Dr.WEB®

для Qbik WinGate

Защити созданное

Руководство администратора

Dr.Web для Qbik WinGate
Версия 6.0
Руководство администратора
04.12.2014

«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

Введение

Благодарим вас за приобретение **Dr.Web для Qbik WinGate**. Данная программа подключается к прокси-серверу Qbik WinGate и обеспечивает надежную защиту сетевого трафика и электронной почты от вирусов и спама.

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 Qbik WinGate проверяет сетевой трафик, передаваемый по протоколам HTTP/POP3/FTP прокси-сервера и SMTP-сервера, на вирусы, программы дозвона, рекламные программы, потенциально опасные программы, программы взлома и программы-шутки. При обнаружении угроз безопасности к ним применяются действия согласно настройкам приложения.

Программа использует эффективный и компактный модуль **Антиспама**, не требующий обучения и позволяющий задавать различные действия для каждой из трех предусмотренных программой категорий спама, а также создавать черный и белый списки электронных адресов.

Основные функции программы

Dr.Web для Qbik WinGate выполняет следующие функции:

- антивирусную проверку данных, передаваемых по протоколам HTTP, FTP, SMTP и POP3, а именно:
  - почтовых сообщений и вложенных в них файлов;
  - файлов и данных, передаваемых по протоколам HTTP и FTP.
- проверку на спам почтовых сообщений, обрабатываемых службами SMTP server и POP3 proxy server прокси-сервера WinGate;
- обнаружение вредоносного программного обеспечения;
- лечение инфицированных файлов, передаваемых по протоколу HTTP;
- изоляцию инфицированных файлов в **Карантине Dr.Web** и/или карантине WinGate;
- использование эвристического анализатора для дополнительной защиты от неизвестных вирусов;
- регулярное автоматическое обновление вирусных баз.

Настоящее руководство призвано помочь администраторам корпоративных сетей, использующих прокси-сервер Qbik WinGate, установить и настроить программу **Dr.Web для Qbik WinGate**, а также ознакомиться с ее основными функциями.

Дополнительную информацию об антивирусной проверке сетевого трафика при использовании прокси-сервера Qbik WinGate вы можете найти на официальном сайте компании по адресу http://www.wingate.com/products/wingate/index.php.

Используемые обозначения

В данном руководстве применены следующие условные обозначения (табл. 1).

Таблица 1. Условные обозначения

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

Техническая поддержка

Страница службы технической поддержки компании **«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/.

Ближайшее к вам представительство компании **«Доктор Веб»** и всю необходимую пользователю контактную информацию можно найти по адресу http://company.drweb.com/contacts/moscow.

Лицензирование

Права пользователя на использование программы **Dr.Web для Qbik WinGate** регулируются при помощи специального файла, называемого *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.

Лицензионный ключевой файл является *действительным* при одновременном выполнении следующих условий:

- срок действия лицензии наступил и не истек,
- лицензия распространяется на все используемые программой модули,
- целостность ключевого файла не нарушена.

При нарушении любого из условий ключевой файл становится *недействительным,* при этом программа **Dr.Web для Qbik WinGate** перестает обнаруживать вредоносные программы и пропускает объекты проверки сетевого трафика без изменений. Факт нарушения корректности ключевого файла записывается в журнал регистрации событий операционной системы.

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 ключевой файл был включен в состав дистрибутива при комплектации;
- на отдельном носителе в виде файла.

Получение лицензионного 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, который 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 Qbik WinGate и уже установлена программа **Dr.Web для Qbik WinGate** 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 Qbik WinGate**. 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 Qbik WinGate\).
2. Программа **Dr.Web для Qbik WinGate** 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 Qbik WinGate** ключевой файл копируется в каталог установки программы (обычно %ProgramFiles%\DrWeb for Qbik WinGate).

В процессе работы **Dr.Web для Qbik WinGate** осуществляется поиск первого рабочего ключа (по маске `*.key`) в каталоге установки 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 Qbik WinGate**.

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. Можете проверить следующие параметры лицензирования (табл. 2):

Таблица 2. Параметры ключевого файла

Параметр	Комментарий
Группа `[Key]`, параметр `Applications`	Указывает компоненты программы, которые разрешено использовать владельцу лицензии  Для использования ключевого файла с программой **Dr.Web для Qbik WinGate** в списке компонентов обязательно должны присутствовать компоненты Update и WinGatePlugin.
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 `PluginsAdd`	Указывает, поддерживается ли лицензией **Антиспам** (значение WinGateSpamFilter)

3. Закройте файл, не сохраняя изменений.

Установка и удаление программы

Программа **Dr.Web для Qbik WinGate** устанавливается на тот же компьютер, на котором установлен прокси-сервер Qbik WinGate, и используется им в качестве внешнего антивирусного программного обеспечения, подключаемого через «plug-in» интерфейс.

