый сервер перестает доставлять почту получателям. Настроить доставку почты без ее проверки на вирусы можно путем отключения использования приложения **Dr.Web для Kerio MailServer**, для возобновления антивирусной проверки электронной почты необходим действительный ключевой файл. Факт нарушения корректности



ключевого файла записывается в журнал регистрации событий операционной системы, а также в текстовый журнал регистрации событий программы. 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 на компьютер, на котором установлен почтовый сервер Kerio и уже установлена программа **Dr.Web для Kerio MailServer** или планируется ее установка.

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 технической 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 Kerio MailServer**. 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, выполните одно из следующих действий:
 - замените имеющийся ключевой файл в каталоге, заданном параметром `LicenseFile` в секции `[StandaloneMode]` конфигурационного файла `/etc/drweb/agent.conf`, новым ключевым файлом;
 - укажите путь к новому ключевому файлу в качестве значения параметра `LicenseFile` в секции `[StandaloneMode]` конфигурационного файла `/etc/drweb/agent.conf`.



При задании пути необходимо учитывать, что он является регистрозависимым (например, пути `/opt/drweb/` и `/opt/DrWeb/` различны).

2. Чтобы программа переключилась на использование нового ключевого файла, выполните следующую команду:

```
/etc/init.d/drweb-monitor reload
```



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

Использование ключевого файла

Для работы **Dr.Web для Kerio MailServer** необходим ключевой файл, путь к которому нужно указать в качестве значения параметра `LicenseFile` в разделе `[StandaloneMode]` конфигурационного файла `/etc/drweb/agent.conf`.



В качестве значения параметра `LicenseFile` в разделе `[StandaloneMode]` конфигурационного файла `/etc/drweb/agent.conf` можно указать пути к нескольким ключевым файлам, перечислив их через запятую.

В процессе работы **Dr.Web для Kerio MailServer** осуществляется поиск первого рабочего ключа в каталоге, заданного одним из значений параметра `LicenseFile` в секции `[StandaloneMode]` конфигурационного файла `/etc/drweb/agent.conf`. Если не будет найден ни один рабочий ключ, то программа перестанет функционировать.



Редактирование ключевого файла делает его недействительным! Поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.



Изменение пути к ключевому файлу

1. Чтобы изменить путь к ключевому файлу программы, в секции [StandaloneMode] конфигурационного файла /etc/drweb/agent.conf укажите новый путь к ключевому файлу в качестве значения параметра LicenseFile.



При задании пути необходимо учитывать, что он является регистрозависимым.

2. Чтобы программа переключилась на использование ключевого файла, расположенного по указанному пути, выполните следующую команду:

```
/etc/init.d/drweb-monitor reload
```

Определение параметров лицензирования

Лицензионный ключевой файл регулирует использование программы **Dr.Web для Kerio MailServer**.

Определение параметров лицензирования

1. Чтобы определить параметры лицензирования, записанные в вашем ключевом файле, откройте файл для просмотра.





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.



2. Вы можете проверить следующие параметры лицензирования (табл. 2).

Таблица 2. Параметры ключевого файла.

Параметр	Комментарий
Группа [Key], параметр Applications	<p>Указывает компоненты программы, которые разрешено использовать владельцу лицензии.</p> <p> Для использования ключа с программой Dr.Web для Kerio MailServer в списке компонентов обязательно должен присутствовать компонент KerioPlugin.</p> <p>Если для антивирусного демона drwebd используется тот же ключевой файл, что и для приложения Dr.Web для Kerio MailServer, то в списке также должны присутствовать компоненты MailDaemonUnix и FileDaemonUnix.</p>
Группа [Key], параметр Expires	Указывает срок действия лицензионного ключа в формате Год-Месяц-День.
Группа [User], параметр Name	Указывает регистрационное имя владельца лицензии.
Группа [User], параметр Computers	Указывает количество пользователей, защищаемых программой.
Группа [Settings], параметр MailServer	<p>Указывает на разрешение (Yes) или запрет (No) использования ключа на почтовых серверах.</p> <p> Для использования ключа с продуктом Dr.Web для Kerio MailServer значение данного параметра обязательно должно быть Yes, иначе ключевой файл будет считаться недействительным.</p>

3. Закройте файл, не сохраняя изменений.



3. Установка и удаление программы

Программа **Dr.Web для Kerio MailServer** устанавливается на тот же компьютер, на котором установлен почтовый сервер Kerio, и используется им в качестве внешнего антивирусного программного обеспечения, подключаемого через "plug-in" интерфейс.

Программа **Dr.Web для Kerio MailServer** поставляется в виде самораспаковывающегося архива **drweb-keriomailserver-600-linux-x86.run** и может быть установлена [через графический интерфейс](#) и [консоль управления](#). В архиве содержатся следующие пакеты ([табл. 3](#)):

Таблица 3. Пакеты установочного архива программы.

