



# Dr.WEB

для Kerio MailServer

## Руководство администратора

Жасағаныңды қорға

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Жасағаныңды қорға

Защити созданное

Proteggi ciò che crei

Verteidige, was du erschaffen hast

Захисти створене

**Defend what you create**

脅威からの保護を提供します

Protégez votre univers

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

© 2003-2017 «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!, CureNet!, AV-Desk и логотип Dr.WEB 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 6.0.6**

**Руководство администратора**

**27.03.2017**

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

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

Веб-сайт: <http://www.drweb.com/>

Телефон: +7 (495) 789-45-87

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

## **«Доктор Веб»**

«Доктор Веб» – российский разработчик средств информационной безопасности.

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

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

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

**Мы благодарны пользователям за поддержку решений семейства Dr.Web!**



# Содержание

<b>1. Введение</b>	<b>6</b>
1.1. Используемые обозначения	7
1.2. Техническая поддержка	7
<b>2. Лицензирование</b>	<b>8</b>
2.1. Лицензионный ключевой файл	8
2.2. Получение ключевого файла	8
2.3. Обновление лицензии	9
2.4. Использование ключевого файла	10
2.5. Определение параметров лицензирования	10
<b>3. Установка и удаление программы</b>	<b>12</b>
3.1. Системные требования	12
3.2. Совместимость	14
3.3. Установка программы	14
3.4. Удаление программы	15
3.5. Настройка подключения через прокси	16
<b>4. Подключение и настройка работы программы</b>	<b>17</b>
4.1. Настройка параметров проверки	17
4.2. Настройка уведомлений	20
<b>5. Проверка на вирусы</b>	<b>22</b>
5.1. Методы обнаружения вирусов	22
5.2. Карантин	24
<b>6. Веб-консоль</b>	<b>27</b>
6.1. Информация о программе	27
6.2. Статистика работы программы	28
<b>7. Обновление вирусных баз</b>	<b>29</b>
<b>8. Регистрация событий</b>	<b>30</b>
8.1. Журнал операционной системы	30
8.2. Текстовый журнал	31
8.3. Журнал отладки	31
<b>9. Диагностика</b>	<b>32</b>
9.1. Проверка установки	32
9.2. Проверка работоспособности	33



<b>10. Приложения</b>	<b>35</b>
10.1. Приложение А. Параметры командной строки для модуля обновления	35
10.2. Приложение Б. Действия в случае возникновения проблем	38
10.3. Приложение В. Работа в режиме централизованной защиты	40
<b>Предметный указатель</b>	<b>43</b>



## 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 вирусных 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/products/kerio-connect>.



## 1.1. Используемые обозначения

В данном руководстве используются следующие условные обозначения:

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

## 1.2. Техническая поддержка

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

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

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

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

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



## 2. Лицензирование

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

### 2.1. 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](#).

### 2.2. Получение ключевого файла

Вы можете получить лицензионный ключевой файл одним из следующих способов:

- в виде ZIP-архива по электронной почте;
- вместе с дистрибутивом продукта, если лицензионный файл был включен в состав дистрибутива при его комплектации;
- на отдельном носителе в виде файла с расширением .key.





### 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 <https://download.drweb.ru/demoreq/biz/v2/>.

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

## 2.3. Обновление лицензии

В некоторых случаях, например, при окончании срока действия лицензии или при изменении характеристик защищаемой системы или требований к ее безопасности, вы можете принять решение о приобретении новой или расширенной лицензии на Dr.Web 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, скопируйте новый ключевой файл в каталог установки программы (по умолчанию %ProgramFiles%\DrWeb for Kerio MailServer\).
2. Программа Dr.Web для Kerio MailServer автоматически переключится на использование нового ключевого файла.

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



## 2.4. Использование ключевого файла

При установке программы Dr.Web для Kerio MailServer ключевой файл копируется в каталог установки программы (обычно, C:\Program Files\DrWeb for Kerio MailServer). Мастер установки автоматически регистрирует ключевой файл в реестре операционной системы.

В процессе работы Dr.Web для Kerio MailServer осуществляется поиск первого рабочего ключа (по маске \*.key) в каталоге установки, начиная с ключа, указанного при установке приложения. 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.

## 2.5. 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 (например, в Блокноте).




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.
Группа [Key], параметр Expires	Указывает срок действия лицензионного ключа в формате Год-Месяц-День.



Параметр	Комментарий
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 ( <b>Yes</b> ) или запрет ( <b>No</b> ) 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.
C:\Windows\	Наименования файлов и каталогов, фрагменты программного кода.
<a href="#">Приложение А</a>	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

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. Дополнительную информацию об использовании антивирусного программного обеспечения на почтовом сервере Kerio вы можете найти на официальном сайте компании по адресу <http://www.kerio.ru/products/kerio-connect>.

### 3.1. Системные требования

Компьютер, на который устанавливается Dr.Web для Kerio MailServer, должен удовлетворять следующим системным требованиям ([Таблица 3](#)):

**Таблица 3. Системные требования**

Компонент	Требование
Место на жестком диске	Не менее 350 МБ свободного дискового пространства.
Операционная система	Одна из следующих: <ul style="list-style-type: none"><li>• Microsoft® Windows® 2000 (Professional Edition, Server, Advanced Server или Datacenter Server) с пакетом обновлений SP4 и Update Rollup 1;</li><li>• Microsoft® Windows® XP (Home Edition или Professional Edition);</li><li>• Microsoft® Windows Server® 2003 (Standard Edition, Enterprise Edition или Datacenter Edition);</li><li>• Microsoft® Windows Server® 2008 (Standard Edition, Enterprise Edition или Datacenter Edition);</li><li>• Microsoft® Windows Server® 2008 R2;</li><li>• Windows Vista® (Starter, Home Basic, Home Premium, Business, Enterprise или Ultimate);</li><li>• Microsoft® Windows 7® (Starter, Home Basic, Home Premium, Business, Enterprise или Ultimate);</li><li>• Microsoft® Windows Server® 2012 R2.</li></ul> Поддерживаются 32- и 64-битные версии операционных систем.
Почтовый сервер	Если вы впервые устанавливаете Dr.Web для Kerio MailServer, возможно использование следующих версий почтового сервера: <ul style="list-style-type: none"><li>• Kerio MailServer 6.2 или выше;</li></ul>