Дополнительную информацию об использовании антивирусного программного обеспечения совместно с прокси-сервером Qbik WinGate вы можете найти на официальном сайте компании по адресу http://www.wingate.com/products/wingate/index.php.

Системные требования

Компьютер, на который устанавливается **Dr.Web для Qbik WinGate**, должен удовлетворять следующим системным требованиям (табл. 3):

Таблица 3. Системные требования

Компонент	Требование
Место на жестком диске	не менее 350 МБ свободного дискового пространства
Операционная система	одна из следующих: • 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); • Microsoft® Windows Server® 2003 R2; • Microsoft® Windows Server® 2008 (Standard Edition, Enterprise Edition или Datacenter Edition); • Microsoft® Windows Server® 2008 R2; • Microsoft® Windows Server® 2012; • Microsoft® Windows Server® 2012 R2; • Windows Vista® (Starter, Home Basic, Home Premium, Business, Enterprise или Ultimate). Поддерживаются 32- и 64-битные версии операционных систем.
Прокси-сервер	Qbik WinGate 6 ⚠ Проверка работоспособности **Dr.Web для Qbik WinGate** была проведена на версиях 6.2.2 и 6.6.4, которые доступны на сайте разработчика Qbik WinGate по адресу http://www.wingate.com/download/wingate/download.php.

Если помимо **Dr.Web для Qbik WinGate** в системе функционирует антивирусный файловый сторож **Dr.Web SpIDer Guard**, тогда в настройках файлового сторожа необходимо добавить в исключения проверки файлы по маскам `wgf*.tmp` и `*.quo`, а также путь к карантину WinGate (обычно C:\Program Files\WinGate\Quarantine), для того чтобы программой **Dr.Web для Qbik WinGate** осуществлялась проверка сетевого трафика.

Нормальная работа программы не может быть гарантирована, если в системе функционирует антивирусный продукт стороннего производителя.
Для защиты операционной системы используйте решения **«Доктор Веб»** для рабочих станций или для файловых серверов (для серверных ОС).
Ознакомиться с основными функциями как этих так и других продуктов **«Доктор Веб»** можно на официальном сайте компании по адресу http://products.drweb.com/.

Dr.Web для Qbik WinGate не совместим со следующими программными продуктами:

- Webroot Spy Sweeper;
- Webroot AntiVirus with Spy Sweeper.

Настоящие системные требования относятся только к **Dr.Web для Qbik WinGate**. Требования к прокси-серверу содержатся в документации Qbik WinGate. **Dr.Web для Qbik WinGate** может работать на тех же компьютерах, на которых установлен прокси-сервер Qbik WinGate.

Установка программы

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

Для установки **Dr.Web для Qbik WinGate** необходимо иметь права администратора.

Установка Dr.Web для Qbik WinGate

1. Скопируйте следующие файлы на компьютер, где установлен Qbik WinGate:
   - установочный файл программы;
   - лицензионный ключевой файл.
2. Остановите службу WinGate Engine.
3. В зависимости от используемой версии операционной системы запустите установочный файл программы:
   - **drweb-QbikWinGate-600-windows-nt-x86.exe,** если используется 32-битная операционная система;
   - **drweb-QbikWinGate-600-windows-nt-x64.exe,** если операционная система – 64-битная.
4. Откроется окно с предложением выбрать язык установки. Вы можете выбрать русский или английский язык. Нажмите кнопку **OK.**
5. Откроется окно Мастера установки. Нажмите кнопку **Далее.**
6. Откроется окно с текстом Лицензионного соглашения. Для продолжения установки его необходимо прочитать и принять. Нажмите кнопку **Далее**.
7. На шаге **Лицензионный ключ** укажите путь к лицензионному ключевому файлу программы. Нажмите кнопку **Далее.**
8. На шаге **Папка назначения** укажите путь к папке, в которую вы хотите установить программу (по умолчанию папка **%ProgramFiles%\DrWeb for Qbik WinGate**). Если вы хотите выбрать другую папку, нажмите кнопку **Изменить** и укажите путь к этой папке. Нажмите **Далее.**
9. На шаге **Готова к установке программы** нажмите кнопку **Установить.** Начнется

установка программы **Dr.Web для Qbik WinGate** на ваш компьютер.

10. 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.
11. Запустите службу WinGate Engine.

Приложение **Dr.Web для Qbik WinGate** установлено и может быть подключено к прокси-серверу.

Удаление программы

Для удаления программы **Dr.Web для Qbik WinGate** необходимо иметь права администратора.

