Dr.WEB®

для Kerio MailServer

Защити созданное

Руководство администратора

Dr.Web для Kerio MailServer
Версия 6.00.2
Руководство администратора
07.03.2013

«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

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 (Таблица 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.
Зеленое подчеркивание	Ссылки на разделы документа и веб-сайты.
`Моноширинный`	Примеры программного кода, вводимый пользователем и выводимый программой текст
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.

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 (Таблица 2).

Таблица 2. Параметры ключевого файла.

Параметр	Комментарий
Группа `[Key]`, параметр `Applications`	Указывает компоненты программы, которые разрешено использовать владельцу лицензии. Для использования ключа с программой **Dr.Web для Kerio MailServer** в списке компонентов обязательно должен присутствовать компонент KerioPlugin. 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.
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`	Указывает на разрешение (**Yes**) или запрет (**No**) использования ключа на почтовых серверах. Для использования ключа с продуктом **Dr.Web для Kerio MailServer** значение данного параметра обязательно должно быть **Yes**, иначе ключевой файл будет считаться недействительным.

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-kerio_6.0.2.*[patch]*-*[build]*~linux_x86.run** (вместо *[patch]* указывается номер обновления, вместо *[build]* – номер сборки, например, drweb-kerio_6.0.2.0-1109201904~linux_x86.run) и может быть установлена через графический интерфейс и консоль управления. В архиве содержатся следующие пакеты (Таблица 3):

Таблица 3. Пакеты установочного архива программы.

Название	Описание
drweb-common	Содержит: • основной конфигурационный файл `drweb32.ini`; • библиотеки; • файлы документации; • структуру директорий. В ходе установки данного пакета создаются: • пользователь **drweb**; • группа **drweb**.
drweb-bases	Содержит: • антивирусное ядро (Scan Engine); • антивирусные базы (vdb). Для установки требуется пакет drweb-common.

Название	Описание
drweb-updater	Содержит модуль обновления антивирусного ядра и антивирусных баз. Для установки требуется пакет drweb-common.
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 Agent**, необходимые библиотеки и документацию к нему. Для установки требует пакеты drweb-boost144 и drweb-common.
drweb-boost144	Содержит библиотеки, которые использует **Dr.Web 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.

Название	Описание
drweb-epm6.0.0-uninst	Содержит файлы графического деинсталлятора. Для установки требует пакет drweb-epm6.0.0-libs.
drweb-monitor	Содержит исполняемые файлы **Dr.Web Monitor**, необходимые библиотеки и документацию к нему. Для установки требует пакеты drweb-boost144 и drweb-common.

Дополнительную информацию об использовании антивирусного программного обеспечения на почтовом сервере Kerio вы можете найти на официальном сайте компании по адресу http://www.kerio.ru/kms_home.html.

Системные требования

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

Таблица 4. Системные требования.

Компонент	Требование
Место на жестком диске	Не менее 290 МБ свободного дискового пространства.
Операционная система	Одна из следующих: • 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.

Компонент	Требование
Почтовый сервер	Если вы впервые устанавливаете **Dr.Web для Kerio MailServer**, возможно использование следующих версий почтового сервера: • Kerio MailServer 6.2 или выше; • Kerio Connect версий с 7.0.0 по 7.4.3. Если у вас уже установлено приложение **Dr.Web для Kerio MailServer**, возможно обновление почтового сервера Kerio Connect до версии 8.0 включительно. **Dr.Web для Kerio MailServer** при этом продолжит корректно функционировать.
Прочее ПО	**Dr.Web Agent 6.0** или выше (для работы в режиме централизованной защиты)

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 Agent** – это постоянно загруженный модуль, который передает компонентам параметры их конфигурации. Кроме того, **Dr.Web Agent** управляет политиками антивирусной проверки, в зависимости от активной лицензии **Dr.Web**
- **Веб-консоль** предназначена для просмотра через браузер информации о программе **Dr.Web для Kerio MailServer**, в частности, сведений о лицензии, обновлениях и статистике ее работы.

Установка программы

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

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

Установка с помощью графической программы установки

Чтобы установить **Dr.Web для Kerio MailServer**, выполните следующие действия:

1. Разрешите исполнение архива **drweb-kerio_6.0.2.*[patch]*-*[build]*~linux_x86.run** (вместо *[patch]* указывается номер обновления, вместо *[build]* – номер сборки, например, drweb-kerio_6.0.2.0-1109201904~linux_x86.run). Вы можете воспользоваться следующей командой:

   ```
   # chmod +x drweb-kerio_6.0.2.[patch]-[build]~linux_x86.run
   ```

2. Запустите файл на исполнение следующей командой:

   ```
   # ./drweb-kerio_6.0.2.[patch]-[build]~linux_x86.run
   ```

3. Во время распаковки будет создана директория drweb-kerio_6.0.2.[patch]-[build]~linux_x86. Далее запустится графическая программа установки (см. Рисунок 1).

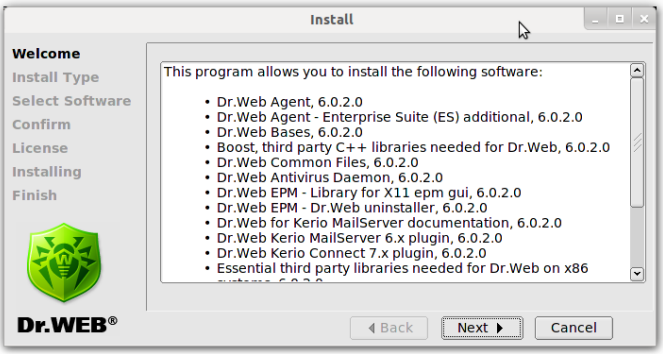

Рисунок 1. Окно начала установки программы

Навигация между окнами установки программы осуществляется с помощью кнопок **Back** и **Next**. Вы можете прервать установку в любой момент, для этого нажмите кнопку **Cancel**.