Компонент	Требование
	<ul style="list-style-type: none"><li>• Kerio Connect версий с 7.0.0 по 9.2.1.</li></ul>
Прочее ПО	Dr.Web Agent 6.0 или выше (для работы в режиме централизованной защиты)



Если помимо Dr.Web для Kerio MailServer в системе функционирует антивирусный файловый сторож Spider Guard, например, в составе продуктов Dr.Web for FileServers или Dr.Web Security Space, то необходимо исключить из проверки каталог выгрузки временных файлов сервера Kerio (по умолчанию, %ProgramFiles%\Kerio\MailServer\Store\tmp).

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.



## 3.2. Совместимость

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

1. Программа Dr.Web для Kerio MailServer версии 6.0.6 совместима только с продуктами Dr.Web версии 6.
2. Если помимо Dr.Web для Kerio MailServer в системе работают антивирусные приложения стороннего производителя, возможны конфликты.
3. Если помимо Dr.Web для Kerio MailServer в системе функционирует антивирусный файловый сторож Spider Guard, например, в составе продуктов Dr.Web для файловых серверов или Dr.Web Security Space, то необходимо исключить из проверки каталог выгрузки временных файлов сервера Kerio (по умолчанию, %ProgramFiles%\Kerio\MailServer\Store\tmp).
4. Перед установкой программы должны быть установлены все последние обновления, выпущенные для операционной системы.

## 3.3. 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

1. Остановите почтовый сервер Kerio MailServer/Kerio Connect.
2. Скопируйте следующие файлы на компьютер, где установлен почтовый сервер Kerio:
  - установочный файл программы;
  - лицензионный ключевой файл.
3. В зависимости от используемой операционной системы, запустите установочный файл **drweb-6.0.6-av-kerio-mail-win-x86.exe** (для 32-битной операционной системы) или **drweb-6.0.6-av-kerio-mail-win-x64.exe** (для 64-битной операционной системы).
4. Откроется окно с текстом Лицензионного соглашения. Для продолжения установки его необходимо прочитать и принять. Нажмите кнопку **Далее**.
5. Если ранее вы не остановили почтовый сервер Kerio MailServer/Kerio Connect, вам будет предложено это сделать.
6. Укажите путь к ключевому файлу. Для этого нажмите кнопку **Обзор** и выберите необходимый файл. Нажмите кнопку **Далее**.
7. На шаге **Путь к Kerio MailServer** необходимо указать путь к папке установки почтового сервера Kerio (например: C:\Program Files\Kerio\MailServer\). Нажмите кнопку **Далее**.



8. На шаге **Система готова к установке** вы можете запустить обновление программы во время установки. Для этого установите флажок **Запустить обновление** в появившемся окне.
9. Нажмите кнопку **Установить**. Начнется установка Dr.Web для Kerio MailServer на ваш компьютер.
10. После окончания установки программы вам будет предложено перезапустить операционную систему.

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

## 3.4. 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 почтового сервера Kerio;
  - откройте подраздел **Конфигурация** -> **Фильтр содержимого** -> **Антивирус**;
  - снимите флажок **Использовать внешнюю антивирусную программу** для выбранного антивируса **Dr.Web for Kerio Mail Servers**;
  - нажмите кнопку **Применить**. Использование Dr.Web для Kerio MailServer будет отключено.
2. Для удаления Dr.Web для Kerio MailServer выполните одно из следующих действий:
  - откройте **Панель управления** и выберите пункт **Установка и удаление программ**. В окне **Установка и удаление программ** выберите программу **Dr.Web for Kerio Mail Servers** и нажмите кнопку **Удалить**. Откроется окно подтверждения удаления. Нажмите кнопку **Да**;
  - запустите установочный файл программы **drweb-6.0.6-av-kerio-mail-win-x86.exe** или **drweb-6.0.6-av-kerio-mail-win-x64.exe** в зависимости от используемой версии операционной системы. Откроется окно Мастера установки. Нажмите **Удалить программу**. На следующем шаге подтвердите удаление программы. По окончании удаления вам будет предложено перезагрузить компьютер.
3. Компоненты программы и задание на обновление вирусных баз будут удалены.



Лицензионный ключевой файл, а также файл статистики и программный журнал регистрации событий не удаляются по умолчанию. Вы можете удалить оставшиеся файлы вручную из каталога установки приложения (по умолчанию %ProgramFiles%\DrWeb for Kerio MailServer).



## 3.5. Настройка подключения через 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.

### Настройка подключения к прокси-серверу

1. Чтобы настроить параметры соединения с прокси-сервером, запустите на исполнение файл `drwebupw.exe`, хранящийся в папке установки программы Dr.Web для Kerio MailServer (обычно, `C:\Program Files\DrWeb for Kerio MailServer`).
2. В открывшемся окне нажмите **Settings**.
3. В окне настроек откройте вкладку **Proxy**.
4. Укажите IP-адрес и порт прокси-сервера.
5. При необходимости, в поле **User name** введите имя пользователя, а в поле **Password** – пароль для доступа к прокси-серверу. Если прокси-сервер разрешает анонимный доступ, оставьте поля пустыми.
6. Нажмите **OK**.