Удаление Dr.Web для Qbik WinGate

Для удаления **Dr.Web для Qbik WinGate** выполните следующие действия:

1. Остановите службу WinGate.
2. Откройте **Панель управления** и выберите пункт **Установка и удаление программ,** в окне Установка и удаление программ выберите программу **Dr.Web for Qbik WinGate** и нажмите кнопку **Удалить**. Откроется окно подтверждения удаления. Нажмите кнопку **Да**.
3. 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 **Dr.Web для Qbik WinGate** с вашего компьютера. По завершении удаления нажмите кнопку **Готово.**

Компоненты программы и задание на обновление вирусных баз будут удалены.

Некоторые файлы, которые создаются при работе **Dr.Web для Qbik WinGate**, не будут удалены автоматически. Можно удалить эти файлы вручную:

- файл с настройками программы %ProgramFiles%\DrWeb for Qbik WinGate\drweb32.ini;
- файл статистики работы программы %ProgramFiles%\DrWeb for Qbik WinGate \drwebwingate.stat;
- лицензионный ключевой файл, указанный при установке (по умолчанию, %ProgramFiles% \DrWeb for Qbik WinGate\drweb32.key);
- журнал отладки программы %ProgramFiles%\DrWeb for Qbik WinGate\drwebforwingate.log;
- файл со списком обновляемых файлов %ProgramFiles%\DrWeb for Qbik WinGate\drweb32.lst;
- журнал модуля обновлений %AllUsersProfile%\Application Data\Doctor Web\Logs\drwebupw.log.

Начало работы

Перед работой с программой **Dr.Web для Qbik WinGate** необходимо подключить ее к прокси-серверу WinGate.

Для запуска графического интерфейса программы выполните одно из следующих действий:

- запустите файл **drwebforwingateconfigurator.exe,** расположенный в каталоге установки программы %ProgramFiles%\DrWeb for Qbik WinGate;
- запустите интерфейс для управления и настройки **Wingate engine** – откройте **GateKeeper** (см. рис. 1) и в меню **Options** выберите пункт **Plug-ins** -> **Dr.Web for Qbik Wingate.**

Настройка программы через графический интерфейс осуществляется только для локального компьютера.

Подключение программы

Dr.Web для Qbik WinGate подключается к прокси-серверу WinGate в качестве внешнего антивирусного программного обеспечения и осуществляет проверку различных видов сетевого трафика в соответствии с настройками приложения.

Подключение Dr.Web для Qbik WinGate

1. Запустите интерфейс для управления и настройки **Wingate engine** – откройте **GateKeeper** (рис. 1).