4. На шаге **Install type** (см. Рисунок 2) выберите установочный пакет в зависимости от версии почтового сервера Kerio. Нажмите кнопку **Next**.

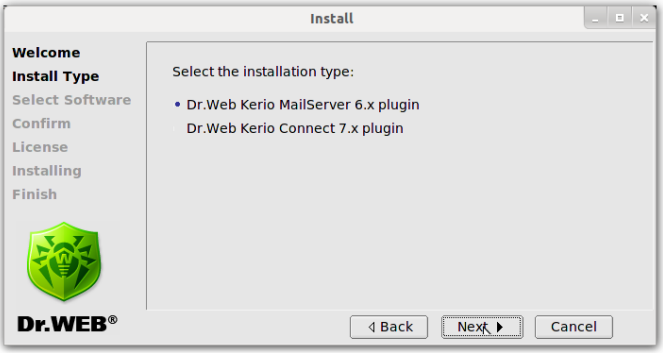

Рисунок 2. Окно выбора типа установки

5. На шаге **Select Software** (см. Рисунок 3) вы можете выбрать компоненты для установки.

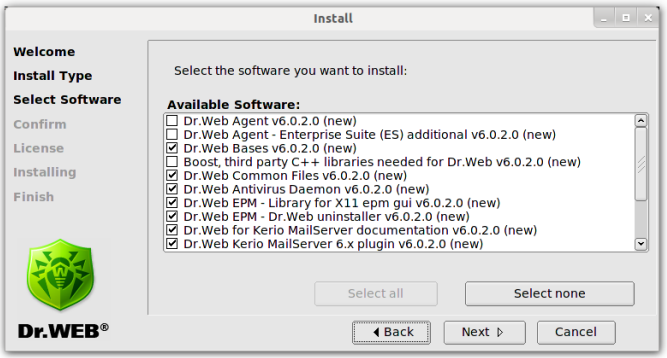

Рисунок 3. Окно выбора компонентов для установки

Если для установки какого-либо выбранного компонента должен быть предварительно установлен другой компонент, соответствующая зависимость будет отмечена автоматически. Таким образом, если вы выберете компонент **Dr.Web Antivirus Daemon**, автоматически будут выбраны компоненты **Dr.Web Bases** и **Dr.Web Common Files**.

Чтобы выбрать все компоненты, нажмите кнопку **Select all**. Чтобы снять флажки напротив всех выбранных компонентов, нажмите кнопку **Select none**. Нажмите кнопку **Next**, когда выберете все необходимые компоненты.

6. На шаге **Confirm** (см. Рисунок 4) проверьте список выбранных на предыдущем шаге компонентов и подтвердите их установку, нажав кнопку **Next**.

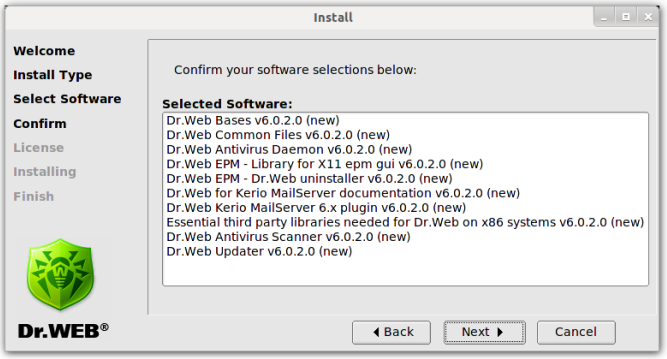

Рисунок 4. Окно подтверждения установки компонентов

7. На шаге **License** (см. Рисунок 5) прочтите лицензионное соглашение (вы можете выбрать язык отображения лицензионного соглашения в списке **Select language**). Для продолжения установки его необходимо принять. Далее нажмите кнопку **Next**.

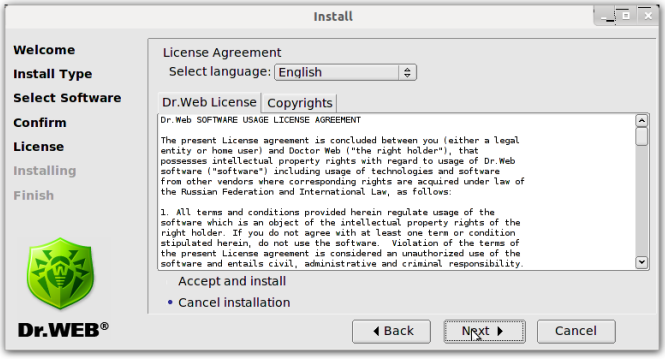

Рисунок 5. Окно Лицензионного соглашения

8. Начнется установка программы **Dr.Web для Kerio MailServer** на ваш компьютер. Отчет о процессе установки будет показан в окне **Installing** (см. Рисунок 6) в режиме реального времени.