Название	Описание
drweb-common	Содержит: <ul style="list-style-type: none">• основной конфигурационный файл <code>drweb32.ini</code>;• библиотеки;• файлы документации;• структуру директорий. В ходе установки данного пакета создаются: <ul style="list-style-type: none">• пользователь drweb;• группа drweb.
drweb-bases	Содержит: <ul style="list-style-type: none">• антивирусное ядро (Scan Engine);• антивирусные базы (vdb). Для установки требуется пакет drweb-common.
drweb-updater	Содержит модуль обновления антивирусного ядра и антивирусных баз. Для установки требуется пакет drweb-common.



Название	Описание
drweb-daemon	Содержит исполняемые файлы Dr.Web Daemon и документацию к нему. Для установки требуется пакет drweb-bases.
drweb-scanner	Содержит исполняемые файлы консольного сканера Dr.Web Scanner и документацию к нему. Для установки требуется пакет drweb-bases.
drweb-kerio-plugin6	Содержит библиотеку avir_drweb.so антивирусного приложения Dr.Web для Kerio MailServer . Используется для установки и работы с почтовым сервером Kerio MailServer версии 6.x.x.
drweb-kerio-plugin7	Содержит библиотеку avir_drweb.so антивирусного приложения Dr.Web для Kerio MailServer . Используется для установки и работы с почтовым сервером Kerio Connect версии 7.x.x.
drweb-kerio-plugin-doc	Содержит документацию к Dr.Web для Kerio MailServer .
drweb-agent	Содержит исполняемые файлы Dr.Web Enterprise Agent , необходимые библиотеки и документацию к нему. Для установки требует пакеты drweb-boost144 и drweb-common.
drweb-boost144	Содержит библиотеки, которые использует Dr. Web Enterprise Agent . Для установки требует пакет drweb-libs.
drweb-libs	Содержит библиотеки, общие для всех компонентов продукта.
drweb-epm6.0.0-libs	Содержит библиотеки для графических инсталлятора и деинсталлятора. Для установки требует пакет drweb-libs.
drweb-epm6.0.0-uninst	Содержит файлы графического деинсталлятора. Для установки требует пакет drweb-epm6.0.0-libs.



Название	Описание
drweb-monitor	Содержит исполняемые файлы Dr.Web Monitor , необходимые библиотеки и документацию к нему. Для установки требует пакеты drweb-boost144 и drweb-common.

Системные требования

Компьютер, на который устанавливается **Dr.Web для Kerio MailServer**, должен удовлетворять следующим системным требованиям ([табл. 4](#)):

Таблица 4. Системные требования.

Компонент	Требование
Место на жестком диске	Не менее 55 МБ свободного дискового пространства.
Операционная система	Одна из следующих: <ul style="list-style-type: none">• Red Hat 9.0;• Red Hat Enterprise Linux 4/5;• Fedora Core 7 / 8;• SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0 и 11.1;• CentOS Linux 5.2 и 5.3;• Debian 5.0;• Ubuntu 8.04 LTS.
Почтовый сервер	Один из следующих: <ul style="list-style-type: none">• Kerio MailServer 6.2 или выше;• Kerio Connect 7.0.0 или выше.
Прочее ПО	Dr.Web Enterprise Agent из состава Dr.Web Enterprise Suite 6.0 или выше (для взаимодействия с Dr.Web Enterprise Suite)



Для работы **Dr.Web для Kerio MailServer**, в частности, антивирусного демона **drwebd**, необходимо отключить систему Security-Enhanced Linux.

Настоящие системные требования относятся только к **Dr.Web для Kerio MailServer**. Требования к почтовому серверу содержатся в документации Kerio. **Dr.Web для Kerio MailServer** может работать на тех же компьютерах, на которых установлен почтовый сервер Kerio.

Dr.Web для Kerio MailServer также поддерживает установку и работу в среде Kerio MailServer VMware Virtual Appliance. Информацию о данном программном решении можно найти на официальном сайте компании по адресу <http://www.kerio.ru/ru/mailserver>.

Компоненты программы

Dr.Web для Kerio MailServer - это антивирусный продукт, состоящий из нескольких дополняющих друг друга компонентов, которые взаимодействуют между собой и обеспечивают тем самым защиту электронной почты. Ниже приведен список этих компонентов с кратким описанием каждого:

- **Антивирусный демон (drwebd)** осуществляет антивирусную проверку;
- **Консольный сканер** (файл для запуска `/opt/drweb/drweb`) служит для обнаружения и лечения вирусов при проверке файлов на локальной машине, в том числе и в директориях общего доступа. Он запускается по расписанию или вручную и применяет предустановленные действия к зараженным и подозрительным объектам;



- **Модуль обновления** (скрипт `update.pl`), который входит в состав антивирусного пакета **Dr.Web для Kerio MailServer**, предназначен для автоматического обновления антивирусных баз. Модуль загружает копии антивирусных баз из сети Интернет либо из папки или сервера в локальной сети;
- **Dr.Web Monitor** (файл для запуска `/opt/drweb/drweb-monitor`) - это постоянно загруженный модуль, основной задачей которого является повышение отказоустойчивости всей антивирусной системы. Он обеспечивает корректный запуск и остановку антивирусных модулей и их компонентов, а также их перезапуск в случае сбоев.
- **Dr.Web Enterprise Agent** - это постоянно загруженный модуль, который передает компонентам параметры их конфигурации. Кроме того, **Dr.Web Enterprise Agent** управляет политиками антивирусной проверки, в зависимости от активной лицензии **Dr.Web**.