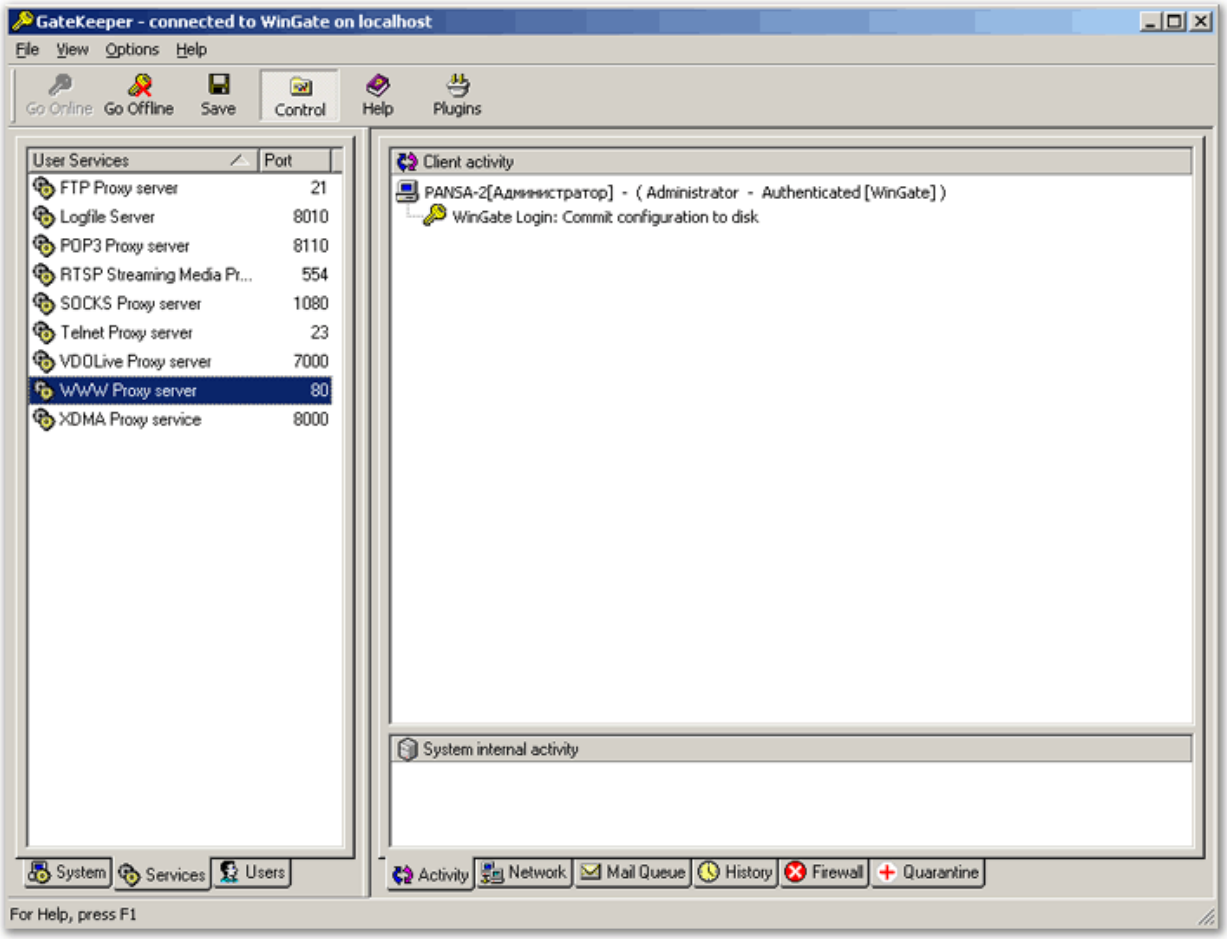

Рисунок 1. GateKeeper

2. Выберите один из следующих разделов, соответствующих системным сервисам, защищаемым программой **Dr.Web для Qbik WinGate**:
   - системный сервис SMTP Server;
   - пользовательский сервис FTP Proxy server;
   - пользовательский сервис POP3 Proxy server;
   - пользовательский сервис WWW Proxy server.
3. В окне свойств сервиса (например, WWW Proxy server, рис. 2) выберите **Configuration** -> **Plug-ins.**

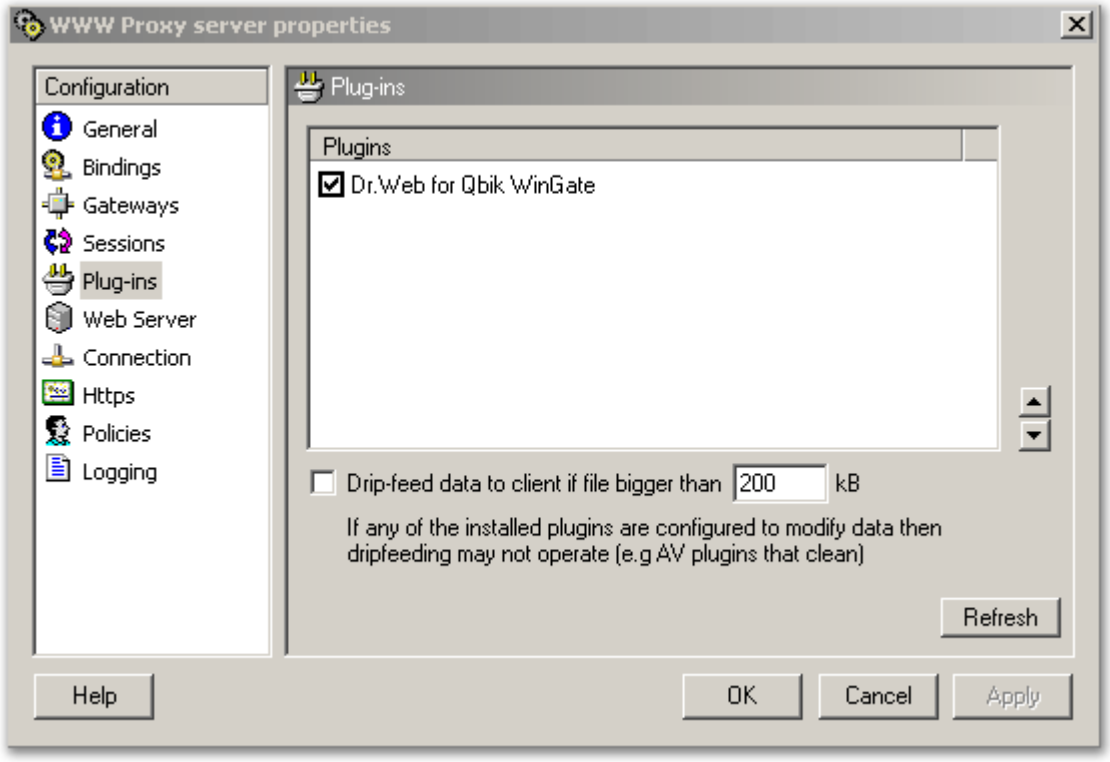

Рисунок 2. Окно свойств WWW Proxy server

4. В окне **Plugins** установите флажок **Dr.Web для Qbik WinGate.** Если в списке отсутствует вариант **Dr.Web для Qbik WinGate,** нажмите кнопку **Refresh.**
5. Нажмите кнопку **Apply** или **OK.**

Если при подключении программы **Dr.Web для Qbik WinGate** возникли ошибки, проверьте корректность установки программы, а также проконсультируйтесь с документацией Qbik WinGate для решения возникшей проблемы.