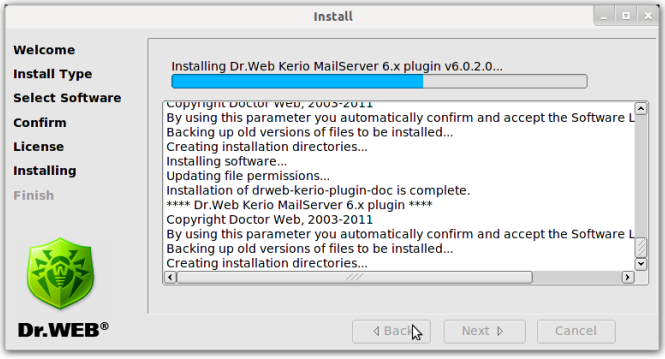

Рисунок 6. Окно прогресса установки программы

9. В случае 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 `/opt/drweb`;
   - путь к ключевому файлу будет записан в конфигурационные файлы **Dr.Web Agent** и демона **drwebd**;
   - для **Dr.Web Monitor** и демона **drwebd** будет настроен автоматический запуск;
   - будет осуществлен запуск **Dr.Web Monitor** и демонов **drwebd** и **drweb-kerio-webstatd**.
10. На шаге **Finish** нажмите кнопку **Close** (см. Рисунок 7) чтобы завершить работу программы установки.

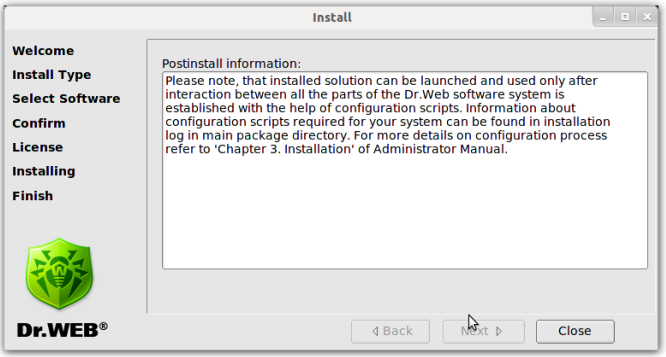

Рисунок 7. Окно завершения установки программы

Установка программы из консоли

Программа **Dr.Web для Kerio MailServer** может быть установлена без использования графической программы установки. Обычно программа установки из консоли (см. Рисунок 8) запускается автоматически в том случае, если не удалось запустить графическую программу установки.

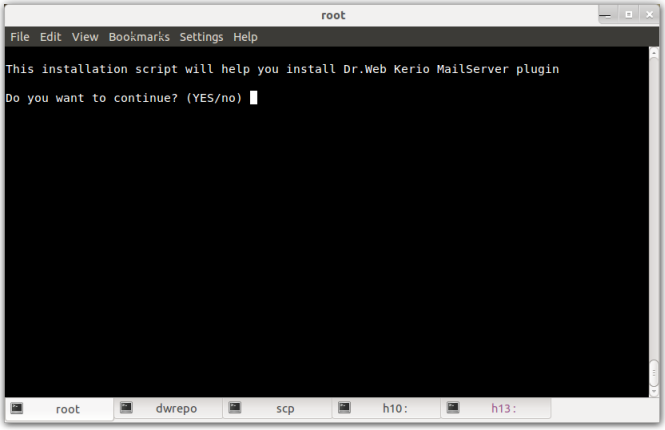

Рисунок 8. Установка программы из консоли

1. Для продолжения установки **Dr.Web для Kerio MailServer** введите `Y` или `Yes` в строке ввода (значения регистронезависимы) и нажмите клавишу ENTER. В противном случае введите `N` или `No`.

2. Далее выберите установочный пакет в зависимости от версии сервера Kerio (см. Рисунок 9). Введите номер соответствующего пункта и нажмите клавишу ENTER.

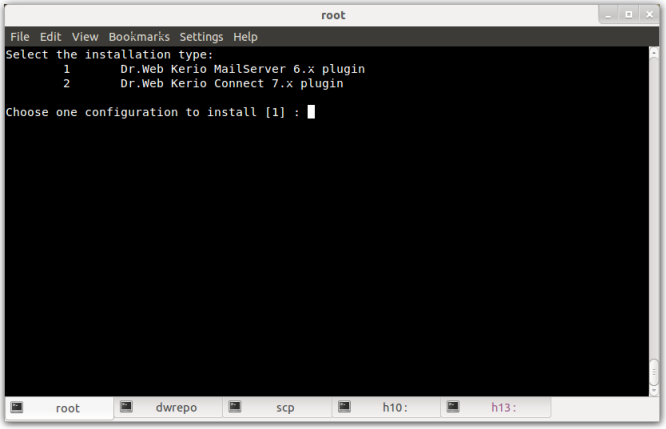

Рисунок 9. Выбор установочного пакета

3. Откроется Лицензионное Соглашение (см. Рисунок 10). Для прокрутки текста используйте клавишу ПРОБЕЛ. Для продолжения установки требуется принять Лицензионное Соглашение. Для этого введите `Y` или `Yes` в строке ввода и нажмите клавишу ENTER. В противном случае установка будет прекращена.

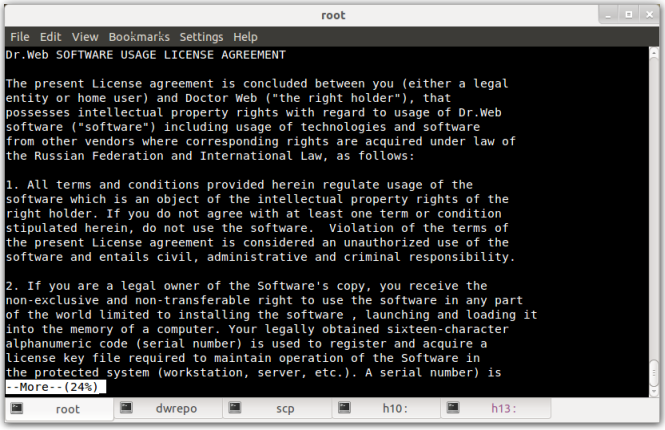

Рисунок 10. Лицензионное соглашение

4. Начнется установка программы **Dr.Web для Kerio MailServer** на ваш компьютер. Отчет о результатах прохождения каждого из этапов установки будет выводиться на экран в режиме реального времени (см. Рисунок 11).