## 4. 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 почтового сервера Kerio.
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. Нажмите кнопку **Параметры** справа от выбранной антивирусной программы. Откроется список параметров программы, с помощью которых вы можете настроить [проверку на вирусы](#), [рассылку уведомлений](#) и параметры работы с [веб-консолью](#). 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**.
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/products/kerio-connect>.

### 4.1. Настройка параметров проверки

С помощью данной группы параметров вы можете настроить проверку архивов, задать действия программы для различных типов вредоносного ПО, а также включить использование карантина ([Таблица 4](#)).

**Таблица 4. Параметры проверки**

Параметр	Комментарий
Engine: Check archives (0, 1)	Данный параметр позволяет настроить проверку архивов во вложениях электронных писем. Вы можете указать одно из двух значений параметра: <ul style="list-style-type: none"><li>• <b>0</b> для отключения проверки архивов;</li></ul>




Параметр	Комментарий
	<ul style="list-style-type: none"><li>• <b>1</b> для включения проверки архивов.</li></ul> <p>По умолчанию проверка архивов включена.</p>
Engine: Detect adware (0, 1) Engine: Detect dialers (0, 1) Engine: Detect hacktools (0, 1) Engine: Detect jokes (0, 1) Engine: Detect riskware (0, 1)	<p>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:</p> <ul style="list-style-type: none"><li>• <b>0</b> означает, что объекты, содержащие данный тип вредоносного ПО, будут пропущены;</li><li>• <b>1</b> запрещает передачу подобных объектов. Данное значение установлено по умолчанию для всех типов вредоносных объектов.</li></ul>
Engine: Enable heuristic (0, 1)	<p>С помощью данного параметра вы можете включить или отключить эвристический анализатор, позволяющий обнаруживать неизвестные вирусы. Вы можете указать одно из двух значений параметра:</p> <ul style="list-style-type: none"><li>• <b>0</b> для отключения эвристического анализатора;</li><li>• <b>1</b> для включения эвристического анализатора.</li></ul> <p>По умолчанию эвристический анализатор включен</p>
Quarantine: Enabled (0, 1)	<p>Данный параметр позволяет включить/выключить перемещение инфицированных объектов в карантин.</p> <p>По умолчанию использование карантина включено.</p>
Engine: Max archive level	<p>Данная настройка определяет максимальную глубину вложенности архива. Если глубина вложенности проверяемого архива превысит указанное значение, то к объекту будут применены действия, заданные настройками почтового сервера Kerio для случая, когда проверка объекта невозможна.</p> <p>По умолчанию установлено значение 16.</p>
Engine: Max archive size (KB)	<p>Данная настройка определяет максимально допустимый размер (в килобайтах) файла архива. Если размер файла архива превысит указанное значение, то к объекту будут применены действия, заданные настройками почтового сервера Kerio для случая, когда проверка объекта невозможна.</p> <p>По умолчанию установлено значение 0 КБ (неограниченный размер файла архива).</p>
Engine: Max scan time (ms)	<p>Данный параметр определяет максимально допустимое время проверки объекта (в миллисекундах). Если время проверки объекта превысит указанное значение, то к такому объекту будут применены действия, заданные</p>



Параметр	Комментарий
	настройками почтового сервера Kerio для случая, когда проверка объекта невозможна.  По умолчанию установлено значение 0 мс (неограниченное время проверки).

С помощью данной группы параметров вы можете настроить регистрацию событий программы ([Таблица 5](#)).

**Таблица 5. Параметры регистрации событий**

Параметр	Комментарий
Logging: Log level (0, 1)	<p>С помощью данной настройки вы можете включить или отключить ведение журнала регистрации событий программы Dr.Web для Kerio MailServer. Вы можете указать одно из двух значений:</p> <ul style="list-style-type: none"><li>• <b>1</b> чтобы включить ведение журнала регистрации событий;</li><li>• <b>0</b> чтобы отключить ведение журнала регистрации событий.</li></ul> <p>По умолчанию ведение журнала регистрации событий выключено.</p> <div style="background-color: #f0f0f0; padding: 5px;"> Для применения данной настройки необходимо повторно подключить Dr.Web для Kerio MailServer к почтовому серверу.</div>
Logging: Max file size (KB)	<p>Данная настройка позволяет задать максимальный размер (в килобайтах) файла журнала регистрации событий программы Dr.Web для Kerio MailServer.</p> <p>По умолчанию задано значение 50000 КБ.</p>



## 4.2. Настройка уведомлений

Данная группа параметров позволяет определить типы отправляемых уведомлений ([Таблица 6](#)) и задать параметры сервера, используемого для их рассылки ([Таблица 7](#)).

**Таблица 6. Параметры рассылки почтовых уведомлений**

Параметр	Комментарий
Notify: Check failed (0, 1)	Данный параметр позволяет включить/отключить отправку почтовых уведомлений о невозможности проверки какого-либо объекта (например, если он поврежден или защищен паролем).  По умолчанию отправка данного типа уведомлений отключена.
Notify: Bases out of date (0, 1)	Данный параметр позволяет включить/отключить отправку почтовых уведомлений об устаревании вирусных баз.  По умолчанию отправка данного типа уведомлений отключена.
Notify: Daily statistics (0, 1)	Данный параметр позволяет включить/отключить отправку почтовых уведомлений с информацией о статистике за предыдущие сутки.  По умолчанию отправка данного типа уведомлений отключена.
Notify: Key not found (0, 1)	Данный параметр позволяет включить/отключить отправку почтовых уведомлений о невозможности найти лицензионный ключ.  По умолчанию отправка данного типа уведомлений отключена.
Notify: License expires (0, 1)	Данный параметр позволяет включить/отключить отправку почтовых уведомлений о приближении срока окончания действия лицензионного ключа.  По умолчанию отправка данного типа уведомлений отключена.
Notify: Start error (0, 1)	Данный параметр позволяет включить/отключить отправку почтовых уведомлений об ошибке запуска приложения.  По умолчанию отправка данного типа уведомлений отключена.
Notify: Threat detected (0, 1)	Данный параметр позволяет включить/отключить отправку почтовых уведомлений об обнаружении угроз при проверке почтовых вложений.  По умолчанию отправка данного типа уведомлений отключена.