Дополнительную информацию об использовании антивирусного программного обеспечения совместно с Qbik WinGate и возможных ошибках подключения можно найти в документации к Qbik WinGate и на официальном сайте компании по адресу http://www.wingate.com/products/wingate/index.php.

Интерфейс

Графический интерфейс программы служит для проверки текущего состояния и настройки параметров ее работы.

При запуске графического интерфейса открывается окно раздела **Состояние** (рис. 3).

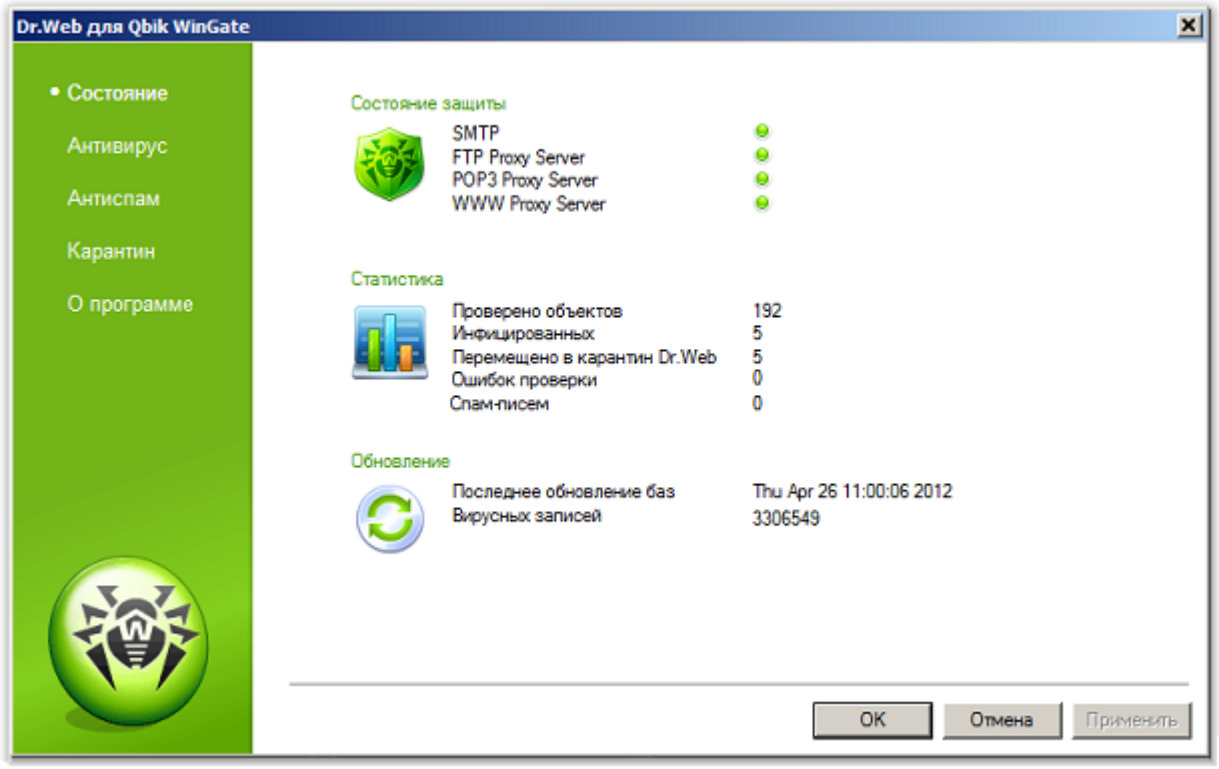

Рисунок 3. Раздел Состояние. Общая информация

В этом разделе отображается основная информация о защите, осуществляемой программой **Dr.Web для Qbik WinGate**, а также о статистике работы и обновлениях программы.

Состояние защиты

В данном разделе приведен список системных сервисов, защищаемых приложением. Индикатор зеленого цвета справа от названия сервиса означает, что сервис использует для проверки данных программу **Dr.Web для Qbik WinGate**.

Статистика

В разделе **Статистика** можно просмотреть общее количество проверенных объектов, количество инфицированных и помещенных в карантин Dr.Web объектов, а также число ошибок, возникших при проверках на вирусы.

Обновление

В данном разделе можно просмотреть дату последнего обновления и количество вирусных записей программы.