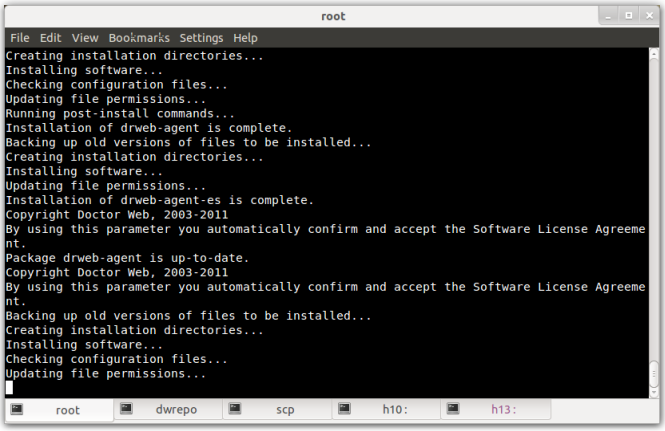

Рисунок 11. Прогресс установки программы

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

Удаление программы

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

Перед удалением программы 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.

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

Удаление с помощью графической программы удаления

Чтобы удалить **Dr.Web для Kerio MailServer**, выполните следующие действия:

1. Запустите графическую программу удаления (см. Рисунок 12) с помощью команды `# /opt/drweb/remove.sh`.

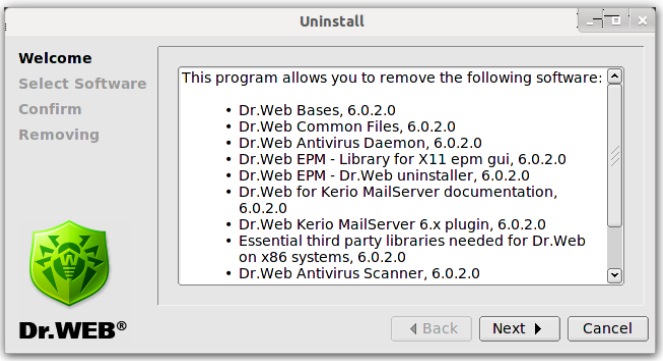

Рисунок 12. Окно удаления программы

Навигация между окнами удаления программы осуществляется с помощью кнопок **Back** и **Next**. Вы можете прервать удаление в любой момент, для этого нажмите кнопку **Cancel**.

2. На шаге **Select Software** (см. Рисунок 13) выберите компоненты, которые вы хотите удалить. Для этого установите флажки напротив этих компонентов. При этом, для зависимых компонентов флажки будут установлены автоматически.

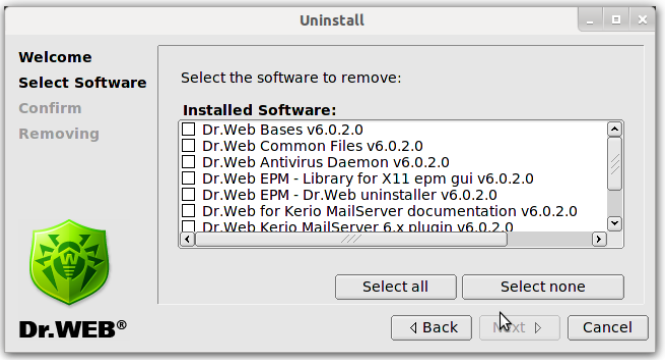

Рисунок 13. Окно выбора компонентов для удаления

В случае, если ранее на этом компьютере был установлен какой-либо другой продукт **Dr.Web**, в списке компонентов для удаления будут также присутствовать его модули. Поэтому необходимо быть крайне внимательным при выборе, чтобы случайно не удалить те компоненты, которые планируется использовать в дальнейшем.

Чтобы выбрать все компоненты, нажмите кнопку **Select all**. Чтобы снять флажки напротив всех выбранных компонентов, нажмите кнопку **Select none**. Нажмите кнопку **Next**, когда выберете все необходимые компоненты.

3. На шаге **Confirm** (см. Рисунок 14) проверьте список выбранных на предыдущем шаге компонентов и подтвердите их удаление, нажав кнопку **Next**.

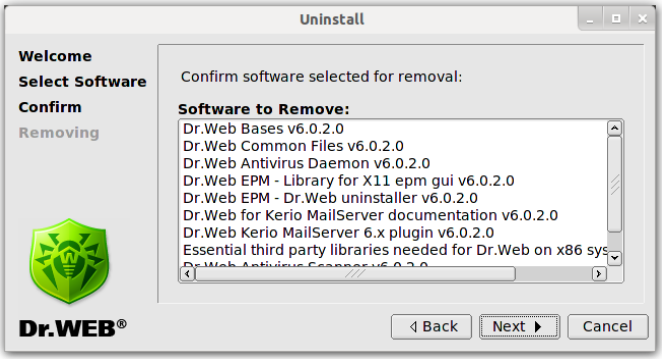

Рисунок 14. Окно подтверждения удаления компонентов

4. Начнется процесс удаления программы **Dr.Web для Kerio MailServer**. Отчет о данном процессе будет показан в окне **Removing** (см. Рисунок 15) в режиме реального времени.

