



Защити созданное

Руководство администратора

© 2003-2013 «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 логотипы 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 WinRoute
Версия 6.00.2
Руководство администратора
10.06.2013**

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

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

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

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!



Содержание

Глава 1. Введение	6
Используемые обозначения	8
Техническая поддержка	9
Глава 2. Лицензирование	10
Лицензионный ключевой файл	10
Получение ключевого файла	11
Обновление лицензии	12
Использование ключевого файла	13
Определение параметров лицензирования	13
Глава 3. Установка и удаление программы	15
Системные требования	15
Совместимость	17
Установка программы	17
Удаление программы	19
Настройка подключения через прокси	21
Глава 4. Подключение к межсетевому экрану	22
Настройка параметров антивируса	23
Настройка параметров проверки	24
Настройка уведомлений	27
Выбор протоколов	29
Глава 5. Проверка на вирусы	30
Методы обнаружения вирусов	32



Карантин	33
Глава 6. Веб-консоль	37
Информация о программе	38
Статистика работы программы	38
Глава 7. Обновление вирусных баз	40
Глава 8. Регистрация событий	43
Журнал операционной системы	43
Текстовый журнал	44
Журнал отладки	45
Глава 9. Диагностика	46
Проверка установки	46
Проверка работоспособности	48
Приложения	49
Приложение А. Параметры командной строки для модуля обновления	49
Приложение Б. Действия в случае возникновения проблем	53
Приложение В. Работа в режиме централизованной защиты	56
Предметный указатель	60



Глава 1. Введение

Благодарим вас за приобретение программы **Dr.Web для Kerio WinRoute**. Данный антивирусный продукт представляет собой приложение, которое подключается к межсетевому экрану Kerio Winroute Firewall/Kerio Control и осуществляет антивирусную проверку файлов, передаваемых по протоколам HTTP, FTP, SMTP и POP3, обеспечивая тем самым надежную защиту сетевого трафика.

В программе 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 WinRoute 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 WinRoute Firewall/Kerio Control.



Основные функции программы

Dr.Web для Kerio WinRoute 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;
 - файлов, передаваемых посредством веб-сервиса Kerio Clientless SSL VPN;
- 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.



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

Настоящее руководство призвано помочь администраторам корпоративных сетей, использующих межсетевой экран Kerio WinRoute Firewall/Kerio Control, установить и настроить программу **Dr.Web для Kerio WinRoute**, а также ознакомиться с ее основными функциями.

Дополнительную информацию о настройках межсетевого экрана Kerio WinRoute Firewall/Kerio Control и проверке сетевого трафика можно найти на официальном сайте компании по адресу http://www.kerio.ru/kwf_home.html.



Используемые обозначения

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

Таблица 1. Условные обозначения.

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



Техническая поддержка

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

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

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

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

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



Глава 2. Лицензирование

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

Лицензионный ключевой файл

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

- период, в течение которого разрешено использование программы;
- перечень компонентов, разрешенных к использованию;
- 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 WinRoute** перестает обнаруживать вредоносные программы и пропускает объекты проверки сетевого трафика без изменений. Факт нарушения корректности ключевого файла записывается в журнал регистрации событий операционной системы, а также в текстовый журнал регистрации событий программы. Детальную информацию о регистрации событий вы можете найти в главе [Регистрация событий](#).



Получение ключевого файла

Вы можете получить лицензионный ключевой файл одним из следующих способов:

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

Получение ключевого файла по электронной почте

1. Зайдите на сайт, адрес которого указан в регистрационной карточке, прилагаемой к продукту.
2. Заполните форму со сведениями о покупателе.
3. Введите регистрационный серийный номер (находится на регистрационной карточке).
4. Ключевой файл будет выслан по указанному вами адресу электронной почты в виде ZIP-архива, содержащего файл с расширением .key.
5. Извлеките ключевой файл на компьютер, где установлен межсетевой экран Kerio WinRoute Firewall/Kerio Control и уже установлена программа **Dr.Web для Kerio WinRoute** или планируется ее установка.

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

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

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



Обновление лицензии

В некоторых случаях, например, при окончании срока действия лицензии или при изменении характеристик защищаемой системы или требований к ее безопасности, вы можете принять решение о приобретении новой или расширенной лицензии на программу **Dr.Web для Kerio WinRoute**. 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 WinRoute\).
2. Программа **Dr.Web для Kerio WinRoute** автоматически переключится на использование нового ключевого файла.