Также можно просмотреть информацию о лицензии и об используемых программой модулях в разделе **О программе.**

Настройка работы **Dr.Web для Qbik WinGate** осуществляется в следующих разделах:

- Антивирус – служит для настройки проверки на вирусы и выбора действий программы для обнаруженных вредоносных объектов;
- Антиспам – позволяет настроить работу спам-фильтра, а также создать черный и белый списки электронных адресов;
- Карантин – служит для настройки перемещения вредоносных объектов в карантин и просмотра списка объектов в **Карантине Dr.Web**.

Проверка на вирусы

Программа **Dr.Web для Qbik WinGate** обнаруживает инфицированные вложения в электронных письмах, а также инфицированные объекты, передаваемые по протоколам HTTP и FTP, в том числе следующие вредоносные объекты:

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

Dr.Web для Qbik WinGate не проверяет:

- данные, передаваемые по протоколу HTTP в зашифрованном виде (HTTPs);
- зашифрованные почтовые сообщения;
- поврежденные и архивы с паролем.

Dr.Web для Qbik WinGate использует различные методы обнаружения вирусов, в случае обнаружения при проверке сетевого трафика вредоносных объектов к ним применяются действия в соответствии с настройками программы.

Вы можете определить действия программы для нейтрализации инфицированных файлов, различных типов обнаруженных вредоносных объектов, а также в случае невозможности проверки объекта.

Если при передаче файла по протоколу FTP **Dr.Web для Qbik WinGate** обнаружит в нем угрозу, то процесс передачи данных будет прерван, а используемый FTP-клиент может вернуть ошибку копирования. Безопасная часть копируемого файла может быть записана на диск, но данные в нем будут потеряны.

В случае возникновения проблем при проверке больших файлов по протоколу HTTP настройте работу приложения **Dr.Web for Qbik Wingate** в окне свойств WWW Proxy server (см. рис. 2). Для этого:

1. Установите флажок **Drip-feed data to client if file bigger than.**
2. Укажите максимальный размер файла.
3. Нажмите кнопку **Apply** или **OK.**

Данная опция позволяет передавать клиенту часть полученных данных во время сканирования файла. Это предотвращает простой в работе почтовых клиентов, таких как Outlook или Internet Explorer, при ожидании загрузки данных.

Методы обнаружения вирусов

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. *Сигнатурой* 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 шифрованных 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.

Настройки проверки

Настроить антивирусную проверку интернет-трафика можно в разделе **Антивирус** (рис. 4), определив действия программы для обнаруженных вредоносных объектов.