Установка программы

Перед установкой программы удостоверьтесь, что компьютер удовлетворяет минимальным [системным требованиям](#).



Для установки **Dr.Web для Kerio MailServer** необходимо иметь права администратора.

Установка Dr.Web для Kerio MailServer с помощью графической программы установки

1. Разрешите исполнение архива **drweb-keriomailserver-600-linux-x86.run**. Например, вы можете воспользоваться следующей командой:

```
# chmod +x drweb-keriomailserver-600-linux-x86.run
```

2. Запустите файл на исполнение следующей командой:

```
# ./drweb-keriomailserver-600-linux-x86.run
```



- Во время распаковки будет создана директория `drweb-kerio_6.0.1.[patch]-[build]_linux`, где вместо `[patch]` указывается номер обновления, вместо `[build]` - номер сборки (например, `drweb-kerio_6.0.1.2-1001120900_linux`). Далее запустится графическая программа установки (см. [рис. 1](#)).

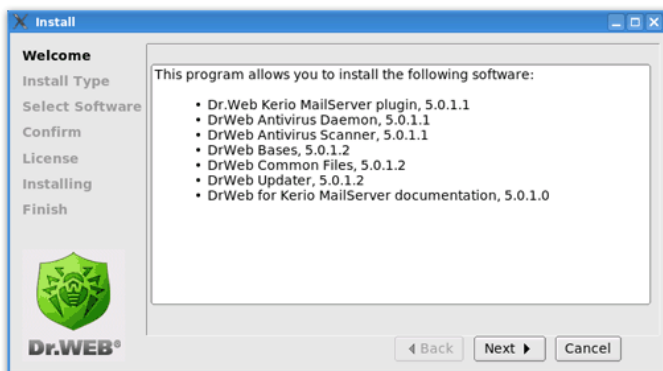


Рисунок 1. Графическая программа установки Dr.Web для Kerio MailServer.

- На шаге **Install type** выберите установочный пакет в зависимости от версии почтового сервера Kerio. Нажмите кнопку **Next**.
- На шаге **License** прочтите лицензионное соглашение (вы можете выбрать язык отображения лицензионного соглашения в списке **Languages**). Для продолжения установки его необходимо принять. Нажмите кнопку **Next**.
- Начнется установка программы **Dr.Web для Kerio MailServer** на ваш компьютер.
- После успешной установки будет выведено окно с сообщением **Installation complete**. Чтобы запустить скрипт для настройки программы, установите флажок **Run interactive postinstall script** и нажмите кнопку **Next**. В результате работы скрипта будут выполнены следующие действия:
 - лицензионный ключ программы будет скопирован в директорию `/etc/drweb`;



- путь к ключевому файлу будет записан в конфигурационные файлы **Dr.Web Enterprise Agent** и демона **drwebd**;
 - для **Dr.Web Monitor** и демона **drwebd** будет настроен автоматический запуск;
 - будет осуществлен запуск **Dr.Web Monitor** и демона **drwebd**.
8. Нажмите кнопку **Close** чтобы завершить работу программы установки.

Установка Dr.Web для Kerio MailServer из консоли (без запуска графической программы установки)

1. Разрешите исполнение архива **drweb-keriomailserver-600-linux-x86.run**. Например, вы можете воспользоваться следующей командой:

```
# chmod +x drweb-keriomailserver-600-linux-x86.run
```
2. Запустите файл на исполнение следующей командой:

```
# ./drweb-keriomailserver-600-linux-x86.run
```
3. Во время распаковки будет создана директория **drwebkerio_6.0.1.[patch]-[build]_linux**, где вместо **[patch]** указывается номер обновления, вместо **[build]** - номер сборки (например, **drweb-kerio_6.0.1.2-1001120900_linux**). Далее запустится программа установки и вам будет предложена помощь в установке программы.
4. Выберите установочный пакет в зависимости от версии сервера Kerio.
5. Откроется Лицензионное Соглашение. Для продолжения установки его необходимо принять.
6. Начнется установка программы **Dr.Web для Kerio MailServer** на ваш компьютер.



7. Далее вам будет предложено настроить основные компоненты программы. В случае вашего согласия будут выполнены следующие действия:
 - лицензионный ключ программы будет скопирован в директорию `/etc/drweb`;
 - путь к ключевому файлу будет записан в конфигурационные файлы **Dr.Web Enterprise Agent** и демона **drwebd**;
 - для **Dr.Web Monitor** и демона **drwebd** будет настроен автоматический запуск;
 - будет осуществлен запуск **Dr.Web Monitor** и демона **drwebd**.
8. По окончании установки будет выведено сообщение о том, что установка завершилась успешно.

Приложение **Dr.Web для Kerio MailServer** установлено и может быть [подключено к почтовому серверу](#).

Удаление программы



Для удаления программы **Dr.Web для Kerio MailServer** необходимо иметь права администратора.

