



Dr.WEB

для межсетевого экрана Kerio Control

Руководство администратора

Жасағаныңды

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

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

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

© «Доктор Веб», 2017. 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).

Антивирус Dr.Web для Kerio Control

Версия 9.0.0

Руководство администратора

24.05.2017

«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

Введение	5
Используемые обозначения	6
Основные функции	6
Лицензирование	7
Лицензионный ключевой файл	7
Получение ключевого файла	7
Обновление лицензии	8
Использование ключевого файла	8
Определение параметров лицензирования	9
Установка и удаление Dr.Web для межсетевого экрана Kerio Control	10
Системные требования	10
Компоненты Dr.Web для межсетевого экрана Kerio Control	11
Установка Dr.Web для межсетевого экрана Kerio Control	11
Удаление Dr.Web для межсетевого экрана Kerio Control	12
Подключение к межсетевому экрану	14
Настройка параметров антивируса	14
Выбор протоколов	15
Проверка на вирусы	16
Параметры проверки	17
Методы обнаружения вирусов	18
Карантин	20
Обновление вирусных баз	22
Регистрация событий	23
Журнал отладки	23
Диагностика	24
Проверка установки	24
Проверка работоспособности	24
Приложения	26
Техническая поддержка	26



Введение

Благодарим вас за приобретение Dr.Web для Kerio Control. Данный продукт представляет собой приложение, которое подключается к межсетевому экрану Kerio Control и осуществляет антивирусную проверку файлов, передаваемых по протоколам HTTP, FTP, SMTP и POP3, обеспечивая тем самым надежную защиту сетевого трафика от всех видов вредоносного программного обеспечения.

В Dr.Web для Kerio Control применены наиболее передовые разработки и технологии компании «Доктор Веб», которые позволяют обнаруживать различные типы вредоносных объектов, представляющих угрозу функционирования сети и информационной безопасности пользователей.

Dr.Web для Kerio Control проверяет сетевой 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 Kerio Control.

Настоящее руководство призвано помочь администраторам корпоративных сетей, использующих межсетевой экран Kerio Control, установить и настроить Dr.Web для Kerio Control, а также ознакомиться с его основными функциями.

Дополнительную информацию о настройках межсетевоего экрана Kerio Control и проверке сетевого трафика можно найти на официальном сайте компании Kerio по адресу <http://www.kerio.ru/>.



Используемые обозначения

В данном руководстве применены следующие условные обозначения ([Таблица 1](#)).

Таблица 1. 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.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
C:\Windows\	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Основные функции

Dr.Web для Kerio Control выполняет следующие функции:

- антивирусную проверку файлов, передаваемых по протоколам HTTP, FTP, SMTP и POP3, а именно:
 - вложенных файлов почтовых сообщений;
 - файлов веб-трафика, загружаемых по протоколам HTTP и FTP.
- обнаружение вредоносного программного обеспечения;
- изоляцию инфицированных файлов в Карантине;
- использование эвристического анализатора для дополнительной защиты от неизвестных вирусов;
- регулярное автоматическое обновление вирусных баз.



Dr.Web для Kerio Control не проверяет файлы, передаваемые по протоколу HTTPS.



Лицензирование

Права пользователя на использование Dr.Web для Kerio Control 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 подключаемого модуля;
- перечень компонентов, разрешенных к использованию;
- 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 Dr.Web для Kerio Control компоненты;
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится *недействительным*, при этом Dr.Web для Kerio Control перестает обнаруживать вредоносные программы и пропускает объекты проверки сетевого трафика без изменений.

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 межсетевой экран Kerio Control и уже установлен Dr.Web для Kerio Control или планируется его установка.

Для ознакомления с продуктом 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 Dr.Web для Kerio Control. 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 `/etc/opt/drweb.com/etc`.
2. Чтобы модуль переключился на использование нового ключевого файла, необходимо перезапустить [конфигурационного демона configd](#).

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 Control необходим ключевой файл, путь к которому указывается при установке.

В процессе работы Dr.Web для Kerio Control осуществляется поиск первого действительного ключевого файла в каталоге `/etc/opt/drweb.com/etc`, в который он был скопирован при установке. Если не будет найден ни один рабочий ключевой файл, Dr.Web для Kerio Control перестанет функционировать.