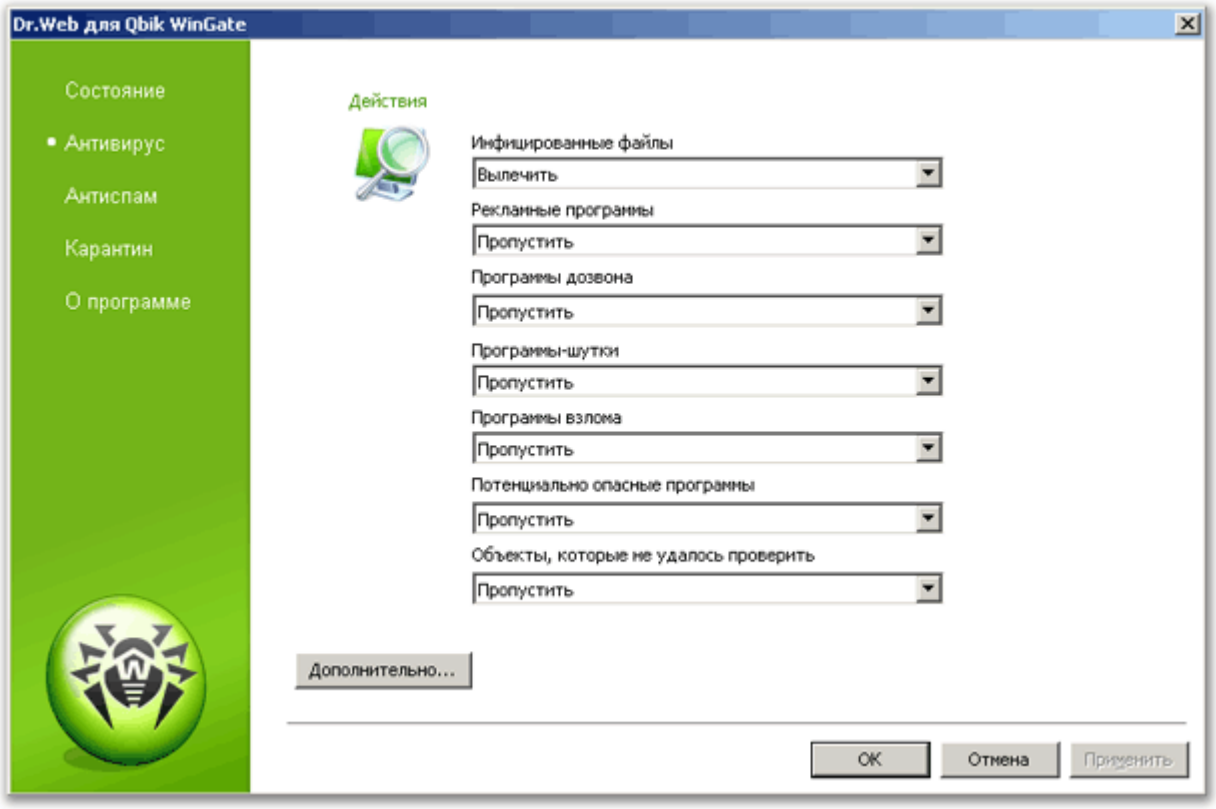

Рисунок 4. Раздел Антивирус

Если файл содержит вирус или относится к одному из типов вредоносных объектов, а также в случае невозможности его проверки к нему могут быть применены следующие действия:

- **Вылечить –** программа предпримет попытку вылечить объект. В случае, если вылечить объект не удалось, он будет заблокирован, как неизлечимый;
- **Переместить в карантин –** объект будет заблокирован, а его копия будет перемещена в **Карантин Dr.Web** и/или Карантин WinGate (в соответствиями с настройками карантина);
- **Удалить –** объект будет заблокирован без сохранения его копии в карантине;
- **Пропустить –** объект будет пропущен без изменений.

Дополнительные настройки сканирования

Для доступа к дополнительным настройкам программы нажмите кнопку **Дополнительно** в разделе **Антивирус.** В открывшемся окне **Дополнительные настройки** (рис. 5) можно определить специфические настройки антивирусной проверки, а также настроить ведение отчетов программы.

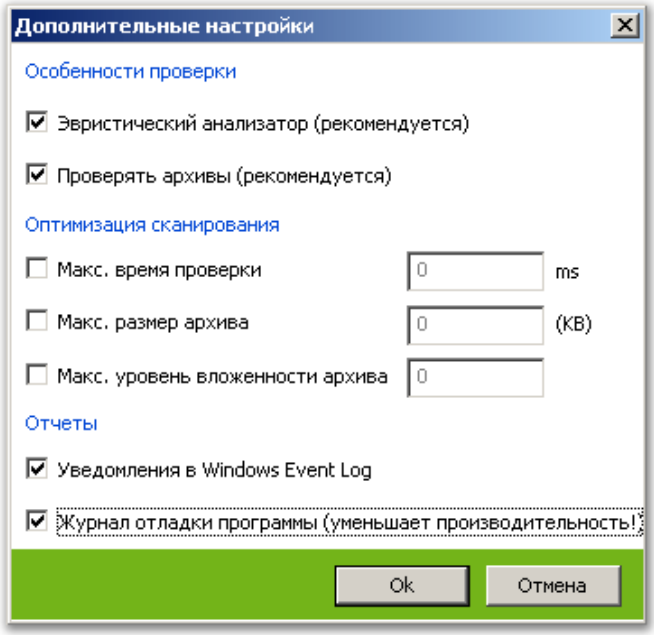

Рисунок 5. Дополнительные настройки сканирования

В группе настроек **Особенности проверки** можно определить следующие параметры проверки:

- **Эвристический анализатор –** с помощью данного параметра можно включить/выключить эвристический анализатор, который обнаруживает неизвестные вирусы;
- **Проверять архивы –** данный параметр позволяет включить/выключить проверку архивов.

В группе настроек **Оптимизация сканирования** можно задать ограничения на время проверки и характеристики проверяемых объектов:

- **Макс. время проверки –** с помощью данного параметра вы можете задать максимальное время (в миллисекундах) на сканирование одного файла. По умолчанию время проверки не ограничено;
- **Макс. размер архива –** данный параметр определяет максимальный размер файла архива (в килобайтах) при проверке. По умолчанию размер файла архива не ограничен;
- **Макс. уровень вложенности архива –** данный параметр служит для ограничения уровня вложенности архива (от 0 до 16 уровней). По умолчанию количество уровней вложенности не ограничено.

Если соответствующие характеристики проверяемого объекта превысят значения, заданные параметрами **Макс. время проверки, Макс. размер архива** и **Макс. уровень вложенности архива,** то к нему будут применены действия, определенные параметром **Объекты, которые не удалось проверить.**

В группе настроек **Отчеты** можно настроить ведение отчетов программы, включив/выключив регистрацию событий в журнал операционной системы и/или журнал отладки программы.