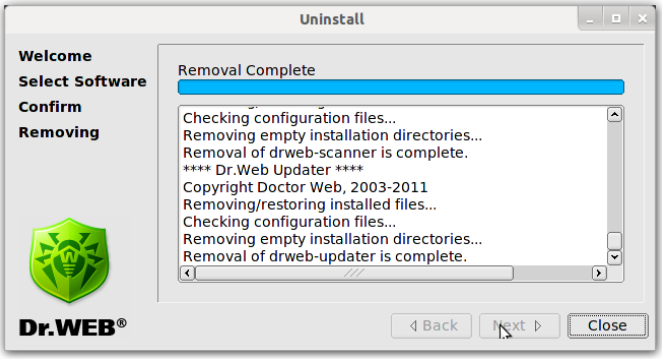

Рисунок 15. Окно удаления компонентов программы

По окончании удаления нажмите кнопку **Close**, чтобы закрыть окно программы удаления компонентов.

Удаление программы из консоли

Чтобы удалить **Dr.Web для Kerio MailServer** без использования графической программы удаления, выполните следующие действия:

1. Выполните команду `# /opt/drweb/remove.sh`. Программа удаления из консоли (см. Рисунок 16) запускается автоматически в том случае, если не удалось запустить графическую программу удаления.

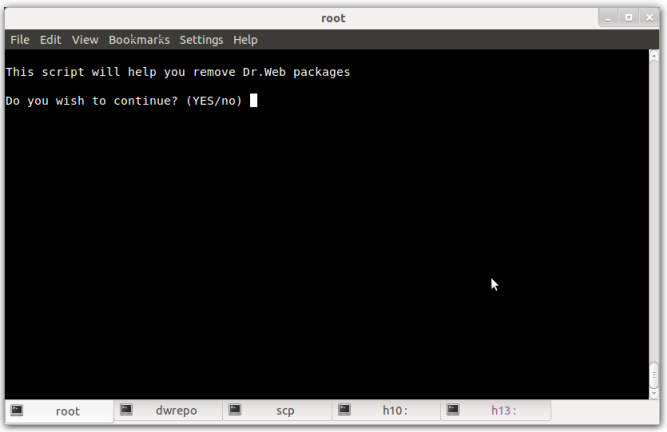

Рисунок 16. Удаление программы из консоли

Для продолжения удаления **Dr.Web для Kerio MailServer** введите `Y` или `Yes` в строке ввода (значения регистронезависимы) и нажмите клавишу ENTER. В противном случае введите `N` или `No`.

2. На следующем шаге (см. Рисунок 17) выберите компоненты, которые вы хотите удалить (следуйте инструкциям на экране).

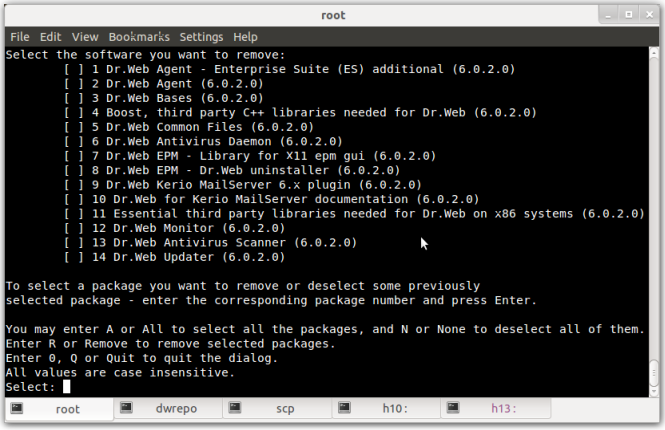

Рисунок 17. Выбор компонентов для удаления

3. Подтвердите удаление выбранных компонентов (см. Рисунок 18). Для этого введите `Y` или `Yes` в строке ввода (значения регистронезависимы) и нажмите клавишу ENTER.

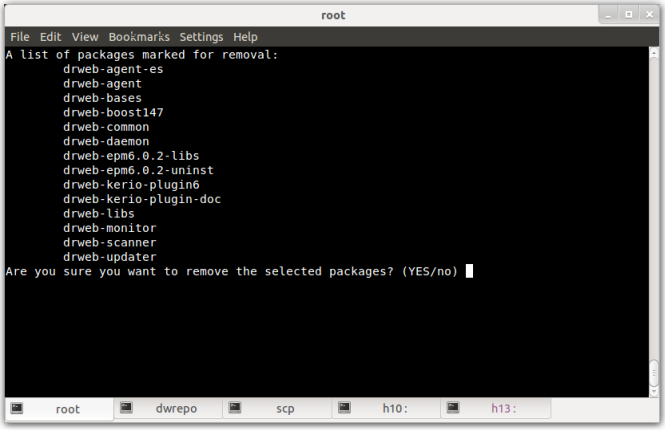

Рисунок 18. Подтверждение удаления выбранных компонентов

4. Начнется процесс удаления выбранных компонентов. Отчет о результатах прохождения каждого из этапов данного процесса выводится на экран в режиме реального времени (см. Рисунок 19).