Удаление Dr.Web для Kerio MailServer

1. Отключите использование антивируса **Dr.Web для Kerio MailServer** почтовым сервером Kerio. Для этого:
 - запустите Консоль управления **Administration Console для Kerio MailServer**;
 - откройте подраздел **Конфигурация** -> **Фильтр содержимого** -> **Антивирус**;
 - снимите флажок **Использовать внешнюю антивирусную программу** для выбранного антивируса **Dr.Web for Kerio MailServer**;
 - нажмите кнопку **Применить**. Использование **Dr.Web для Kerio MailServer** будет отключено.



2. Для удаления **Dr.Web для Kerio MailServer** при помощи графической программы удаления:
 - перейдите в каталог `drweb-kerio_6.0.1.[patch]-[build]_linux`, созданный в директории, из которой был запущен установочный пакет **Dr.Web для Kerio MailServer**;
 - выполните команду `# ./uninst`. Запустится графическая программа удаления (см. [рис. 2](#)). Нажмите кнопку **Next**;

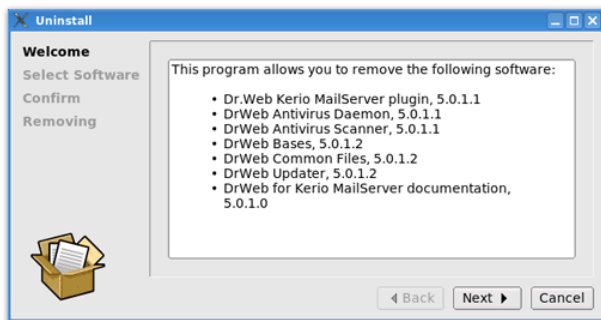


Рисунок 2. Графическая программа удаления Dr. Web для Kerio MailServer.

- на шаге **Select software** выберите компоненты, которые вы хотите удалить. Для удаления всех компонентов нажмите кнопку **Remove all**. Нажмите кнопку **Next**;
- на шаге **Confirm** подтвердите удаление выбранных компонентов, нажав кнопку **Next**. Выбранные компоненты программы **Dr.Web для Kerio MailServer** будут удалены с вашего компьютера;
- по завершении процесса удаления нажмите кнопку **Close** для завершения работы графической программы удаления.



3. Для удаления **Dr.Web для Kerio MailServer** из консоли (без запуска графической программы удаления):

- запустите по очереди все файлы удаления (*.remove) установленных пакетов:

```
# /drweb-kerio_6.0.1. [patch]-[build]_linux/[имя_файла]
.remove
```

- если директория, в которую был распакован дистрибутив продукта, удалена, то файлы *.remove можно запустить из директории `/etc/drweb/software`.



Лицензионный ключевой файл не удаляется по умолчанию. Вы можете удалить его вручную.



4. Настройка компонентов программы

В случае, если во время установки **Dr.Web для Kerio MailServer** не был установлен флажок **Run interactive postinstall script** и, соответственно, не запускался скрипт настройки компонентов программы, необходимо настроить работу [антивирусного демона](#) и компонента [Dr.Web Monitor](#).

В том случае, если для подключения компьютера, на котором установлено приложение, к сети Интернет используется прокси-сервер, необходимо также определить его [параметры](#).

Запуск и настройка демона

После установки **Dr.Web для Kerio MailServer** необходимо настроить работу антивирусного демона **drwebd**. Для этого выполните следующие действия:

1. Откройте файл `/etc/drweb/drwebd.enable` и установите параметр `ENABLE=1`.
2. Скопируйте ключевой файл, разрешающий работу демона **drwebd** в каталог, указанный в параметре `Key` раздела `[Daemon]` конфигурационного файла `/etc/drweb/drweb32.ini`. По умолчанию выбран ключ **/opt/drweb/drweb32.key**.
3. Запустите демон **drwebd** следующей командой:

```
/etc/init.d/drwebd start.
```

Убедитесь, что при загрузке не возникло ошибок.



Запуск и настройка компонента Dr.Web Monitor

Чтобы настроить работу компонента **Dr.Web Monitor**, выполните следующие действия:

1. Откройте файл `/etc/drweb/drweb-monitor.enable` и установите значение параметра `ENABLE=1`.
2. Запустите компонент **Dr.Web Monitor** следующей командой:

```
/etc/init.d/drweb-monitor start.
```

Убедитесь, что при загрузке не возникло ошибок.



Настройка прокси

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

Параметры подключения к прокси-серверу задаются в конфигурационном файле (по умолчанию `/etc/drweb/drweb32.ini`) в секции [Updater] ([табл. 5](#)):

Таблица 5. Параметры подключения к прокси.

Параметр	Комментарий
<code>ProxyServer = <имя или IP-адрес прокси-сервера></code>	Имя или IP-адрес используемого прокси-сервера.
<code>ProxyLogin = <имя пользователя прокси-сервера></code>	Имя пользователя прокси-сервера.
<code>ProxyPassword = <пароль пользователя прокси-сервера></code>	Пароль пользователя прокси-сервера.