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

Определение параметров лицензирования

Лицензионный ключевой файл регулирует использование Dr.Web для Kerio Control.

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, которые разрешено использовать владельцу лицензии.  Для использования ключа с Dr.Web для Kerio Control в списке компонентов обязательно должен присутствовать компонент KerioPlugin.
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 Dr.Web для Kerio Control.

3. Закройте файл, не сохраняя изменений.



Установка и удаление Dr.Web для межсетевого экрана Kerio Control

Dr.Web для Kerio Control устанавливается на тот же компьютер, где установлен межсетевой экран Kerio Control, и используется им в качестве внешнего антивирусного программного обеспечения, подключаемого через «plug-in» интерфейс.

Dr.Web для Kerio Control поставляется в виде самораспаковывающегося архива `drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run` (вместо `[patch]` указывается номер обновления, вместо `[build]` – номер сборки, например, `drweb-kerio-control_9.0.0.0-1312241911~linux_x86.run`) и может быть установлена через консоль управления.

Дополнительную информацию об использовании антивирусного программного обеспечения межсетевым экраном Kerio Control вы можете найти на официальном сайте компании Kerio по адресу <http://www.kerio.ru/>.

Системные требования

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

Таблица 3. Системные требования.

Компонент	Требование
Место на жестком диске	Не менее 290 МБ свободного дискового пространства.
Операционная система	<ul style="list-style-type: none">• Kerio Control VMware Virtual Appliance• Kerio Control Software Appliance• Kerio Control Hyper-V Virtual Appliance
Межсетевой экран	Kerio Control версий 8.x, 9.0 или 9.1

Настоящие системные требования относятся только к Dr.Web для Kerio Control. Требования к межсетевому экрану содержатся в документации Kerio Control. Dr.Web для Kerio Control может работать на тех же компьютерах, на которых установлен межсетевой экран Kerio Control.



Dr.Web для Kerio Control поддерживает установку и работу в средах Kerio Control VMware Virtual Appliance, Kerio Control Software Appliance и Kerio Control Hyper-V Virtual Appliance. Информацию о данных программных решениях можно найти на официальном сайте компании Kerio по адресу <http://www.kerio.ru/>.

Компоненты Dr.Web для межсетевого экрана Kerio Control

Dr.Web для Kerio Control состоит из нескольких дополняющих друг друга компонентов, которые взаимодействуют между собой:

- Конфигурационный демон (**configd**) управляет активностью всех компонентов Dr.Web для Kerio Control в зависимости от выбранных настроек, а также хранит информацию о лицензии и настройках, предоставляя ее тем или иным компонентам при необходимости;
- Сканирующее ядро (**drweb-se**) осуществляет антивирусную проверку;
- Модуль обновления (**drweb-update**) предназначен для автоматического обновления вирусных баз. Модуль загружает копии вирусных баз из сети Интернет.

Установка Dr.Web для межсетевого экрана Kerio Control

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



Для установки Dr.Web для Kerio Control необходимо иметь права администратора.

Перед установкой Dr.Web для Kerio Control также необходимо выполнить следующие действия:

1. Включите SSH-доступ на Kerio Control VMware Virtual Appliance. Для этого:
 - Запустите терминал, нажмите в терминале Alt+F2.
 - Выполните вход под пользователем root.
 - Выполните команду start-ssh.
2. Скопируйте на Kerio Control VMware Virtual Appliance архив `drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run` и лицензионный ключевой файл для Dr.Web для Kerio Control.

Установка Антивируса Dr.Web для Kerio Control

1. Разрешите исполнение архива `drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run` (вместо `[patch]` указывается номер обновления, вместо `[build]` – номер сборки, например, `drweb-kerio-control_9.0.0.0-1401221455~linux_x86.run`). Вы можете воспользоваться следующей командой: `# chmod +x drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run`



2. Запустите файл на исполнение следующей командой: `# ./drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run`

Вы также можете сразу задать путь к лицензионному ключевому файлу с помощью опции `-k`: `# drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run -- -k <путь>`

3. Во время распаковки будет создана директория `drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86`. Далее запустится скрипт установки.