**Таблица 7. Параметры сервера уведомлений**

Параметр	Комментарий
SMTP Notify: From	Данный параметр определяет электронный адрес отправителя уведомлений.
SMTP Notify: Password	Данный параметр определяет пароль пользователя для доступа к серверу уведомлений.
SMTP Notify: Server	Данный параметр определяет IP-адрес и порт сервера уведомлений. Например: 192.168.0.1:25.
SMTP Notify: To	Данный параметр определяет электронные адреса получателей уведомлений. Вы можете указать один электронный адрес или несколько через запятую или точку с запятой.
SMTP Notify: Username	Данный параметр определяет имя пользователя для доступа к серверу уведомлений.



## 5. 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 почтового сервера Kerio, 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.

### 5.1. 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 вирусных базах данных, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения и лечения зараженных файлов. Вирусная 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 grcode). 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 вирусных баз](#) позволяет обнаруживать даже самые новые вирусы.



## 5.2. Карантин

Инфицированные вложения могут быть перемещены в Карантин, который служит для изоляции и безопасного хранения вредоносных объектов.

По умолчанию, опция перемещения инфицированных объектов в карантин включена. Для ее отключения, установите значение **0** для [параметра антивируса](#) **Quarantine: Enabled**. В случае выключения карантина инфицированные вложения будут удаляться.

### Управление карантинном

Просмотр файлов, находящихся в карантине, и работа с ними осуществляются с помощью специальной утилиты **Dr.Web Quarantine**. Для запуска утилиты зайдите в меню **Пуск** -> **Программы** -> **Dr.Web for Kerio Mail Servers** и выберите **Dr.Web Quarantine**. Откроется список объектов, помещенных в карантин (см. [Рисунок 1](#)).

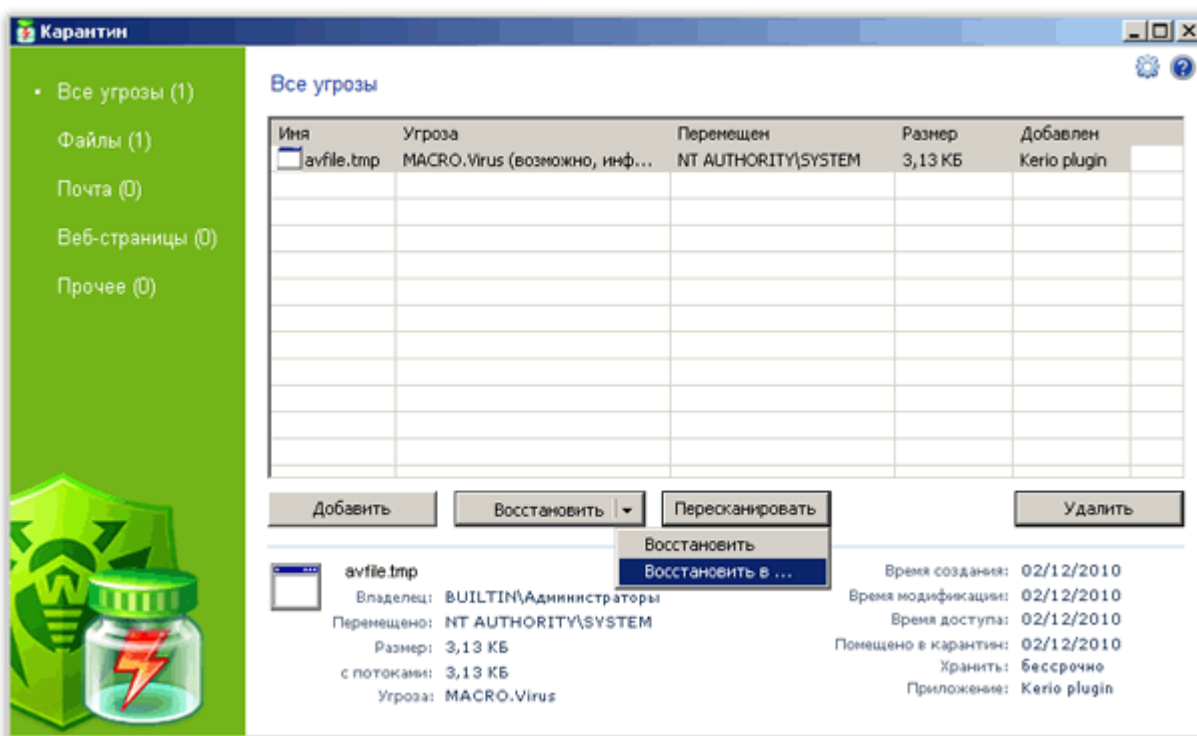


Рисунок 1. Карантин

Для каждого объекта в списке содержится информация об имени и размере зараженного файла, имени вируса, а также путь к папке хранения объекта. Вы можете настроить отображение информации об объектах. Для этого щелкните правой кнопкой мыши по столбцу в таблице и нажмите **Выбрать колонки**. Далее выберите типы отображаемой информации в открывшемся окне.