5. Подключение программы

Dr.Web для Kerio MailServer подключается к почтовому серверу Kerio в качестве внешнего антивирусного программного обеспечения и осуществляет проверку электронной почты в соответствии с настройками сервера Kerio.

Подключение Dr.Web для Kerio MailServer

1. Запустите Консоль управления **Administration Console для Kerio MailServer**.
2. Откройте подраздел **Конфигурация -> Фильтр содержимого -> Антивирус**.
3. Установите флажок **Использовать внешнюю антивирусную программу** и выберите **Dr.Web для Kerio MailServer** в выпадающем списке.
4. Определите [параметры антивирусной программы](#).
5. Нажмите кнопку **Применить**.

Если при подключении антивируса возникли ошибки, проверьте [корректность установки программы](#), а также просмотрите журнал ошибок error сервера Kerio и проконсультируйтесь с руководством администратора почтового сервера Kerio для решения возникшей проблемы.

Дополнительную информацию об использовании антивирусного программного обеспечения почтовым сервером Kerio и возможных ошибках подключения вы можете найти в руководстве администратора Kerio MailServer/Kerio Connect и на официальном сайте компании по адресу http://www.kerio.ru/kms_home.html.



Настройка параметров антивируса

Параметры приложения **Dr.Web для Kerio MailServer** определяют специфику его работы, а также регистрацию событий программы. Они могут быть изменены с помощью Консоли управления почтовым сервером **Administration Console для Kerio MailServer** в разделе **Конфигурация -> Фильтр содержимого -> Антивирус**:

1. Нажмите кнопку **Параметры** справа от выбранной антивирусной программы.
2. Откроется список параметров (табл. 6). Для того чтобы изменить значение того или иного параметра, выберите его в списке и нажмите кнопку **Редактировать**. В окне **Редактировать значение** укажите значение выбранного параметра, после чего нажмите кнопку **ОК**.

Таблица 6. Параметры программы Dr.Web для Kerio MailServer.

Параметр	Комментарий
Detect adware (Yes/No)	Перечисленные параметры позволяют настроить проверку электронной почты на наличие рекламных программ, программ дозвона, программ взлома, программ-шуток и потенциально опасных программ. Каждый параметр может принимать одно из следующих значений:
Detect dialers (Yes/No)	
Detect hacktools (Yes/No)	
Detect jokes (Yes/No)	
Detect riskware (Yes/No)	
	<ul style="list-style-type: none">• No означает, что объекты, содержащие данный тип вредоносного ПО, будут пропущены;• Yes запрещает передачу подобных объектов. Данное значение установлено по умолчанию для всех типов вредоносных объектов.



Dr.Web Agent socket path	<p>Данная настройка задает сокет для взаимодействия с Dr.Web Enterprise Agent. По умолчанию установлено значение pid:/var/drweb/run/drweb-agent.pid.</p> <p>Дополнительную информацию по настройке работы данного компонента вы можете найти в документации для Dr.Web Enterprise Agent.</p>
Dr.Web Daemon socket path	<p>Данная настройка задает сокет для взаимодействия с антивирусным демоном drwebd. По умолчанию установлено значение pid:/var/drweb/run/drwebd.pid.</p> <p>С помощью данного параметра вы также можете настроить выполнение антивирусной проверки на удаленном компьютере с установленным демоном Dr.Web Daemon (drwebd), например, если компьютер, на котором установлен почтовый сервер Kerio, не имеет доступа в Интернет или организован единый сервер антивирусной проверки. Для этого в качестве значения параметра необходимо указать IP адрес и порт, на который настроен удаленный демон, в следующем виде:</p> <p><ip-address>:<port>.</p> <p>Например: 192.168.100.10:3000.</p> <p>Дополнительную информацию по настройке проверки на удаленном компьютере вы можете найти в документации для Dr.Web Daemon.</p>



Enable heuristic (Yes/No)	<p>С помощью данного параметра вы можете включить или отключить эвристический анализатор, позволяющий обнаруживать неизвестные вирусы. По умолчанию эвристический анализатор включен. Вы можете указать одно из двух значений параметра:</p> <ul style="list-style-type: none">• No для отключения эвристического анализатора;• Yes для включения эвристического анализатора.
Quarantine directory	<p>Данная настройка задает путь к директории карантина. По умолчанию установлено значение /var/drweb/infected.</p>
Quarantine enabled (Yes/No)	<p>Данный параметр позволяет включить/выключить перемещение инфицированных объектов в карантин. По умолчанию выбрано значение Yes.</p>

3. Нажмите кнопку **ОК** в окне **Параметры антивирусной программы**, когда измените значения параметров.
4. Нажмите кнопку **Применить** в разделе **Антивирус** для сохранения сделанных изменений.



6. Проверка на вирусы

Программа **Dr.Web для Kerio MailServer** обнаруживает следующие вредоносные объекты:

- инфицированные вложения электронных писем, в том числе:
 - инфицированные архивы;
 - файлы-бомбы или архивы-бомбы;
 - рекламные программы;
 - программы взлома;
 - программы дозвона;
 - программы-шутки;
 - потенциально опасные программы.