4. Для продолжения установки Dr.Web для Kerio Control введите `Y` или `Yes` в строке ввода (значения регистронезависимы) и нажмите клавишу `ENTER`, в результате чего будет запущен процесс установки компонентов. Если вы не хотите продолжать установку, введите `N` или `No`.

5. Если вы не указали путь к лицензионному ключевому файлу при запуске `run`-файла, вам будет предложено его указать.

6. По окончании установки на экран будет выведено сообщение о том, что установка компонентов успешно завершена.

Удаление Dr.Web для межсетевого экрана Kerio Control



Для удаления Dr.Web для Kerio Control необходимо иметь права администратора.

Удаление Антивируса Dr.Web для Kerio Control

4. Отключите использование Dr.Web для Kerio Control межсетевым экраном Kerio Control. Для этого:

- запустите консоль администрирования межсетевого экрана Kerio;
- выберите подраздел **Конфигурация** -> **Антивирус**;
- снимите флажок **Использовать внешнее антивирусное ПО** для выбранного Dr.Web для Kerio Control;
- нажмите кнопку **Применить**. Использование Dr.Web для Kerio Control будет отключено.

5. Выполните команду `# /opt/dweb.com/bin/remove-kerio-control.sh`.

6. Для продолжения удаления Dr.Web для Kerio Control введите `Y` или `Yes` в строке ввода (значения регистронезависимы) и нажмите клавишу `ENTER`, в результате чего начнется процесс удаления компонентов. Если вы не хотите продолжать удаление, введите `N` или `No`.

7. По завершении удаления на экран будет выведено сообщение о том, что выбранные компоненты успешно удалены.



Лицензионный ключевой файл и файлы карантина не удаляются по умолчанию. Вы можете удалить их вручную.

Кроме того, установленные [параметры проверки](#) сохраняются и автоматически используются при переустановке программы.

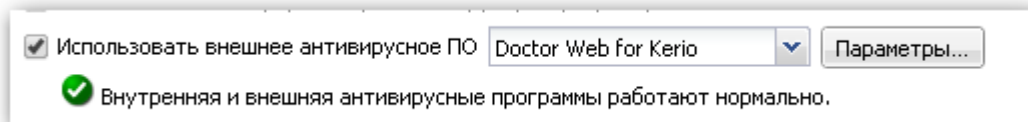


Подключение к межсетевому экрану

Dr.Web для Kerio Control подключается к межсетевому экрану Kerio Control в качестве внешнего антивирусного ПО и осуществляет проверку различных видов сетевого трафика в соответствии с настройками Kerio Control.

Подключение Dr.Web для Kerio Control

1. Запустите консоль администрирования межсетевому экрану Kerio.
2. Выберите подраздел **Конфигурация** -> **Антивирус**.
3. В группе настроек **Антивирусное ПО** вкладки **Антивирусная программа** установите флажок **Использовать внешнее антивирусное ПО** и выберите **Doctor Web for Kerio** в выпадающем списке.
4. Определите [параметры антивируса](#).
5. [Выберите протоколы](#) для сканирования.
6. Нажмите кнопку **Применить**. Если подключение прошло успешно, под настройкой выбора антивирусного ПО появится соответствующее сообщение (см. иллюстрацию ниже).



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



Для работы Dr.Web для Kerio Control требуется действительный ключевой файл. В случае его отсутствия или при возникновении проблем в работе конфигурационного демона configd антивирусная проверка сетевого трафика осуществляться не будет! Информация о проблеме будет занесена в журнал error межсетевому экрану Kerio Control.

Дополнительную информацию об использовании антивирусного программного обеспечения межсетевым экраном Kerio Control и возможных ошибках подключения вы можете найти в руководстве администратора Kerio Control и на официальном сайте компании Kerio по адресу <http://www.kerio.ru/>.

Настройка параметров антивируса

Параметры Dr.Web для Kerio Control определяют специфику его работы. Вы можете задать параметры модуля с помощью консоли администрирования межсетевому экрану



Kerio в разделе **Конфигурация** -> **Антивирус**:

1. Нажмите кнопку **Параметры** справа от названия антивируса в группе настроек **Антивирусное ПО** вкладки **Антивирусная программа**.
2. Откроется список параметров программы, с помощью которых вы можете настроить [проверку на вирусы](#) и [работу с карантином](#).
3. Нажмите кнопку **ОК** окна **Параметры антивирусной программы**, когда закончите изменять параметры антивируса.
4. Нажмите кнопку **Применить** на вкладке **Антивирусная программа** для сохранения сделанных изменений.