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



Использование ключевого файла

При установке программы **Dr.Web для Kerio WinRoute** ключевой файл копируется в каталог установки программы (обычно, %ProgramFiles%\DrWeb for Kerio WinRoute). Мастер установки автоматически регистрирует ключевой файл в реестре операционной системы.

В процессе работы **Dr.Web для Kerio WinRoute** 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.

Определение параметров лицензирования

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

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 WinRoute 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 программой.
Группа [Settings] , параметр MailServer	Указывает на разрешение (Yes) или запрет (No) использования ключа на почтовых серверах.

3. Закройте файл, не сохраняя изменений.



Глава 3. Установка и удаление программы

Программа **Dr.Web для Kerio WinRoute** устанавливается на тот же компьютер, где установлен межсетевой экран Kerio WinRoute Firewall/Kerio Control, и используется им в качестве внешнего антивирусного программного обеспечения, подключаемого через "plug-in" интерфейс.

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

Системные требования

Компьютер, на который устанавливается **Dr.Web для Kerio WinRoute**, 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">• Microsoft® Windows® 2000 (Professional Edition, Server, Advanced Server или Datacenter Server) с пакетом обновлений SP4 и Update Rollup 1;• Microsoft® Windows® XP (Home Edition или Professional Edition);• Microsoft® Windows Server® 2003 (Standard Edition, Enterprise Edition или Datacenter Edition);



	<ul style="list-style-type: none">• Microsoft® Windows Server® 2003 R2;• Microsoft® Windows Server® 2008 (Standard Edition, Enterprise Edition или Datacenter Edition);• Microsoft® Windows Server® 2008 R2;• Windows Vista® (Starter, Home Basic, Home Premium, Business, Enterprise или Ultimate);• Microsoft® Windows 7® (Starter, Home Basic, Home Premium, Business, Enterprise или Ultimate). <p>Поддерживаются 32- и 64-битные версии операционных систем.</p>
Межсетевой экран	<p>Если вы впервые устанавливаете Dr.Web для Kerio WinRoute, возможно использование следующих версий межетевого экрана:</p> <ul style="list-style-type: none">• Kerio WinRoute Firewall 6.2 или выше;• Kerio Control версий с 7.0.0 по 7.4.2.
Прочее ПО	<p>Dr.Web Enterprise Agent 6.0 или выше (для работы в режиме централизованной защиты)</p>

Перед установкой также необходимо ознакомиться с информацией о [совместимости Dr.Web для Kerio WinRoute](#).

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



Совместимость

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

- программа **Dr.Web для Kerio WinRoute** версии 6.00.2 совместима только с продуктами **Dr.Web** версии 6;
- если помимо **Dr.Web для Kerio WinRoute** в системе работают антивирусные приложения стороннего производителя, возможны конфликты;
- если помимо **Dr.Web для Kerio WinRoute** в системе функционирует антивирусный файловый сторож **Spider Guard**, то для того, чтобы проверка сетевого трафика осуществлялась программой **Dr.Web для Kerio WinRoute**, необходимо в настройках файлового сторожа исключить из проверки путь выгрузки файлов межсетевого экрана Kerio (обычно, %ProgramFiles%\Kerio\WinRoute Firewall\tmp\).
- перед установкой программы должны быть установлены все последние обновления, выпущенные для операционной системы.

Установка программы

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



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



Установка Dr.Web для Kerio WinRoute

1. Остановите сервис межсетевого экрана Kerio WinRoute Firewall/Kerio Control.
2. Скопируйте следующие файлы на компьютер, где установлен межсетевой экран Kerio WinRoute Firewall/Kerio Control:
 - установочный файл программы;
 - лицензионный ключевой файл.
2. В зависимости от используемой версии операционной системы запустите установочный файл программы:
 - **drweb-KerioWinRoute-600-windows-nt-x86.exe**, если используется 32-битная операционная система;
 - **drweb-KerioWinRoute-600-windows-nt-x64.exe** в случае использования 64-битной операционной системы.
3. Откроется окно с предложением выбрать язык установки. Вы можете выбрать русский или английский язык. Нажмите кнопку **ОК**.
4. Откроется окно Мастера установки. Нажмите кнопку **Далее**.
5. Откроется окно с текстом Лицензионного соглашения. Для продолжения установки его необходимо прочитать и принять. Нажмите кнопку **Далее**.
6. В открывшемся окне выберите вариант лицензирования. Вы можете использовать ключ, полученный от **Центра управления Dr.Web**, либо локальный ключ. Нажмите кнопку **Далее**.
7. Если на предыдущем шаге установки вы выбрали использование локального ключа, необходимо указать путь к нему. Для этого нажмите кнопку **Обзор** и выберите необходимый файл. Нажмите кнопку **Далее**.
8. На шаге **Путь к Kerio WinRoute** необходимо указать путь к папке установки межсетевого экрана Kerio WinRoute Firewall/Kerio Control (обычно, %ProgramFiles%\Kerio\WinRoute Firewall\). Нажмите кнопку **Далее**.