Вы можете определить типы обнаруживаемых вредоносных объектов с помощью соответствующих [параметров антивирусной программы](#).

Dr.Web для Kerio MailServer использует различные [методы обнаружения вирусов](#), к найденным вредоносным объектам применяются действия в соответствии с настройками почтового сервера Kerio.

Действия почтового сервера в случае обнаружения программой **Dr. Web для Kerio MailServer** вирусов во вложенных файлах электронных сообщений, а также в случае невозможности проверки файлов, определяются с помощью Консоли управления **Administration Console для Kerio MailServer**, в соответствующих группах настроек раздела **Конфигурация** -> **Фильтр содержимого** -> **Антивирус** или на вкладке **Действия** (в зависимости от версии сервера Kerio).

Вы можете запретить передачу сообщения, разрешить доставку сообщения, удалить инфицированные вложения, переслать исходное сообщение или сообщение с удаленными инфицированными вложениями администратору, вернуть сообщение отправителю или направить ему предупреждение о наличии вредоносных объектов в сообщении.



В случае невозможности проверки вложенного файла, например, если он защищен паролем или поврежден, вы можете запретить его передачу, применив действия, заданные для инфицированных вложений, или разрешить доставку сообщения и вложения с информированием о возможном наличии в нем вирусов.

Подробнее о настройках антивирусного сканирования электронной почты и действиях почтового сервера над обнаруженными вредоносными объектами можно узнать из руководства администратора Kerio MailServer/Kerio Connect.

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 продуктов 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 любой из проверок компоненты антивирусов **Dr.Web** используют самую свежую информацию об 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. Таким образом, регулярное автоматическое [обновление антивирусных баз](#) позволяет обнаруживать даже самые новые вирусы.



Карантин

Инфицированные вложения могут быть перемещены в **Карантин** - специальную директорию `/var/drweb/infected`, предназначенную для изоляции и безопасного хранения вредоносных объектов.

По умолчанию, опция перемещения инфицированных объектов в карантин включена. Для ее отключения, установите значение **No** для параметра антивируса **Quarantine enabled**. В случае выключения карантина инфицированные вложения будут удаляться.



В случае, если в карантин помещается файл, имя которого совпадает с именем уже находящегося в карантине файла, то к имени помещаемого файла будет добавлен числовой индекс. Например, `file.com` будет переименован в `file.com_01` и т.д.

Управление карантинном

Просмотр файлов, находящихся в карантине, и работа с ними доступны только суперпользователю (`root`). Вы можете удалить файлы из директории карантина или сохранить их на диск.



При использовании версий Kerio MailServer с 6.2 по 6.7.2 включительно возможны ошибки в отображении кириллических имен файлов в журналах регистрации событий и в списке карантина. Таким образом, если имя инфицированного файла содержит кириллические символы, то они будут удалены из имени при перемещении файла в карантин Dr.Web. Однако, эти ошибки не влияют на доставку почтовых сообщений.



7. Обновление антивирусных баз

Для автоматизации получения и установки обновлений антивирусных баз рекомендуется использовать Модуль обновления. Модуль содержится в пакете **drweb-updater**, который входит в состав продукта **Dr.Web для Kerio MailServer**.



Если **Dr.Web Enterprise Agent** настроен на работу в режиме **Enterprise**, обновление антивирусных баз и антивирусного ядра происходит из репозитория **Dr.Web Enterprise Suite**.

Модуль обновления представляет собой скрипт, написанный на языке Perl, и располагается в директории, содержащей исполняемые файлы программы (по умолчанию `/opt/drweb/update.pl`). Настройки Модуля обновления хранятся в секции [Updater] главного конфигурационного файла (по умолчанию `/etc/drweb/drweb32.ini`). Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске скрипта.

При установке пакета **drweb-updater** создается задание на периодический (раз в полчаса) запуск скрипта `update.pl` с помощью стандартного планировщика (cron). Для этого в каталоге `/etc/cron.d` создается файл `drweb-update` со следующей строкой:

```
*/30 * * * * drweb /opt/drweb/update.pl
```




Секция [Updater] конфигурационного файла содержит следующие параметры (табл. 7):

Таблица 7. Параметры модуля обновления.

Параметр	Комментарий
Section	<p>Указывает, какой компонент будет обновляться. Может быть установлено одно из следующих значений:</p> <ul style="list-style-type: none">• Daemon - для обновления демона;• Scanner - для обновления сканера. <p>По умолчанию установлено значение Daemon.</p> <p>Данные о расположении обновляемых файлов будут получены из соответствующих секций конфигурационного файла. Значение может быть переопределено при запуске модуля обновления при помощи параметра командной строки <code>--what</code>.</p>
ProgramPath = <путь к файлу>	<p>Путь к исполняемому файлу обновляемого компонента. Требуется модулю обновления для получения информации о версии компонента.</p> <p>По умолчанию указан путь <code>%bin_dir/drwebd</code>.</p>
SignedReader = <путь к файлу программы>	<p>Путь к файлу программы чтения подписанных файлов.</p> <p>По умолчанию указан путь <code>%bin_dir/read_signed</code>.</p>
LzmaDecoderPath = <путь к файлу программы>	<p>Путь к файлу программы для распаковывания Lzma-архивов.</p>
LockFile = <путь к файлу>	<p>Путь к файлу, предназначенному для предотвращения совместного использования некоторых файлов на время их обработки модулем обновления.</p> <p>По умолчанию указан путь <code>%var_dir/run/update.lock</code>.</p>