Выбор протоколов

Dr.Web для Kerio Control осуществляет проверку сетевого трафика по нескольким протоколам, которые могут быть выбраны на вкладке **Антивирусная программа** раздела **Конфигурация** -> **Антивирус** в консоли администрирования межсетевого экрана Kerio.

Чтобы выбрать протоколы для сканирования:

1. В группе настроек **Протоколы** укажите протоколы, которые будут подлежать проверке Dr.Web для Kerio Control. Вы можете выбрать следующие протоколы для сканирования: HTTP, FTP, SMTP и POP3.
2. При желании, вы также можете включить ограничение на размер сканируемого файла и указать максимальное значение размера файла (в килобайтах) в соответствующем текстовом поле. По умолчанию установлено значение 4096 КБ.

Подробнее о настройках сканирования, определяемых с помощью консоли администрирования межсетевого экрана Kerio, вы можете узнать из руководства администратора Kerio Control.



Проверка на вирусы

Dr.Web для Kerio Control обнаруживает следующие вредоносные объекты:

- инфицированные вложения в электронных письмах;
- инфицированные объекты, передаваемые по протоколам HTTP и FTP.

Dr.Web для Kerio Control проверяет сетевой трафик на наличие следующих типов вредоносных объектов и ПО:

- инфицированные архивы;
- файлы-бомбы или архивы-бомбы;
- рекламные программы;
- программы взлома;
- программы дозвона;
- программы-шутки;
- потенциально опасные программы.

Вы можете [выбрать протоколы](#), которые будут проверяться Dr.Web для Kerio Control, а также определить типы обнаруживаемых вредоносных объектов, задав соответствующие [параметры антивируса](#).

Dr.Web для Kerio Control использует различные [методы обнаружения вирусов](#), в случае обнаружения вредоносных объектов при проверке сетевого трафика к ним применяются действия в соответствии с настройками межсетевого экрана Kerio Control ([Таблица 4](#)). Эти настройки определяются с помощью вкладок раздела **Конфигурация** -> **Антивирус** в консоли администрирования межсетевого экрана Kerio.

Таблица 4. Настройки проверки сетевого трафика и действий над обнаруженными вредоносными объектами.

Вкладка	Комментарий
Сканирование HTTP, FTP	При обнаружении вируса, передаваемого по протоколам HTTP и FTP, его передача будет запрещена, и межсетевой экран выполнит действия, установленные администратором на данной вкладке настроек. Здесь же определяются действия в случае, если антивирусу не удалось проверить файл, и правила сканирования, определяющие типы файлов, проверяемых Dr.Web для Kerio Control.
Сканирование электронной почты	На данной вкладке вы можете задать настройки антивирусной проверки протоколов SMTP, POP3 и определить действия в случае обнаружения вирусов во вложениях электронных писем и в случае невозможности проверки файла (например, если файл поврежден или защищен паролем).



В случае обнаружения Dr.Web для Kerio Control угроз администратору может быть отправлено уведомление по электронной почте или в виде текстового сообщения SMS. Кроме того, информация обо всех обнаруженных угрозах фиксируется в журнале alert межсетевое экрана Kerio Control. Подробную информацию о настройках антивирусного сканирования различных типов сетевого трафика, а также об отправке уведомлений можно найти в руководстве администратора Kerio Control.



Антивирусная проверка файлов больших размеров (более 50 Мб) может занять продолжительное время. В результате, в некоторых случаях данные, проходящие через межсетевой экран Kerio Control, могут быть не доставлены получателям. Это необходимо учитывать при настройке времени ожидания получаемых данных для соответствующих программных продуктов и максимального размера проверяемых файлов для межсетевого экрана Kerio Control.



В целях повышения безопасности рекомендуется включить использование правила **Forbid resume due to antivirus scanning** в разделе **Политика FTP** консоли администрирования межсетевого экрана Kerio, в противном случае существует возможность попадания инфицированных объектов на компьютеры пользователей из-за повторной попытки их загрузки.