9. На шаге **Папка назначения** укажите путь к папке, в которую вы хотите установить программу. По умолчанию указана папка **%ProgramFiles%\DrWeb for Kerio WinRoute**. Если вы хотите выбрать другую папку, нажмите кнопку **Изменить** и укажите путь к этой папке. Нажмите **Далее**.
10. На шаге **Готова к установке программы** нажмите кнопку **Установить**, после чего начнется установка программы **Dr.Web для Kerio WinRoute** на ваш компьютер.
11. После окончания установки программы вы можете запустить обновление вирусных баз, установив в появившемся окне флажок **Запустить обновление**. Нажмите кнопку **Готово** для выхода из программы Мастера установки.

Приложение **Dr.Web для Kerio WinRoute** установлено и может быть [подключено к межсетевому экрану](#).

Удаление программы



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

Удаление Dr.Web для Kerio WinRoute

1. Отключите использование антивируса **Dr.Web для Kerio WinRoute** межсетевым экраном Kerio WinRoute Firewall/ Kerio Control. Для этого:
 - запустите консоль администрирования меж сетевого экрана Kerio;
 - выберите подраздел **Конфигурация** -> **Фильтрация содержимого** -> **Антивирус**;



- в группе настроек **Антивирусное ПО** вкладки **Антивирусный сканер** снимите флажок **Использовать внешний антивирус** для выбранного антивируса **Dr.Web for Kerio WinRoute**;
 - нажмите кнопку **Применить**. Использование **Dr.Web для Kerio WinRoute** будет отключено, о чем сигнализирует надпись «Отключен» под флажком **Использовать внешний антивирус**.
2. Для удаления **Dr.Web для Kerio WinRoute** 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 WinRoute** и нажмите кнопку **Удалить**. Откроется окно подтверждения удаления. Нажмите кнопку **Да**;
 - Запустите установочный файл программы, выберите язык интерфейса (английский или русский) и нажмите кнопку **ОК**. Откроется окно мастера InstallShield. Нажмите **Далее**. На шаге **Удаление программы** нажмите кнопку **Удалить** для того, чтобы удалить программу **Dr.Web для Kerio WinRoute** с вашего компьютера. По завершении удаления нажмите кнопку **Готово**;
 3. Компоненты программы и задание на обновление вирусных баз будут удалены.



Лицензионный 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 WinRoute).



Настройка подключения через прокси

Если компьютер, на котором установлена программа **Dr.Web для Kerio WinRoute**, 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 WinRoute** (обычно, `%ProgramFiles%\DrWeb for Kerio WinRoute`).
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**.

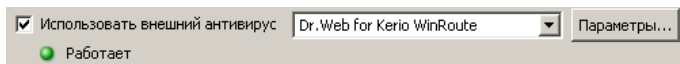


Глава 4. Подключение к межсетевому экрану

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

Подключение Dr.Web для Kerio WinRoute

1. Запустите консоль администрирования межсетевому экрану Kerio.
2. Выберите подраздел **Конфигурация** -> **Фильтрация содержимого** -> **Антивирус**.
3. В группе настроек **Антивирусное ПО** вкладки **Антивирусный сканер** установите флажок **Использовать внешний антивирус** и выберите **Dr.Web для Kerio WinRoute** в выпадающем списке.
4. Определите [параметры антивируса](#).
5. [Выберите протоколы](#) для сканирования.
6. Нажмите кнопку **Применить**. Если подключение прошло успешно, появится надпись «**Работает**» рядом с названием выбранного антивируса (см. иллюстрацию ниже).