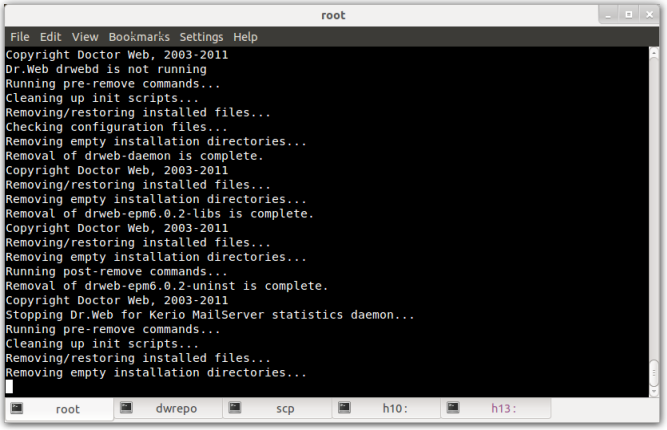

Рисунок 19. Удаление компонентов программы

5. По окончании процесса удаления будет выведено сообщение о том, что выбранные компоненты успешно удалены.

Установка и удаление из нативных пакетов

Вы можете установить **Dr.Web для Kerio MailServer** из нативных пакетов для распространенных дистрибутивов Linux.

Установка из нативных пакетов возможна только для Kerio Connect 7.0 и выше.

Пакеты находятся в официальном репозитории **Dr.Web** по адресу http://officeshield.drweb.com/drweb/. После подключения репозитория к менеджеру пакетов вашей системы, вы можете устанавливать пакеты как любую другую программу из репозитория. Необходимые зависимости будут разрешены автоматически.

После установки пакетов через репозиторий не будет запущен пост-инсталляционный скрипт для автоматической установки лицензионного ключевого файла. Ключевой файл необходимо скопировать вручную. После обновления через репозиторий все сервисы **Dr.Web** необходимо перезапустить, чтобы обновления вступили в силу.

Ниже приведены инструкции для подключения репозитория **Dr.Web** к поддерживаемым менеджерам пакетов и установки **Dr.Web для Kerio MailServer** с помощью консоли.

Все описанные ниже команды для подключения репозиториев, импортирования ключей, установки и удаления пакетов должны быть выполнены с правами администратора (root).

Debian, Ubuntu (apt)

1. Репозиторий для Debian защищен с помощью механизма цифровой подписи. Для корректной работы требуется импортировать ключ цифровой подписи с помощью одной из команд:

   ```
   wget -O - http://officeshield.drweb.com/drweb/drweb.key | apt-key add -
   ```

   или

   ```
   curl http://officeshield.drweb.com/drweb/drweb.key | apt-key add -
   ```

2. Чтобы подключить репозиторий, добавьте в файл `/etc/apt/sources.list` следующую строку:

```
deb http://officeshield.drweb.com/drweb/debian stable non-free
```

3. Чтобы установить **Dr.Web для Kerio MailServer**, выполните следующие команды:

```
apt-get update

apt-get install drweb-kerio
```

4. Чтобы удалить **Dr.Web для Kerio MailServer**, выполните команду:

```
apt-get remove drweb-kerio
```

Кроме того, установка и удаление пакетов могут быть осуществлены с помощью графического менеджера (например, Synaptic).

Обратите внимание, что при установке из нативных пакетов, файл `drwebd.enable` будет расположен следующим образом:

- `/etc/defaults` – для deb пакетов;
- `/etc/sysconfig` – для rpm пакетов.

Red Hat Enterprise Linux, Fedora, CentOS (yum)

1. В директорию `/etc/yum.repos.d` добавьте файл со следующим содержанием:

```
[drweb]

name=DrWeb - stable

baseurl=http://officeshield.drweb.com/drweb/

el5/stable/i386/

gpgcheck=1

enabled=1
```

```
gpgkey=http://officeshield.drweb.com/drweb/

drweb.key
```

2. Чтобы установить **Dr.Web для Kerio MailServer**, выполните команду:

```
yum install drweb-kerio
```

3. Чтобы удалить **Dr.Web для Kerio MailServer**, выполните команду:

```
yum remove drweb-kerio
```

Кроме того, установка и удаление пакетов могут быть осуществлены с помощью графического менеджера (например, PackageKit, Yumex).

SUSE Linux (Zypper)

1. Чтобы подключить репозиторий, запустите следующую команду:

```
zypper ar -t YUM http://officeshield.drweb.com/drweb/
el5/stable/i386/ drweb
```

или

```
zypper ar -t YUM http://officeshield.drweb.com/drweb/
el5/stable/x86_64/ drweb
```

2. Чтобы установить **Dr.Web для Kerio MailServer**, выполните следующие команды:

```
zypper refresh

zypper install drweb-kerio
```

3. Чтобы удалить **Dr.Web для Kerio MailServer**, выполните команду:

```
zypper remove drweb-kerio
```

Кроме того, установка и удаление пакетов могут быть осуществлены с помощью графического менеджера (например, YaST).

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, демона для работы с веб-консолью 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 drwebd

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.

Запуск и настройка демона drweb-kerio-webstatd

Для работы с веб-консолью необходимо запустить демон **drweb-kerio-webstatd** с помощью следующей команды:

```
/etc/init.d/drweb-kerio-webstatd start
```

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]` (Таблица 5):

Таблица 5. Параметры подключения к прокси.