Вы можете удалить или восстановить объекты, помещенные в карантин. Для этого:

- выберите один или несколько объектов в списке;






- для удаления объекта(ов) нажмите кнопку **Удалить**;
- для восстановления объекта(ов) нажмите кнопку **Восстановить** и выберите пункт **Восстановить в**, после чего выберите папку для восстановления объекта(ов).

Кроме того, с помощью кнопки **Пересканировать** вы можете повторно проверить находящиеся в карантине объекты, в частности, подозрительные файлы, после [обновления вирусных баз Dr.Web](#).

Вы также можете перенести в карантин файлы с локального диска и сменных носителей с помощью кнопки **Добавить**, после чего осуществить антивирусную проверку этих файлов. Обратите внимание, что в данном случае вернуть файл в исходную папку можно только с помощью кнопки **Восстановить**.



## Свойства карантина

Для доступа к свойствам карантина нажмите кнопку **Свойства**  в верхней части окна **Карантин**. В открывшемся окне **Свойства карантина** (см. [Рисунок 2](#)) вы можете изменить следующие настройки:

1. Ограничение размера карантина. Вы можете определить необходимый размер дискового пространства, отводимого для карантина в разделе **Задать размер карантина**. По умолчанию установлен неограниченный размер карантина.
2. Перед лечением инфицированного файла в карантине обязательно сохраняется его резервная копия. Это позволяет восстановить файл, например, в случае его повреждения при лечении. Для включения отображения резервных копий в карантине в разделе **Вид** установите флажок **показывать резервные копии**.

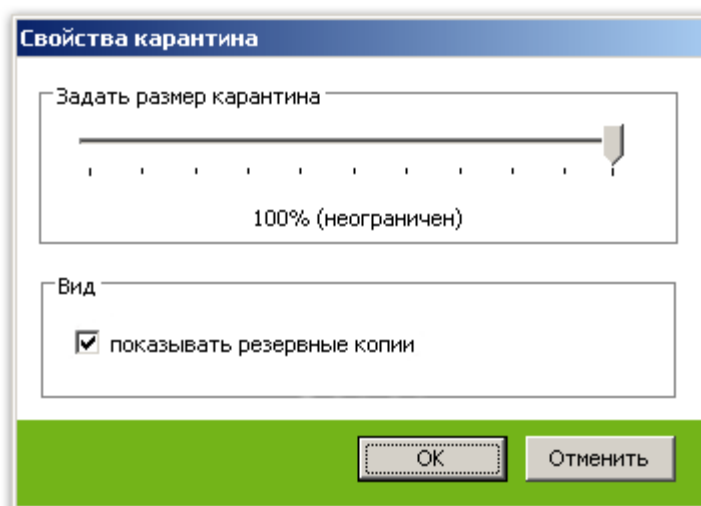


Рисунок 2. Свойства карантина

Объекты карантина сохраняются в том же разделе жесткого диска, на котором установлен почтовый сервер Kerio. Если места в разделе будет недостаточно для сохранения файла или будет превышен заданный максимальный размер карантина, файл не будет перемещен в карантин.



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.



## 6. 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 3](#)).

**Dr.WEB**  
Антивирус для Kerio

Статистика угроз

Последняя обнаруженная угроза:  
Wed Feb 16 12:25:57 2011 EICAR Test File (NOT a Virus!)  
файл удален.

Тип угрозы	За сегодня	За неделю	За все время
Всего проверено	0	0	21
Инфицированные объекты	0	0	7
Потенциально опасные программы	0	0	0
Рекламные программы	0	0	0
Программы дозвона	0	0	0
Программы-шутки	0	0	3
Программы взлома	0	0	0
Ошибок проверки	0	0	0

О программе

- Антивирус Dr.Web включен  
6.00.0.201102140
- Последнее обновление  
Wed Feb 16 10:18:10 2011
- Номер лицензии

Владелец лицензии  
Ersh

Количество станций  
1

Дата окончания действия  
Sun Jun 05 16:00:03 2011  
(осталось 109 дн.)

Техническая поддержка | Новости | Политика конфиденциальности | Dr.Web Live | Doctor Web

Рисунок 3. Веб-консоль

### Доступ к веб-консоли

Для доступа к веб-консоли укажите в адресной строке браузера IP-адрес и порт почтового сервера Kerio (например, <http://127.0.0.1:8089>). Порт задается параметром антивируса Web Console: Port и может принимать значения в диапазоне от 1024 до 65536. По умолчанию указано значение 8089.

### 6.1. Информация о программе

В разделе веб-консоли **О программе** (см. [Рисунок 3](#)) отображается следующая информация об активности приложения, пользовательской лицензии и обновлениях вирусных баз:

- версия антивирусного ядра программы;



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

## 6.2. Статистика работы программы

Статистика работы программы отображается в виде таблицы (см. [Рисунок 3](#)) 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 потенциально опасных программ, рекламных программ, программ дозвона, программ-шуток, программ взлома;
  - количество ошибок, возникших при проверке почтовых вложений.

### Удаление статистики

Статистика сохраняется в файле `drw-kerio-stat.dat`, расположенном в каталоге установки программы. В случае если программа прекращает функционировать, статистика за последние сутки и за последнюю неделю сбрасывается. Для удаления статистики за весь период работы программы необходимо удалить файл `drw-kerio-stat.dat`.



## 7. Обновление вирусных баз



Модуль обновления (drwebupw.exe) может быть запущен сразу после установки Dr.Web для Kerio MailServer путем выбора соответствующего флажка на последнем шаге [установки](#). Модуль загружает последние версии антивирусного ядра (drweb32.dll), а также вирусных баз (\*.vdb) и автоматически их обновляет.