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



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

Настройка параметров антивируса

Параметры антивируса **Dr.Web для Kerio WinRoute** определяют специфику его работы, а также регистрацию событий программы и работу системы уведомлений. Вы можете задать параметры программы с помощью консоли администрирования межсетевого экрана Kerio в разделе **Конфигурация -> Фильтрация содержимого -> Антивирус**:


1. Нажмите кнопку **Параметры** справа от названия антивируса в группе настроек **Антивирусное ПО** вкладки **Антивирусный сканер**.
2. Откроется список параметров программы, с помощью которых вы можете настроить [проверку на вирусы](#), [рассылку уведомлений](#) и работу с [веб-консолью](#). Для того чтобы задать значение того или иного параметра, выберите его в списке и нажмите кнопку **Правка**. Откроется окно **Изменить значение**, в котором вы можете редактировать значение выбранного параметра, после чего нажмите кнопку **ОК**.
3. Нажмите кнопку **ОК** окна **Настройки антивируса**, когда закончите изменять параметры антивируса.
4. Нажмите кнопку **Применить** на вкладке **Антивирусный сканер** для сохранения сделанных изменений.



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)	<p>Данный параметр позволяет настроить проверку архивов. Вы можете указать одно из двух значений параметра:</p> <ul style="list-style-type: none">• 0 для отключения проверки архивов;• 1 для включения проверки архивов. <p>По умолчанию проверка архивов включена.</p> <p> Для корректной проверки архивов данная настройка антивируса должна быть согласована с правилами сканирования архивов меж сетевого экрана Kerio.</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 сетевого 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">• 0 означает, что объекты, содержащие данный тип вредоносного ПО, будут пропущены;• 1 запрещает передачу подобных объектов. Данное значение установлено по умолчанию для всех типов вредоносных объектов.




Параметр	Комментарий
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">• 0 для отключения эвристического анализатора;• 1 для включения эвристического анализатора. <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 меж сетевого экрана 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 меж сетевого экрана Kerio для случая, когда проверка объекта невозможна.</p> <p>По умолчанию установлено значение 0 КБ (неограниченный размер файла архива).</p>



Параметр	Комментарий
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 настройками меж сетевого экрана Kerio для случая, когда проверка объекта невозможна.</p> <p>По умолчанию установлено значение 0 мс (неограниченное время проверки).</p>

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 WinRoute. Вы можете указать одно из двух значений:</p> <ul style="list-style-type: none">• 1 чтобы включить ведение журнала регистрации событий;• 0 чтобы отключить ведение журнала регистрации событий. <p>По умолчанию ведение журнала регистрации событий выключено.</p> <p> Для применения данной настройки необходимо выполнить повторное подключение Dr.Web для Kerio WinRoute к межсетевому экрану.</p>
Logging: Max file size (KB)	<p>Данная настройка позволяет задать максимальный размер (в килобайтах) файла журнала регистрации событий программы Dr.Web для Kerio WinRoute.</p> <p>По умолчанию задано значение 50000 КБ.</p>



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.



Параметр	Комментарий
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.



Выбор протоколов

Программа **Dr.Web для Kerio WinRoute** осуществляет сканирование сетевого трафика по нескольким протоколам, которые могут быть выбраны на вкладке **Антивирусный сканер** раздела **Конфигурация** -> **Фильтрация содержимого** -> **Антивирус** в консоли администрирования межсетевого экрана Kerio.

Чтобы выбрать протоколы для сканирования:

1. В группе настроек **Протоколы** укажите протоколы, которые будут подлежать антивирусной проверке программой **Dr.Web для Kerio WinRoute**. Вы можете выбрать следующие протоколы для сканирования: HTTP, FTP, SMTP и POP3. По умолчанию сканирование выбрано для всех указанных протоколов.
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 WinRoute Firewall/Kerio Control.



Глава 5. Проверка на вирусы

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

- инфицированные вложения в электронных письмах, а также инфицированные объекты, передаваемые по протоколам HTTP, FTP и посредством веб-сервиса Kerio Clientless SSL VPN, в том числе:
 - 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 программой **Dr.Web для Kerio WinRoute**, а также определить типы обнаруживаемых вредоносных объектов, задав соответствующие параметры антивируса.

Dr.Web для Kerio WinRoute 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 WinRoute Firewall/Kerio Control (Таблица 8). Эти настройки определяются с помощью вкладок раздела **Конфигурация** -> **Фильтрация содержимого** -> **Антивирус** в консоли администрирования межсетевого экрана Kerio.



Таблица 8. 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 на вирусы программой Dr.Web для Kerio WinRoute .
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).
Сканирование SSL-VPN	Данная вкладка настроек предназначена для задания параметров сканирования файлов, передаваемых посредством веб-сервиса Kerio Clientless SSL VPN. Вы можете выбрать проверку загружаемых и/или выгружаемых файлов, а также задать действия в случае невозможности антивирусной проверки файлов.