Параметр	Комментарий
CronSummary	<p>Данный параметр служит для того, чтобы включить/выключить использование стандартного вывода (stdout) для отчета сессии обновления и может принимать следующие значения:</p> <ul style="list-style-type: none">• Yes для использования стандартного вывода;• No для отмены использования стандартного вывода. <p>По умолчанию установлено значение Yes.</p>
DrlFile = <путь к файлу>	<p>Путь к специальному файлу, содержащему список серверов обновления. Модуль обновления выбирает сервера обновления из этого списка случайным образом.</p> <p>По умолчанию указан путь %var_dir/bases/update.drl.</p> <p> Данный файл подписан «Доктор Веб», не подлежит редактированию пользователем и обновляется автоматически.</p>
Timeout	<p>Максимальное время ожидания (в секундах) для загрузки. По умолчанию установлено значение 90 секунд.</p>
Tries	<p>Количество попыток установки соединения модулем обновления.</p> <p>По умолчанию установлено значение 3.</p>
LogFileName = <полное имя файла>	<p>Имя файла отчета. В качестве имени можно указать значение syslog, тогда отчет будет вестись средствами системного сервиса syslogd.</p> <p>По умолчанию установлено значение syslog.</p>
SyslogFacility = <полное имя файла>	<p>Тип записи при использовании системного сервиса syslogd. Может быть установлено одно из следующих значений: Daemon, Local0 .. Local7, Kern, User, Mail.</p> <p>По умолчанию установлено значение Daemon.</p>



Параметр	Комментарий
LogLevel	Уровень подробности ведения файла отчета. Может быть установлено одно из следующих значений: Debug , Verbose , Info , Warning , Error , Quiet . По умолчанию установлено значение Verbose .

Кроме того, в секции [Updater] содержатся параметры для [подключения через прокси](#).



8. Регистрация событий

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

- журнале регистрации событий операционной системы (syslog);
- отладочном журнале debug почтового сервера Kerio.

Информация об обновлениях также регистрируется программой, настроить регистрацию событий модуля обновления можно с помощью соответствующих [параметров](#) секции [Updater] конфигурационного файла.

Журнал операционной системы

В журнал регистрации операционной системы (syslog) заносится следующая информация:

- сообщения о запуске и остановке программы;
- параметры лицензионного ключевого файла: действительность или недействительность лицензии, срок действия лицензии (информация заносится при запуске программы, в процессе ее работы и при замене лицензионного ключевого файла);
- параметры модулей программы (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).



Сообщения журнала обычно находятся в файле `/var/log/messages` (RedHat, SUSE) или `/var/log/syslog` (Debian). Дополнительную информацию о системном журнале вы можете найти в документации по используемой операционной системе.

Журнал отладки

В журнал `debug` почтового сервера Kerio заносится отладочная информация, которая используется при поиске и анализе ошибок работы программы **Dr.Web для Kerio MailServer**.

Включение регистрации событий программы в журнал `debug`

1. Запустите Консоль управления **Administration Console для Kerio MailServer**.
2. В разделе **Протоколы** выберите журнал **debug**.
3. Щелкните правой кнопкой мыши в любой точке окна журнала `debug` и выберите пункт **Сообщения**.
4. Выберите пункт **Antivirus checking** в окне **Протоколирование сообщений**. Нажмите кнопку **ОК**.



9. Диагностика

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

- [проверка корректности установки](#)
- [проверка работы программы](#)

Проверка установки

Чтобы проверить корректность установки, удостоверьтесь, что следующие папки созданы и содержат все необходимые файлы:

Директория	Имя файла	Описание
/opt/drweb	drwebd	Антивирусный демон
	update.pl	Скрипт обновления
	drwebd.key	Ключевой файл антивирусного демона drwebd
	drweb-agent	Компонент Dr.Web Enterprise Agent
	drweb-monitor	Компонент Dr.Web Monitor
/etc/drweb	drwebd.enable	Включение/отключение демона drwebd
	drweb-monitor.enable	Включение/отключение Dr.Web Monitor
/opt/drweb/kerio	avir_drweb.so	Библиотека антивирусного приложения Dr.Web для Kerio MailServer
/opt/kerio/mailserver/plugins/avirs	avir_drweb.so	Ссылка на файл /opt/drweb/kerio/avir_drweb.so



Проверка работоспособности

Для проверки работоспособности программы необходимо убедиться в способности программы обнаруживать вирусы, а также в корректности работы модуля обновления.

Проверка работы программы

1. Отправьте письмо с тестовым зараженным файлом EICAR-Test-File во вложении через сервер Kerio. Информацию о тестовом вирусе EICAR можно найти по адресу http://en.wikipedia.org/wiki/EICAR_test_file.
2. Проверьте полученное письмо. Инфицированный вложенный файл должен быть удален из письма.