Параметры проверки

С помощью данных [параметров антивируса](#) вы можете задать действия программы для различных типов вредоносного ПО, а также включить использование эвристического анализатора и карантина ([Таблица 5](#)).

Таблица 5. Параметры проверки.

Параметр	Комментарий
Detect adware (Yes/No)	<p>Перечисленные параметры позволяют настроить проверку интернет-трафика 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">• 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. <div data-bbox="517 1756 598 1825"></div> При настройке данных параметров необходимо учитывать, что указанные значения зависят от регистра.
Detect dialers (Yes/No)	
Detect hacktools (Yes/No)	
Detect jokes (Yes/No)	
Detect riskware (Yes/No)	



Параметр	Комментарий
Enable heuristic (Yes/No)	<p>С помощью данного параметра вы можете включить или отключить эвристический анализатор, позволяющий обнаруживать неизвестные вирусы. По умолчанию эвристический анализатор включен. Вы можете указать одно из двух значений параметра:</p> <ul style="list-style-type: none">• No для отключения эвристического анализатора;• Yes для включения эвристического анализатора. <p> При настройке данного параметра необходимо учитывать, что указанные значения зависят от регистра.</p>
Quarantine directory	<p>Данная настройка задает путь к директории карантина. По умолчанию установлено значение <code>/var/lib/drweb/quarantine</code>.</p>
Quarantine enabled (Yes/No)	<p>Данный параметр позволяет включить/выключить перемещение инфицированных объектов в карантин. По умолчанию использование карантина отключено. Вы можете указать одно из двух значений параметра:</p> <ul style="list-style-type: none">• No для отключения опции перемещения инфицированных объектов в карантин;• Yes для включения опции изоляции в карантине. <p> При настройке данного параметра необходимо учитывать, что указанные значения зависят от регистра.</p>



При переустановке Dr.Web для Kerio Control заданные параметры проверки сохраняются.

Методы обнаружения вирусов

Все антивирусные продукты, разработанные компанией «Доктор Веб», применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.



Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он выполняется путем проверки содержимого анализируемого объекта на предмет наличия в нем сигнатур уже известных угроз. Сигатурой называется непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что позволяет значительно снизить размер записей в вирусных базах, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в вирусных базах Dr.Web составлены таким образом, что благодаря одной и той же записи можно обнаруживать целые классы или семейства угроз.

Origins Tracing™

Это уникальная технология Dr.Web, которая позволяет определить новые или модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы заражения или вредоносное поведение. Она выполняется по окончании сигнатурного анализа и обеспечивает защиту пользователей, использующих антивирусные решения Dr.Web, от таких угроз, как троянская программа-вымогатель Trojan.Encoder.18 (также известная под названием «gpcode»). Кроме того, использование технологии Origins Tracing™ позволяет значительно снизить количество ложных срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи Origins Tracing™, добавляется постфикс .Origin.

Эмуляция исполнения

Метод эмуляции исполнения программного кода используется для обнаружения полиморфных и зашифрованных вирусов, когда использование поиска по контрольным суммам сигнатур неприменимо или значительно усложнено из-за невозможности построения надежных сигнатур. Метод состоит в имитации исполнения анализируемого кода при помощи эмулятора – программной модели процессора и среды исполнения программ. Эмулятор оперирует с защищенной областью памяти (буфером эмуляции). При этом инструкции не передаются на центральный процессор для реального исполнения. Если код, обрабатываемый эмулятором, инфицирован, то результатом его эмуляции станет восстановление исходного вредоносного кода, доступного для сигнатурного анализа.



Эвристический анализ

Работа эвристического анализатора основывается на наборе эвристик (предположений, статистическая значимость которых подтверждена опытным путем) о характерных признаках вредоносного и, наоборот, безопасного исполняемого кода. Каждый признак кода имеет определенный вес (т. е. число, показывающее важность и достоверность этого признака). Вес может быть как положительным, если признак указывает на наличие вредоносного поведения кода, так и отрицательным, если признак не свойственен компьютерным угрозам. На основании суммарного веса, характеризующего содержимое объекта, эвристический анализатор вычисляет вероятность содержания в нем неизвестного вредоносного объекта. Если эта вероятность превышает некоторое пороговое значение, то выдается заключение о том, что анализируемый объект является вредоносным.