В случае обнаружения программой **Dr.Web для Kerio WinRoute** вируса администратору может быть отправлено уведомление по электронной почте или в виде текстового сообщения SMS. Кроме того, информация обо всех обнаруженных вирусах фиксируется в журнале alert меж сетевого экрана Kerio WinRoute Firewall/Kerio Control.

Подробнее о настройках антивирусного сканирования различных типов сетевого трафика, а также об отправке уведомлений можно узнать из руководства администратора Kerio WinRoute Firewall/Kerio Control.



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 **gpcode**). Кроме того, именно введение **Origins Tracing** позволяет значительно снизить количество ложных срабатываний эвристического анализатора.



3. Работа эвристического анализатора основывается на неких знаниях (*эвристиках*) о характерных признаках вирусного и, наоборот, безопасного кода. Каждый признак имеет определенный вес (число, показывающее серьезность и достоверность данного признака). На основании суммарного веса, характеризующего каждый конкретный файл, эвристический анализатор вычисляет вероятность заражения файла неизвестным вирусом. Как и любая система проверки гипотез в условиях неопределенности, эвристический анализатор может допускать ошибки как первого (пропуск неизвестных вирусов), так и второго рода (ложная тревога).

Во время любой из проверок компоненты антивирусов **Dr.Web** используют самую свежую информацию об известных вредоносных программах. Сигнатуры вирусов, информация об их признаках и моделях поведения обновляется сразу же, как только специалисты Антивирусной Лаборатории **«Доктор Веб»** обнаруживают новые угрозы, иногда – до нескольких раз в час. Таким образом, регулярное автоматическое [обновление вирусных баз](#) позволяет обнаруживать даже самые новые вирусы.

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 карантином

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 WinRoute** и выберите **Dr.Web Quarantine**. Откроется список объектов, помещенных в карантин (см. [Рисунок 1](#)).

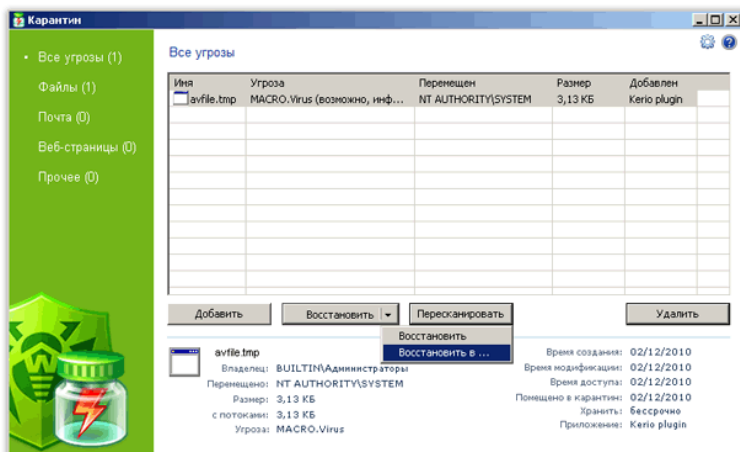


Рисунок 1. Карантин

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**.

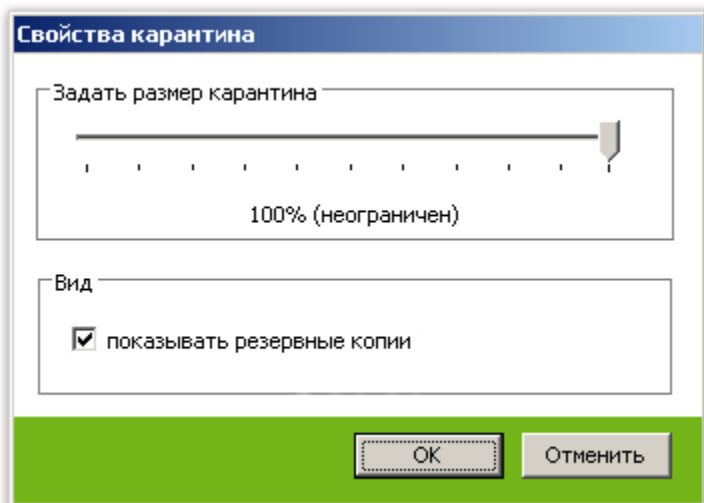


Рисунок 2. Свойства карантина

Объекты карантина сохраняются в том же разделе жесткого диска, на котором установлен межсетевой экран 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 WinRoute с 6.2 по 6.7.1 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.