10. Приложения

Приложение А. Интеграция с Dr.Web Enterprise Suite

Dr.Web для Kerio MailServer может функционировать в сети, защищенной корпоративным решением **Dr.Web® Enterprise Suite**. Данное решение по организации 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. Подключение к системам централизованной защиты позволяет получить гарантированно высокий уровень защиты компьютера при минимальных усилиях со стороны конечных пользователей.

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



Dr.Web для Kerio MailServer версии 6.00 совместим с **Dr. Web Enterprise Suite** версии 6.0 и выше.

Для приложения **Dr.Web для Kerio MailServer**, работающего в режиме централизованной защиты, реализованы следующие возможности:



- регистрация запуска и остановки почтового сервера Kerio с установленным приложением **Dr.Web для Kerio MailServer**. События запуска и остановки будут отображаться в таблице **Запуск/Завершение** сервера **Dr. Web Enterprise Suite**;
- отправка статистики работы программы **Dr.Web для Kerio MailServer**. Статистика работы отображается в таблицах **Статистика** и **Суммарная статистика** сервера **Dr.Web Enterprise Suite Server**;
- отправка оповещений об обнаружении вирусов, а также информации об инфекциях и предпринятых действиях. Эти события отображаются в таблице **Инфекции** сервера **Dr. Web Enterprise Suite Server**;
- обновление антивирусных баз и антивирусного ядра из репозитория **Dr.Web Enterprise Suite**. Это позволяет отключить стандартный модуль обновления **Dr.Web Updater**, запускаемый по расписанию. В этом случае обновление компонентов будет выполняться согласно расписанию **Dr.Web Enterprise Suite** и из его репозитория;
- использование лицензионного ключевого файла **Dr.Web для Kerio MailServer**, зарегистрированного для данной станции в сети **Dr.Web Enterprise Suite**. Для этого необходимо перевести **Dr.Web Enterprise Agent** в режим **Enterprise**, установив значение **Yes** для параметра `UseEnterpriseMode` в конфигурационном файле `/etc/drweb/agent.conf`.



В режиме **Enterprise Dr.Web для Kerio MailServer** не использует локальный лицензионный ключевой файл, указанный в конфигурационном файле `/etc/drweb/agent.conf` в качестве значения параметра `LicenseFile` раздела `[StandaloneMode]`. В режиме **Enterprise** ключ запрашивается у **Dr.Web Enterprise Suite**, и если ключ не получен, программа не осуществляет антивирусную проверку.



Предметный Указатель

Д

- Dr.Web Enterprise Agent 18
- Dr.Web Enterprise Suite 18, 44
- Dr.Web Monitor 18, 26
- Dr.Web для Kerio MailServer
 - карантин 35
 - компоненты 18, 25
 - обновление 36
 - основные функции 6
 - параметры 29
 - проверка работы 42, 43
 - удаление 22
 - установка 19

К

- Kerio Connect 17
- Kerio MailServer 17

S

- syslog 40

А

- антивирусная проверка 32
- антивирусные базы 33
 - обновление 36

В

- вирусная проверка 32

Д

- демон 18, 25
- диагностика 42, 43

И

- интеграция с Dr.Web Enterprise Suite 44
- интернет-подключение 27

К

- карантин 35
- ключ 9
- ключевой файл 11
 - действительность 9
 - использование 12
 - параметры 13
 - получение 10
 - формат 13
- компоненты программы 18, 25
- консольный сканер 18

Л

- лицензионный ключевой файл 9, 11
- лицензирование 9
- лицензия
 - использование 12
 - обновление 11
 - параметры 13
 - получение 10



Предметный Указатель

М

- методы обнаружения вирусов 33
- модуль обновления 18
 - настройка 36

Н

- настройка 27
 - Dr.Web Monitor 26
 - демона 25
 - карантина 35
 - компонентов программы 25
 - подключения 27
 - прокси 27

О

- обновление
 - антивирусных баз 36
 - лицензии 11
 - настройка 36
- обновление лицензии 11
- объекты проверки 32
- операционная система 17
- отладочный журнал 41

П

- параметры
 - Dr.Web для Kerio MailServer 29
 - антивируса 28, 29
- параметры лицензирования 13
- подключение

- Dr.Web для Kerio MailServer 28
- подключение к Интернет 27
- получение ключевого файла 10
- почтовый сервер 17
- приложение 44
- проверка
 - методы 33
 - на вирусы 32
 - установки 42
 - функционирования 42, 43
- прокси 27

Р

- регистрация событий 40

С

- системные требования 17
- сканер 18
- события 40
 - журнал операционной системы 40
- журнал отладки 41
- журналы регистрации 40
- регистрация 40

Т

- техническая поддержка 8
- требования 17



Предметный Указатель

У

удаление Dr.Web для Kerio MailServer
15, 22

условные обозначения 7

установка Dr.Web для Kerio
MailServer 15, 19

 проверка 42

Ф

файл ключа 9

формат ключевого файла 13