Для обнаружения вредоносных объектов Dr.Web для Kerio MailServer использует специальные вирусные базы, в которых содержится информация обо всех известных вредоносных программах. Так как каждый день появляются новые вредоносные программы, то эти базы требуют периодического обновления. Для этого в приложении реализована система обновления вирусных баз через Интернет. В течение срока действия лицензии модуль обновления регулярно скачивает и устанавливает информацию о новых вирусах и вредоносных программах, а так же обновления самого приложения.



При подключении к сети Интернет через прокси-сервер, необходимо настроить модуль обновления программы для [подключения к прокси-серверу](#).

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

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

### Редактирование расписания обновлений

1. Откройте **Планировщик заданий**.
2. В контекстном меню задания **Dr.Web Update for Kerio MailServer Plugin**  выберите пункт **Свойства**.
3. В диалоговом окне **Dr.Web Update for Kerio MailServer Plugin** выберите вкладку **Расписание**, нажмите кнопку **Дополнительно**, и в открывшемся окне измените период обновления. По умолчанию, обновление вирусных баз программы выполняется ежедневно каждые 30 минут.
4. Нажмите кнопку **ОК**.



## 8. Регистрация событий

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

- журнале регистрации событий операционной системы (Event log);
- в протоколах debug, error и security сервера Kerio;
- текстовом файле журнала отладки Dr.Web (если выбрано значение **1** [параметра антивируса Logging: Log level](#)).

Текстовый журнал отладки Dr.Web расположен по умолчанию в файле DrWebForKMS.log в каталоге %ProgramFiles%\DrWeb for Kerio MailServer\.

Информация об обновлениях также заносится в отдельный текстовый журнал drwebupw.log, расположенный в каталоге %AllUsersProfile%\Application Data\Doctor Web\Logs\.

### 8.1. Журнал операционной системы

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

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

#### Просмотр журнала регистрации операционной системы

1. Чтобы просмотреть журнал регистрации событий операционной системы, откройте **Панель управления** операционной системы.
2. Выберите **Администрирование**, а затем выберите **Просмотр Событий**.
3. В левой части окна **Просмотр Событий** выберите **Приложение**. Откроется список событий, зарегистрированных в журнале пользовательскими приложениями.



Источником сообщений Dr.Web для Kerio MailServer является приложение **Dr.Web for Kerio MailServer**.

## 8.2. Текстовый журнал

В текстовый журнал регистрации программы может заноситься следующая информация:

- сообщения о действительности или недействительности лицензии;
- сообщения об обнаружении вирусов;
- сообщения об ошибках записи или чтения файлов, ошибках анализа архивов или файлов, защищенных паролем;
- параметры модулей программы: сканера, ядра, вирусных баз;
- сообщения об экстренных остановках ядра программы;
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 дней до окончания срока).



Ведение текстового журнала регистрации событий приводит к снижению быстродействия сервера, поэтому рекомендуется включать регистрацию событий только в случае возникновения ошибок работы приложения Dr.Web для Kerio MailServer.

При достижении максимального размера, определяемого [параметром Logging: Max file size](#) (по умолчанию 50000 КБ), файл журнала очищается, и журнал начинается заново.

## 8.3. 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 почтового сервера Kerio.
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 работы модуля обновления](#)

### 9.1. Проверка установки

Чтобы проверить корректность установки:

1. Удостоверьтесь, что следующие папки созданы и содержат все необходимые файлы:
  - %ProgramFiles%\DrWeb for Kerio MailServer\

Имя файла	Описание
drwebupw.exe	Исполняемый файл модуля обновления
update.drl	Список URL-адресов для обновления
drweb32.key	Лицензионный ключевой файл
dwqrui.exe	Клиент доступа к карантину Dr.Web
locale.ini	Файл локализации
drwmsg.dll	Служебная библиотека
WebConsole.exe	Исполняемый файл веб-консоли

- %ProgramFiles%\DrWeb for Kerio MailServer\html\, содержащий файлы, используемые веб-консолью;





▫ %CommonProgramFiles%\Doctor Web\Scanning Engine\

Имя файла	Описание
drweb32.dll	Антивирусное ядро
dwinctl.dll	-
dwengine.exe	Сервис Dr.Web Scanning Engine

▫ %AllUsersProfile%\Application Data\Doctor Web\Bases\

Имя файла	Описание
*.vdb	Вирусные базы
drweb32.lst	Список файлов, загружаемых Модулем обновления

2. Откройте Панель управления операционной системы, выберите **Администрирование**, а затем **Службы**. Проверьте, что запущена служба Dr.Web Scanning Engine (DrWebEngine).
3. Откройте журнал регистрации событий операционной системы (Event Log) и убедитесь, что в нем нет ошибок, связанных с приложением Dr.Web для Kerio MailServer.

## 9.2. 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](http://en.wikipedia.org/wiki/EICAR_test_file).
2. Проверьте полученное письмо. Инфицированный вложенный файл должен быть удален из письма.

### Проверка модуля обновления

1. Чтобы проверить работоспособность модуля обновления, откройте **Панель управления** операционной системы, выберите **Назначенные Задания** и проверьте, что задание **Dr.Web Update for Kerio MailServer Plugin**  создано.
2. Проверьте корректность обновления. Приложение и вирусные базы обновляются сразу же после установки. При корректном обновлении, переменная ERRORLEVEL окружения операционной системы устанавливается в 0. Другие значения свидетельствуют об ошибке.



3. Откройте журнал обновлений приложения Dr.Web для Kerio MailServer drwebupw.log, расположенный в каталоге %AllUsersProfile%\Application Data\Doctor Web\Logs\, и убедитесь, что он не содержит ошибок.




## 10. Приложения

### 10.1. Приложение А. Параметры командной строки для модуля обновления

Модуль обновления допускает работу в режиме командной строки.