Глава 6. Веб-консоль

Веб-консоль позволяет просматривать через браузер информацию о работе программы **Dr.Web для Kerio WinRoute**, 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
Идентифицированные объекты	0	0	7
Потенциально опасные программы	0	0	0
Рекламные программы	0	0	0
Программы донора	0	0	0
Программы шутки	0	0	3
Программы взлома	0	0	0
Ошибки 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
Egsh

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 межсетевого экрана Kerio (например, <http://127.0.0.1:8091>). Порт задается параметром антивируса **Web Console: Port** и может принимать значения в диапазоне от 1024 до 65536. По умолчанию указано значение 8091.

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.

Статистика работы программы

Статистика работы программы отображается в разделе веб-консоли **Статистика угроз** в виде таблицы (см. [Рисунок 3](#)). 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 и 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`.



Глава 7. Обновление вирусных баз



Модуль обновления (drwebupw.exe) может быть запущен сразу после установки **Dr.Web для Kerio WinRoute** 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 WinRoute** 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 WinRoute** 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 WinRoute Plugin**  выберите пункт **Свойства**.
3. В диалоговом окне **Dr.Web Update for Kerio WinRoute Plugin** выберите вкладку **Расписание** и измените период обновления. По умолчанию, обновление вирусных баз программы выполняется ежедневно каждые 30 минут.
4. Нажмите кнопку **ОК**.

Обновление без подключения к сети Интернет


1. Создайте центральный каталог для хранения обновлений вирусных баз и модулей программы **Dr.Web для Kerio WinRoute**.



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

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



2. По мере появления обновлений вирусных баз и модулей программы на официальном сайте компании по адресу <http://download.drweb.com/bases/> помещайте файлы обновлений в центральный каталог. Вы можете просмотреть список доступных к обновлению компонентов в файле drweb32.lst, расположенном в каталоге установки **Dr.Web для Kerio WinRoute** (обычно, %ProgramFiles%\DrWeb for Kerio WinRoute).
3. На локальном компьютере, где вы хотите настроить обновление через центральный каталог, откройте Планировщик заданий.
4. В контекстном меню задания **Dr.Web Update for Kerio WinRoute Plugin**  выберите пункт **Свойства**.
5. В диалоговом окне **Dr.Web Update for Kerio WinRoute Plugin** выберите вкладку **Задание** и добавьте следующий ключ к команде в поле **Выполнить**:
/URL:<сервер обновления>, где *<сервер обновления>* – путь к каталогу, в котором хранятся файлы обновления.
6. Нажмите кнопку **ОК**.



Глава 8. Регистрация событий

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

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

Текстовый журнал отладки Dr.Web по умолчанию находится в файле DrWebForKWF.log в каталоге %ProgramFiles%\DrWeb for Kerio WinRoute\.

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

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);



- сообщение о недействительности лицензии: отсутствие ключевого файла, отсутствие в ключевом файле разрешения на использование модулей программы, лицензия заблокирована, нарушение целостности ключевого файла (информация заносится при запуске программы и в процессе ее работы);
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 дней до окончания срока).

Просмотр журнала регистрации операционной системы

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

Текстовый журнал

В текстовый журнал регистрации программы заносится 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 WinRoute**.

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

Журнал отладки

В журнал debug межсетевого экрана Kerio WinRoute Firewall/Kerio Control заносится отладочная информация, которая используется при поиске и анализе ошибок работы программы **Dr.Web для Kerio WinRoute**.

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**.



Глава 9. Диагностика

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

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

Если в процессе установки или работы программы возникли ошибки, вы можете обратиться за помощью в [службу технической поддержки «Доктор Веб»](#). Воспользуйтесь рекомендациями из [приложения Б](#) для получения информации, которую следует отправить специалистам службы технической поддержки вместе с описанием возникшей проблемы.

Проверка установки

Чтобы проверить корректность установки:

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

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 WinRoute\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 WinRoute.
4. Откройте каталог %ProgramFiles%\DrWeb for Kerio WinRoute\ и проверьте, что текстовый журнал регистрации событий DrWebForKWF.log не содержит ошибок.




Проверка работоспособности

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

Проверка работы программы

1. Откройте в браузере страницу <http://www.eicar.org/download/eicar.com>, чтобы скачать тестовый зараженный 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 WinRoute Firewall/Kerio Control должна быть зафиксирована информация о попытке скачать зараженный файл.
2. Отправьте письмо с тестовым зараженным файлом EICAR-Test-File во вложении через сервер, защищаемый Kerio WinRoute Firewall/Kerio Control. Проверьте полученное письмо. Инфицированный файл должен быть удален из письма. Заголовок письма может содержать префикс, оповещающий о найденном вредоносном объекте.