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

5. Подключение и настройка работы 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 (Таблица 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) Detect dialers (Yes/No) Detect hacktools (Yes/No) Detect jokes (Yes/No) Detect riskware (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: • **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	Данная настройка задает сокет для взаимодействия с **Dr.Web Agent**. По умолчанию установлено значение **pid:/var/drweb/run/drweb-agent.pid**. Дополнительную информацию по настройке работы данного компонента вы можете найти в документации для **Dr.Web Agent**.
Dr.Web Daemon socket path	Данная настройка задает сокет для взаимодействия с антивирусным демоном **drwebd**. По умолчанию установлено значение **pid:/var/drweb/run/drwebd.pid**. 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: *<ip-address>:<port>*. Например: 192.168.100.10:3000. Дополнительную информацию по настройке проверки на удаленном компьютере вы можете найти в документации для **Dr.Web Daemon**.
Enable heuristic (Yes/No)	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: • **No** для отключения эвристического анализатора; • **Yes** для включения эвристического анализатора.

Quarantine directory	Данная настройка задает путь к директории карантина. По умолчанию установлено значение **/var/drweb/infected**.
Quarantine enabled (Yes/ No)	Данный параметр позволяет включить/ выключить перемещение инфицированных объектов в карантин. По умолчанию выбрано значение **Yes**.

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 приложением **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, удалив 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 карантином

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

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. Веб-консоль

Веб-консоль позволяет просматривать через браузер информацию о работе программы **Dr.Web для Kerio MailServer**, в частности, сведения о лицензии и обновлениях, а также статистику работы (см. Рисунок 20).

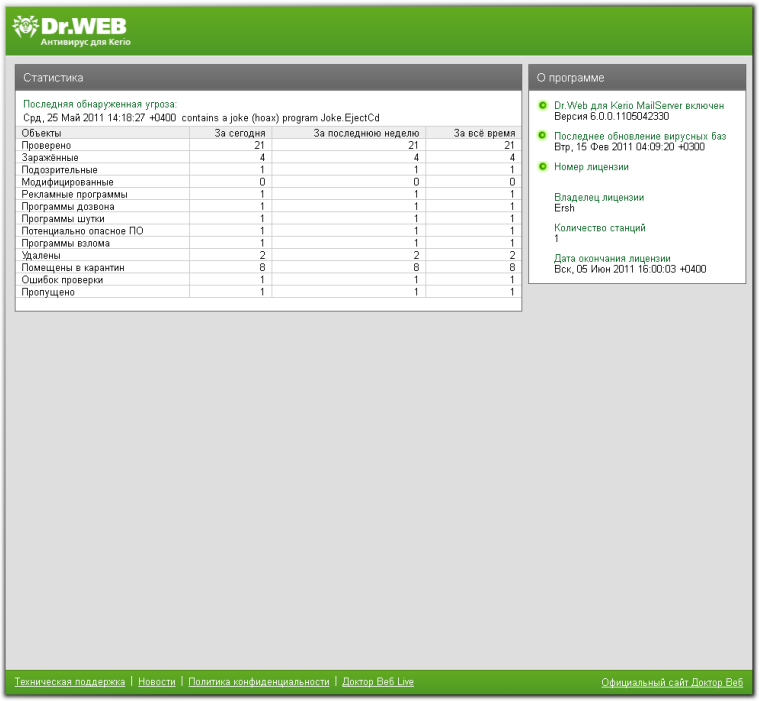

Рисунок 20. Веб-консоль

Доступ к веб-консоли

Для доступа к веб-консоли укажите в адресной строке браузера адрес в следующем формате:

`http://localhost:27182/statistics`, где `localhost` - адрес защищаемого сервера Kerio.

Информация о программе

В разделе веб-консоли **О программе** (см. Рисунок 20) отображается следующая информация об активности приложения, пользовательской лицензии и обновлениях антивирусных баз:

- версия антивирусного ядра программы;
- дата и время последнего обновления антивирусных баз программы;
- номер лицензии;
- имя владельца лицензии;
- количество защищаемых рабочих станций;
- дата окончания срока действия лицензии.

Статистика работы программы

Статистика работы программы отображается в виде таблицы (см. Рисунок 20) в разделе веб-консоли **Статистика**. С помощью веб-консоли вы можете просматривать следующую статистическую информацию:

- дату и время обнаружения последней угрозы, а также имя содержавшегося в ней вируса;
- количество проверенных файлов и обнаруженных угроз за различные периоды времени (за последние сутки, за последнюю неделю и за весь период работы приложения):
    - общее количество проверенных объектов;
    - количество инфицированных объектов;

- количество подозрительных объектов;
- количество потенциально опасных программ, рекламных программ, программ дозвона, программ-шуток, программ взлома и модифицированных программ;
- количество удаленных и перемещенных в карантин объектов;
- количество ошибок, возникших при проверке почтовых вложений
- количество пропущенных объектов.

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

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 (Таблица 7):

Таблица 7. Параметры модуля обновления.

Параметр	Комментарий
`Section`	Указывает, какой компонент будет обновляться. Может быть установлено одно из следующих значений: • **Daemon** - для обновления демона; • **Scanner** - для обновления сканера. По умолчанию установлено значение **Daemon**. 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 `--what`.
`ProgramPath = <путь к файлу>`	Путь к исполняемому файлу обновляемого компонента. Требуется модулю обновления для получения информации о версии компонента. По умолчанию указан путь %bin_dir/drwebd.
`SignedReader = <путь к файлу программы>`	Путь к файлу программы чтения подписанных файлов. По умолчанию указан путь %bin_dir/read_signed.
`LzmaDecoderPath = <путь к файлу программы>`	Путь к файлу программы для распаковывания lzma-архивов.
`LockFile = <путь к файлу>`	Путь к файлу, предназначенному для предотвращения совместного использования некоторых файлов на время их обработки модулем обновления. По умолчанию указан путь %var_dir/run/update.lock.