#### Параметры командной строки в Планировщике заданий

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

#### Допустимые параметры

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

Параметр	Комментарий
/DBG	Включает детальный режим ведения журнала регистрации (%AllUsersProfile%\Application Data\Doctor Web\Logs\drwebupw.log).
/URL: <url>	Указывает сервер обновлений. Допускаются только пути в формате UNC.
/USER: <имя>	Указывает имя пользователя для подключения к серверу обновлений.
/PASS: <пароль>	Указывает пароль для подключения к серверу обновлений.
/UPM: <режим>	Включает режим использования прокси-сервера при подключении к сети Интернет. Параметр <режим> может принимать следующие значения: <ul style="list-style-type: none"><li>• <b>direct</b> – не использовать прокси-сервер;</li><li>• <b>ieproxy</b> – использовать системные настройки прокси-сервера;</li><li>• <b>userproxy</b> – использовать <a href="#">настройки</a>, заданные пользователем.</li></ul>
/PURL: <адрес>	Указывает адрес прокси-сервера.
/PUSER: <имя>	Указывает имя пользователя для подключения к прокси-серверу.
/PPASS: <пароль> >	Указывает пароль для подключения к прокси-серверу.



Параметр	Комментарий
/UA	<p>Включает режим полного обновления, при котором загружаются обновления для всех файлов, указанных в списке обновления, независимо от используемой операционной системы и установленных компонентов продукта. Режим предназначен для получения полной локальной копии серверной области обновления Dr.Web.</p> <p>Этот режим нельзя использовать для обновления антивируса, установленного на компьютере.</p>
/ST	Включает режим невидимого обновления, при котором модуль обновления запускается в невидимом окне (stealth mode).
/LNG: <файл>	Указывает имя файла языковых ресурсов. По умолчанию используется английский язык.
/GO	Включает пакетный режим работы, при котором не выводятся диалоговые окна.
/QU	<p>Включает режим принудительного закрытия модуля обновления по завершении обновления вне зависимости от результата. Код результата записывается в переменную ERRORLEVEL окружения операционной системы:</p> <ul style="list-style-type: none"><li>• нулевое значение указывает на успех,</li><li>• ненулевое значение указывает на неудачу.</li></ul>
/DIR: <каталог> >	Указывает каталога для установки файлов обновления. По умолчанию используется каталог, из которого запущен модуль обновления.
/URM: <режим>	<p>Включает режим перезагрузки компьютера после обновления. Параметр &lt;режим&gt; может принимать следующие значения:</p> <ul style="list-style-type: none"><li>• <b>prompt</b> – перезагрузка по окончании обновления после разрешения пользователя;</li><li>• <b>noprompt</b> – принудительная перезагрузка по окончании обновления при необходимости;</li><li>• <b>force</b> – принудительная перезагрузка всегда вне зависимости от необходимости;</li><li>• <b>disable</b> – запрет перезагрузки.</li></ul>
/REG	Включает режим регистрации продукта и получения регистрационного ключа.
/UPD	Включает режим обычного обновления. Используйте этот режим вместе с режимом /REG для загрузки обновлений сразу же после регистрации продукта.
/UVB	<p>Включает режим обновления только вирусных баз и ядра drweb32.dll.</p> <p>Этот параметр отменяет действие ключа /UA.</p>



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



## 10.2. Приложение Б. Действия в случае возникновения проблем

В случае возникновения проблем при использовании программы Dr.Web для Kerio MailServer или при ее установке, обратитесь в [службу технической поддержки Dr.Web](#).

Для того чтобы специалисты компании «Доктор Веб» смогли помочь вам максимально быстро, постарайтесь сообщить как можно больше информации о проблеме. Ниже приведены общие рекомендации. Полученную информацию следует отправить вместе с вашим запросом в службу технической поддержки.

### Рекомендации

1. Сохраните файл-отчет со сведениями о системе в формате .nfo. Для этого выполните следующие действия:
  - выполните команду **msinfo32** в меню **Пуск -> Выполнить**;
  - в меню **Файл** выберите **Сохранить**;
  - укажите имя файла и нажмите кнопку **ОК**.
2. Укажите полную версию сервера Kerio (например, 6.7 build 6399). Для просмотра версии используемого почтового сервера выполните следующие действия:
  - откройте Панель управления и выберите пункт **Установка и удаление программ**;
  - в окне **Установка и удаление программ** выберите программу Kerio MailServer/Kerio Connect;
  - нажмите **Чтобы получить сведения о поддержке, щелкните здесь**. Откроется окно с информацией о продукте, в котором указана полная версия программы.
3. Сохраните журналы операционной системы **Приложение** и **Система** в формате .evt. Для этого выполните следующие действия:
  - в меню **Пуск -> Выполнить** выполните команду `eventvwr`;
  - щелкните правой кнопкой мыши на журнале **Приложение/Система** и выберите в контекстном меню **Сохранить файл журнала как**;
  - введите имя файла, выберите тип файла **Журнал событий (.evt)** и нажмите **Сохранить**.
4. Если проблема стабильно повторяется, включите [журнал отладки Dr.Web](#) и воспроизведите проблему. После этого, журнал отладки можно отключить. Текстовый журнал отладки программы будет создан по умолчанию в каталоге %ProgramFiles%\DrWeb for Kerio MailServer\DrWebForKMS.log.
5. Приложите журнал модуля обновления Dr.Web. Для этого:
  - скопируйте файл `drwebupw.log` из каталога %AllUsersProfile%\Application Data\Doctor Web\Logs\.
6. Если установка/работа приложения Dr.Web для Kerio MailServer происходит на виртуальной машине, укажите полную версию системы виртуализации, а также



прикрепите файл-отчет со сведениями о системе (.nfo), используемой в качестве хоста виртуальной машины.