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 WinRoute 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 WinRoute** drwebupw.log, расположенный в каталоге %AllUsersProfile%\Application Data\Doctor Web\Logs\, и убедитесь, что он не содержит ошибок.




Приложения

Приложение А. Параметры командной строки для модуля обновления

Модуль обновления допускает работу в режиме командной строки.

Параметры командной строки в Планировщике заданий

1. Чтобы настроить выполнение задания по обновлению приложения **Dr.Web для Kerio WinRoute**, откройте Планировщик Заданий.
2. В контекстном меню задания **Dr.Web Update for Kerio WinRoute 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.



Параметр	Комментарий
/UPM: <режим>	Включает режим использования прокси-сервера при подключении к сети Интернет. Параметр <режим> может принимать следующие значения: <ul style="list-style-type: none">• direct – не использовать прокси-сервер;• ierproxy – использовать системные настройки прокси-сервера;• userproxy – использовать настройки, заданные пользователем.
/PURL: <адрес>	Указывает адрес прокси-сервера.
/PUSER: <имя>	Указывает имя пользователя для подключения к прокси-серверу.
/PPASS: <пароль>	Указывает пароль для подключения к прокси-серверу.
/UA	Включает режим полного обновления, при котором загружаются обновления для всех файлов, указанных в списке обновления, независимо от используемой операционной системы и установленных компонентов продукта. Данный режим предназначен для получения полной локальной копии серверной области обновления Dr.Web . Этот режим нельзя использовать для обновления антивируса, установленного на компьютере.
/ST	Включает режим невидимого обновления, при котором модуль обновления запускается в невидимом окне (stealth mode).
/LNG: <файл>	Указывает имя файла языковых ресурсов. По умолчанию используется английский язык.
/GO	Включает пакетный режим работы, при котором не выводятся диалоговые окна.



Параметр	Комментарий
/QU	Включает режим принудительного закрытия модуля обновления по завершении обновления вне зависимости от результата. Код результата записывается в переменную ERRORLEVEL окружения операционной системы: <ul style="list-style-type: none">• нулевое значение указывает на успех;• ненулевое значение указывает на неудачу.
/DIR: <i><каталог></i>	Указывает каталога для установки файлов обновления. По умолчанию используется каталог, из которого запущен модуль обновления.
/URM: <i><режим></i>	Включает режим перезагрузки компьютера после обновления. Параметр <i><режим></i> может принимать следующие значения: <ul style="list-style-type: none">• prompt – перезагрузка по окончании обновления после разрешения пользователя;• noprompt – принудительная перезагрузка по окончании обновления при необходимости;• force – принудительная перезагрузка всегда вне зависимости от необходимости;• disable – запрет перезагрузки.
/REG	Включает режим регистрации продукта и получения регистрационного ключа.
/UPD	Включает режим обычного обновления. Используйте этот режим вместе с режимом /REG для загрузки обновлений сразу же после регистрации продукта.
/UVB	Включает режим обновления только вирусных баз и ядра drweb32.dll. Этот параметр отменяет действие ключа /UA .



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



Приложение Б. Действия в случае возникновения проблем

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

Для того чтобы специалисты компании **«Доктор Веб»** смогли помочь вам максимально быстро, пожалуйста, 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 Kerio WinRoute Firewall/Kerio Connect (например, 6.7 build 6399). Для просмотра версии используемого межсетевого экрана выполните следующие действия:
 - откройте Панель управления и выберите пункт **Установка и удаление программ**;
 - в окне **Установка и удаление программ** выберите программу Kerio WinRoute Firewall/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 Dr.Web будет создан по умолчанию в каталоге `%ProgramFiles%\DrWeb for Kerio WinRoute\DrWebForKWF.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 WinRoute** 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 WinRoute**, 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 WinRoute**, например `drweb-KerioWinRoute-600-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 WinRoute**. Для этого выполните следующие действия:



- найдите в проводнике установочный файл программы (например, drweb-KerioWinRoute-600-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 быть 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:
 - значение параметров Applications, Created и Expired, например:
Applications=Update, Scheduler,
KerioPlugin
Created=2010-01-05 (12:00) UTC
Expires=2010-07-05 (12:00) UTC
 - секцию [Settings], например:
MailServer=Yes
FileServer=No
InetGateway=No
SpamFilter=No
LotusSpamFilter=No
EmailAddresses=Unlimited
TrafficLimit=Unlimited



Приложение В. Работа в режиме централизованной защиты

Dr.Web для Kerio WinRoute 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 3](#)).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз безопасности и спама *локальными антивирусными компонентами* (клиентами; в данном случае – антивирусом **Dr.Web для Kerio WinRoute**), 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 3. Логическая структура антивирусной сети.