Параметр	Комментарий
`CronSummary`	Данный параметр служит для того, чтобы включить/выключить использование стандартного вывода (stdout) для отчета сессии обновления и может принимать следующие значения: • **Yes** для использования стандартного вывода; • **No** для отмены использования стандартного вывода. По умолчанию установлено значение **Yes**.
`DrlFile = <путь к файлу>`	Путь к специальному файлу, содержащему список серверов обновления. Модуль обновления выбирает сервера обновления из этого списка случайным образом. По умолчанию указан путь %var_dir/bases/update.drl. Данный файл подписан **«Доктор Веб»**, не подлежит редактированию пользователем и обновляется автоматически.
`Timeout`	Максимальное время ожидания (в секундах) для загрузки. По умолчанию установлено значение 90 секунд.
`Tries`	Количество попыток установки соединения модулем обновления. По умолчанию установлено значение 3.
`LogFileName = <полное имя файла>`	Имя файла отчета. В качестве имени можно указать значение **syslog**, тогда отчет будет вестись средствами системного сервиса syslogd. По умолчанию установлено значение **syslog**.
`SyslogFacility = <полное имя файла>`	Тип записи при использовании системного сервиса syslogd. Может быть установлено одно из следующих значений: **Daemon**, **Local0** .. **Local7**, **Kern**, **User**, **Mail**. По умолчанию установлено значение **Daemon**.

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.

9. 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);
- сообщения 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**.

10. 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 (Таблица 8):

Таблица 8. Установленные папки и 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 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

Директория	Имя файла	Описание
/opt/drweb	drweb-kerio-webstatd	Демон веб-консоли

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.

11. Приложения

Приложение А. Работа в режиме централизованной защиты

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

Взаимодействие компонентов антивирусной сети

Решения компании **«Доктор Веб»** по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (Рисунок 21).

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

Обновление и конфигурация локальных компонентов производится через *центральный сервер*. Весь поток команд, данных и

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

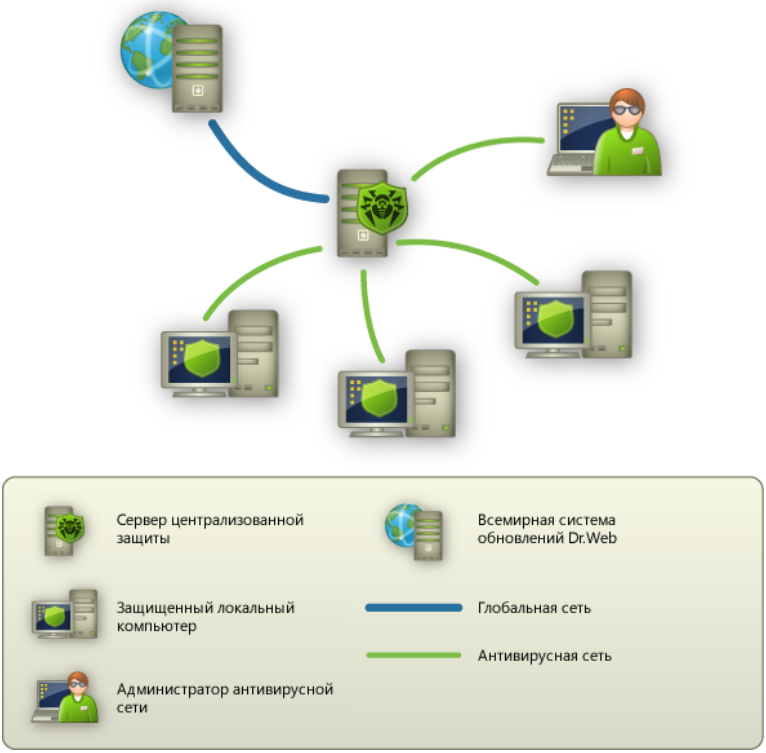

Рисунок 21. Логическая структура антивирусной сети.

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

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

Работа Dr.Web для Kerio MailServer в режиме централизованной защиты

Для работы **Dr.Web для Kerio MailServer** в режиме централизованной защиты необходимо, чтобы в операционной системе был установлен и корректно работал **Dr.Web Agent** версии 6 или выше.

Dr.Web для Kerio MailServer версии 6.00 не совместим с **Dr.Web Agent** версии 5.

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** **Центра Управления Dr.Web**;
- отправка статистики работы программы **Dr.Web для Kerio MailServer**. Статистика работы отображается в таблицах **Статистика** и **Суммарная статистика** **Центра Управления Dr.Web**;

- отправка оповещений об обнаружении вирусов, а также информации об инфекциях и предпринятых действиях. Эти события отображаются в таблице **Инфекции** **Центра Управления Dr.Web**;
- обновление антивирусных баз и антивирусного ядра из репозитория **Центра Управления Dr.Web**. Это позволяет отключить стандартный модуль обновления **Dr.Web Updater**, запускаемый по расписанию. В этом случае обновление компонентов будет выполняться согласно расписанию **Центра Управления Dr.Web** и из его репозитория;
- использование лицензионного ключевого файла **Dr.Web для Kerio MailServer**, зарегистрированного для данной станции в антивирусной сети. Для этого необходимо перевести **Dr.Web 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 **Центра Управления Dr.Web**, и если ключ не получен, программа не осуществляет антивирусную проверку.

Предметный Указатель

Предметный Указатель

Предметный Указатель

Т

У

Ф

Ц