Если проблемы возникли на этапе установки или удаления приложения:

1. Укажите версию установочного файла Dr.Web для Kerio MailServer, с которым возникли проблемы (например, 6.00.0.07120). Для просмотра версии установочного файла выполните следующие действия:
  - найдите в проводнике установочный файл Dr.Web для Kerio MailServer, например drweb-KerioMailServer-602-windows-nt-x86.exe;
  - щелкните правой кнопкой мыши по названию установочного файла и выберите в контекстном меню **Свойства**;
  - в окне **Свойства** откройте вкладку **Версия** и выберите пункт **Версия продукта**.
2. Проверьте корректность электронно-цифровой подписи установочного файла Dr.Web для Kerio MailServer. Для этого выполните следующие действия:
  - найдите в проводнике установочный файл программы (например, drweb-KerioMailServer-602-windows-nt-x86.exe);
  - щелкните правой кнопкой мыши по названию установочного файла и выберите в контекстном меню **Свойства**;
  - в окне **Свойства** откройте вкладку **Цифровые подписи**, выберите в списке электронно-цифровую подпись и нажмите **Сведения**;
  - в открывшемся окне **Состав цифровой подписи** должна выводиться строка «Эта цифровая подпись действительна». Если данная строка отсутствует, попробуйте повторно загрузить установочный файл с сайта компании «Доктор Веб» и повторить шаги по проверке электронно-цифровой подписи.
3. Приложите файл drweb-kerio-setup.log, расположенный во временном каталоге. Для этого:
  - откройте каталог временных файлов %Temp% через меню **Пуск** -> **Выполнить** и в открывшемся окне скопируйте файл drweb-kerio-setup.log.
4. Приложите следующую информацию из используемого лицензионного файла:
  - значения параметров Applications, Created и Expired, например:

```
Applications=Update, Scheduler, KerioPlugin
Created=2010-01-05 (12:00) UTC
Expires=2010-07-05 (12:00) UTC
```
  - параметры секции [Settings], например:

```
MailServer=Yes
FileServer=No
InetGateway=No
SpamFilter=No
LotusSpamFilter=No
EmailAddresses=Unlimited
TrafficLimit=Unlimited
```



## 10.3. Приложение В. 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 4](#)).

Компьютеры компании или пользователей поставщика ИТ-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 4. 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 6.0 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 почтового сервера Kerio с установленным приложением Dr.Web для Kerio MailServer. События запуска будут отображаться в таблице **Запуск/Завершение** Центра Управления Dr.Web. Время остановки почтового сервера Kerio с установленным приложением не регистрируется;
- 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 вирусных 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. При запуске почтового сервера Kerio с установленным приложением Dr.Web для Kerio MailServer будет предпринята попытка использовать лицензионный ключ для данной станции в антивирусной сети. Если ключ не действителен, то будет использован локальный ключ, расположенный в каталоге установки программы.



## Предметный указатель

### D

- Dr.Web для Kerio MailServer
  - веб-консоль 27, 28
  - карантин 24
  - обновление 29
  - основные функции 6
  - параметры 17, 20
  - проверка работы 32, 33
  - статистика 28
  - удаление 15
  - установка 14

### E

- event log 30

### K

- Kerio Connect 12
- Kerio MailServer 12

### A

- антивирусная проверка 22
- антивирусные базы 22
  - обновление 29

### B

- веб-консоль 27, 28
  - доступ 27
  - лицензия 27
  - обновление 27
  - статистика 28
- вирусная проверка 22

### D

- диагностика 32, 33

### I

- интернет-подключение 16

### K

- карантин 24
- ключ 8
- ключевой файл 9
  - действительность 8
  - использование 10
  - параметры 10

- получение 8, 9
- формат 10

### L

- лицензионный ключевой файл 8, 9
- лицензирование 8
- лицензия 27
  - использование 10
  - обновление 9
  - параметры 10
  - получение 8

### M

- методы обнаружения вирусов 22
- модуль обновления
  - настройка 29
  - проверка 32, 33

### H

- настройка 16
- карантина 24
- параметров сервера 20
- подключения 16
- прокси 16
- уведомлений 20

### O

- обновление
  - антивирусных баз 27, 29
  - лицензии 9
  - настройка 29
  - параметры 35
  - проверка 32, 33
- обновление лицензии 9
- объекты проверки 22
- операционная система 12
- отладочный журнал 31

### P

- параметры
  - антивируса 17, 20
  - командной строки 35
  - проверки 17
  - регистрации событий 17
  - сервера 20
  - уведомлений 20



## Предметный указатель

параметры лицензирования 10  
подключение  
    Dr.Web для Kerio MailServer 17  
подключение к Интернет 16  
получение ключевого файла 8  
почтовый сервер 12  
приложение 35, 38, 40  
проверка  
    методы 22  
    на вирусы 22  
    обновления 32, 33  
    установки 32  
    функционирования 32, 33  
прокси 16

### Р

регистрация событий 30  
    настройка 17  
режим работы 40

### С

сервер уведомлений 20  
системные требования 12  
события 30  
    журнал операционной системы 30  
    журнал отладки 31  
    журналы регистрации 30  
    регистрация 30  
    текстовый журнал 31  
совместимость 14  
статистика 28

### Т

текстовый журнал 31  
техническая поддержка 7, 38  
требования 12

### У

уведомления 20  
удаление Dr.Web для Kerio MailServer 12, 15  
условные обозначения 7  
установка Dr.Web для Kerio MailServer 12, 14  
    проверка 32

### Ф

файл ключа 8

формат ключевого файла 10

### Ц

централизованная защита 40