Все необходимые обновления на центральный сервер 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 WinRoute в режиме централизованной защиты

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



Приложение **Dr.Web для Kerio WinRoute** версии 6.00.2 не совместимо с **Dr.Web Enterprise Agent** версии, отличной от 6.

Для **Dr.Web для Kerio WinRoute** реализованы следующие возможности работы в режиме централизованной защиты:

- регистрация запуска межсетевого экрана Kerio с установленным приложением **Dr.Web для Kerio WinRoute**. События запуска будут отображаться в таблице **Запуск/Завершение Центра Управления Dr.Web**. Время остановки межсетевого экрана Kerio с установленным приложением не регистрируется;
- отправка статистики работы программы **Dr.Web для Kerio WinRoute**. 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 **Цentra Управления Dr.Web**. Это позволяет отключить стандартный модуль обновления **Dr.Web Updater**, запускаемый по расписанию. В этом случае обновление компонентов будет выполняться согласно расписанию **Цentra Управления Dr.Web** и из его репозитория;
- использование лицензионного ключевого файла **Dr.Web для Kerio WinRoute**, зарегистрированного для данной станции в антивирусной сети. При запуске межсетевого экрана Kerio с установленным приложением **Dr.Web для Kerio WinRoute** 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

Д

- Dr.Web для Kerio WinRoute
 - веб-консоль 37, 38
 - карантин 33
 - обновление 40
 - основные функции 6
 - параметры 23, 24, 27
 - проверка работы 46
 - статистика 38
 - удаление 19
 - установка 17

Е

- event log 43

К

- Kerio Control 15
- Kerio WinRoute Firewall 15

А

- антивирусная проверка 30

В

- веб-консоль 37, 38
 - доступ 37
 - лицензия 38
 - обновление 38
 - статистика 38
- вирусная проверка 30

Д

- диагностика 46

Ж

- журналы регистрации 43
 - журнал отладки 45
 - операционной системы 43
 - текстовый журнал 44

И

- интернет-подключение 21

К

- карантин 33
- ключ 10
- ключевой файл 12
 - действительность 10
 - использование 13
 - параметры 13
 - получение 11
 - формат 13

Л

- лицензионный ключевой файл 10, 12
- лицензирование 10
- лицензия 38
 - использование 13
 - обновление 12
 - параметры 13



Предметный Указатель

лицензия 38
 получение 11

М

межсетевой экран 15
методы обнаружения вирусов 32

Н

настройка 21
 параметров сервера 27
 подключения 21
 прокси 21
 уведомлений 27
настройки сканирования
 выбор протоколов 29

О

обновление 40
 антивирусных баз 38
 лицензии 12
 параметры 49
 проверка 46
обновление лицензии 12
операционная система 15
отладочный журнал 45

П

параметры
 Dr.Web для Kerio WinRoute 23
 антивируса 22, 23, 24, 27
 командной строки 49

лицензирования 13
проверки 24
 регистрации событий 24
 сервера 27
 уведомлений 27
поддержка 9
подключение
 Dr.Web для Kerio WinRoute 22
 проверка 46
подключение к Интернет 21
получение ключевого файла 11
приложение 49, 53, 56
проверка
 методы 32
 на вирусы 30
 обновления 46
 подключения к Kerio WinRoute
 Firewall/Kerio Control 46
 установки 46
прокси 21
протоколы 29

Р

регистрация событий 43
 настройка 24
режим работы 56

С

сервер уведомлений 27
системные требования 15



Предметный Указатель

сканирование

настройка 29

настройки 22

события 43

журнал операционной системы
43

журнал отладки 45

журналы регистрации 43

регистрация 43

текстовый журнал 44

совместимость 17

статистика 38

Т

текстовый журнал 44

техническая поддержка 9, 53

требования 15

У

уведомления 27

удаление 15

удаление Dr.Web для Kerio WinRoute
19

условные обозначения 8

установка 15

установка Dr.Web для Kerio WinRoute
17

Ф

файл ключа 10

формат ключевого файла 13

Ц

центральная защита 56