Эвристический анализатор также использует технологию FLY-CODE™ – универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта Dr.Web, но и новыми, ранее не исследованными программами. При проверке упакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, упакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».

Во время любой из проверок все компоненты антивирусных продуктов Dr.Web используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты Антивирусной Лаборатории «Доктор Веб» обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту Dr.Web, то она будет обнаружена в списке процессов и нейтрализована после получения [обновленных вирусных баз](#).

Карантин

Инфицированные объекты, обнаруженные при проверке сетевого трафика, могут быть перемещены в Карантин - специальную директорию `/var/lib/drweb/quarantine`, предназначенную для изоляции и безопасного хранения вредоносных объектов.



По умолчанию, опция перемещения инфицированных объектов в Карантин выключена, а все инфицированные объекты удаляются. Чтобы включить ее, установите значение **Yes** для [параметра антивируса Quarantine enabled](#).



В случае, если в карантин помещается файл, имя которого совпадает с именем уже находящегося в карантине файла, то к имени помещаемого файла будет добавлен буквенно-числовой индекс. Например, `file.com` будет переименован в `file.com.drwebq.1524482643`, где 1524482643 - это временная метка (timestamp) создания файла в карантине.

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.



Обновление вирусных баз

Для обнаружения вредоносных объектов Dr.Web для Kerio Control 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 происходит регулярная загрузка информации о новых вирусах и вредоносных программах, а так же обновлений самого приложения.

Для автоматизации получения и установки обновлений вирусных баз используется Модуль обновления. Данный модуль содержится в пакете **drweb-updater**, который входит в состав Dr.Web для Kerio Control. Модуль обновления запускается автоматически при старте операционной системы конфигурационным демоном **configd** и проверяет наличие обновлений, загружает и устанавливает их каждые 30 минут.



Регистрация событий

Dr.Web для Kerio Control регистрирует ошибки и происходящие события в протоколах debug, error и security межсетевого экрана Kerio Control.

Журнал отладки

В журнал debug межсетевого экрана Kerio Control заносится отладочная информация, которая используется при поиске и анализе ошибок в работе Dr.Web для Kerio Control.

Включение регистрации событий программы в журнал debug

1. Запустите консоль администрирования межсетевого экрана Kerio.
2. В разделе **Протоколы** выберите журнал debug.
3. В контекстном меню журнала debug выберите пункт **Сообщения**.
4. Выберите пункт **Antivirus plugin** в окне **Протоколирование сообщений**. Нажмите кнопку **ОК**.



Диагностика

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

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

Если в процессе установки или работы подключаемого модуля возникли ошибки, вы можете обратиться за помощью в [службу технической поддержки «Доктор Веб»](#).

Проверка установки

Чтобы проверить корректность установки, удостоверьтесь, что следующие папки созданы и содержат все необходимые файлы ([Таблица 6](#)):

Таблица 6. Установленные папки и файлы

Директория	Имя файла	Описание
/opt/dweb.com/bin	drweb-configd	Конфигурационный демон
	drweb-update	Модуль обновления
	drweb-se	Сканирующий модуль
/etc/opt/drweb.com	drweb32.key	Ключевой файл
/opt/kerio/winroute/ avirplugins	avir_drweb.so	Библиотека Dr.Web для Kerio Control

Проверка работоспособности

Для проверки работоспособности Dr.Web для Kerio Control необходимо убедиться в его способности обнаруживать вирусы.

Проверка работы Dr.Web для Kerio Control

1. Откройте в браузере страницу <http://www.eicar.org/download/eicar.com>, чтобы скачать тестовый инфицированный файл EICAR-Test-File. Информацию о тестовом вирусе EICAR можно найти по адресу http://en.wikipedia.org/wiki/EICAR_test_file. Указанная страница не должна открыться, а в журнале alert межсетевого экрана Kerio Control должна быть зафиксирована информация о попытке скачать инфицированный файл.



2. Отправьте письмо с тестовым инфицированным файлом EICAR-Test-File во вложении через сервер, защищаемый Kerio Control. Проверьте полученное письмо. Инфицированный файл должен быть удален из письма. Заголовок письма может содержать префикс, оповещающий о найденном вредоносном объекте.



Приложения

Техническая поддержка

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/>;
- 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>.