Карантин

Инфицированные вложения и спам могут быть перемещены в **Карантин Dr.Web**, который служит для изоляции и безопасного хранения вредоносных объектов. При обнаружении угрозы в трафике протоколов FTP и HTTP в карантин перемещается инфицированный файл. При обнаружении угрозы в сообщениях, передаваемых по протоколам SMTP и POP3, а также при перемещении спама, в карантин перемещается исходное письмо (формат .msg) в том виде, в каком оно было передано на сервер.

Объекты, сохраненные в карантине, находятся в каталогах DrWeb Quarantine в корне локальных дисков и остаются на дисках даже после удаления **Dr.Web для Qbik WinGate**, при этом доступ в данные каталоги запрещен. При необходимости, но удалить каталоги, назначив свою учетную запись Windows владельцем каталога (для NTFS).

Включение/выключение карантина

Включить/выключить перемещение инфицированных объектов в **Карантин Dr.Web**, а также использование встроенного карантина WinGate можно с помощью соответствующих настроек в разделе **Карантин** (рис. 6).

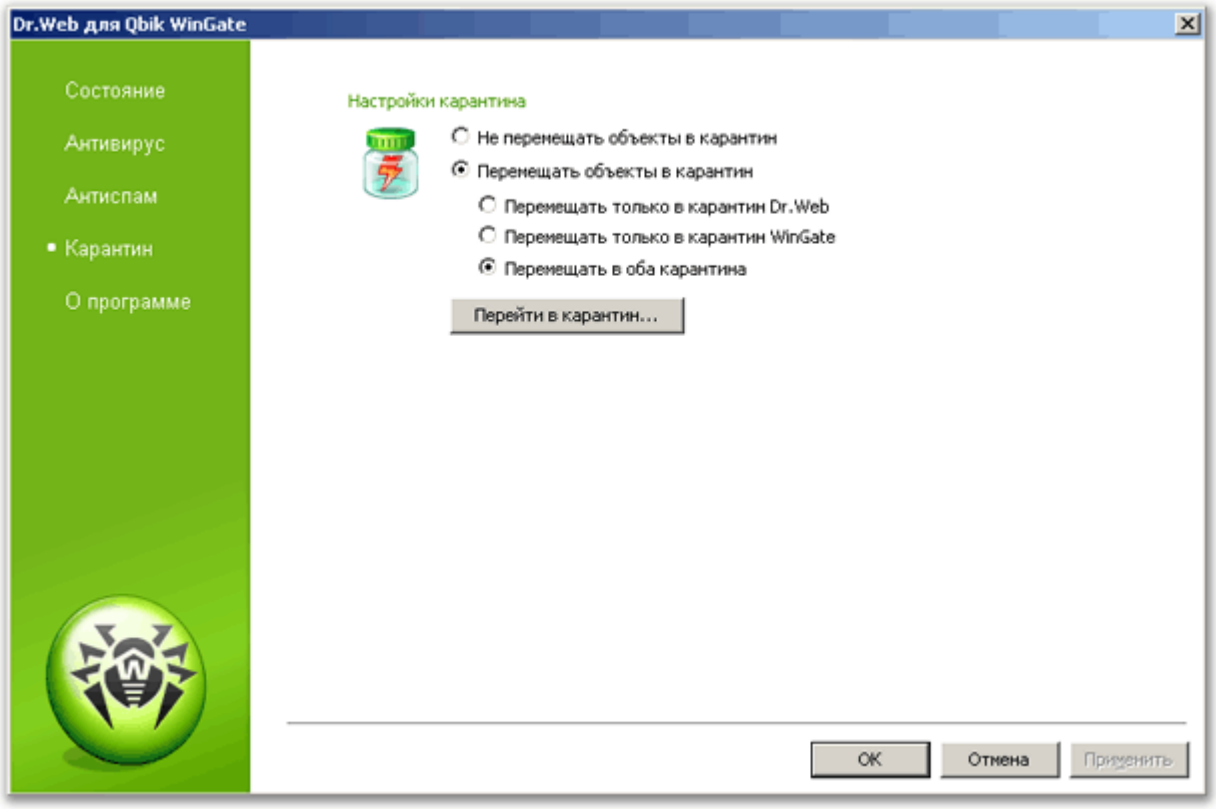

Рисунок 6. Раздел Карантин

Управление карантином Dr.Web

Просмотр файлов, находящихся в **Карантине Dr.Web**, и работа с ними осуществляются с помощью специальной утилиты Dr.Web Quarantine.

Для запуска утилиты зайдите в меню **Пуск** -> **Программы** -> **Dr.Web for Qbik WinGate** и выберите **Dr.Web Quarantine.** Откроется список объектов, помещенных в карантин (рис. 7).

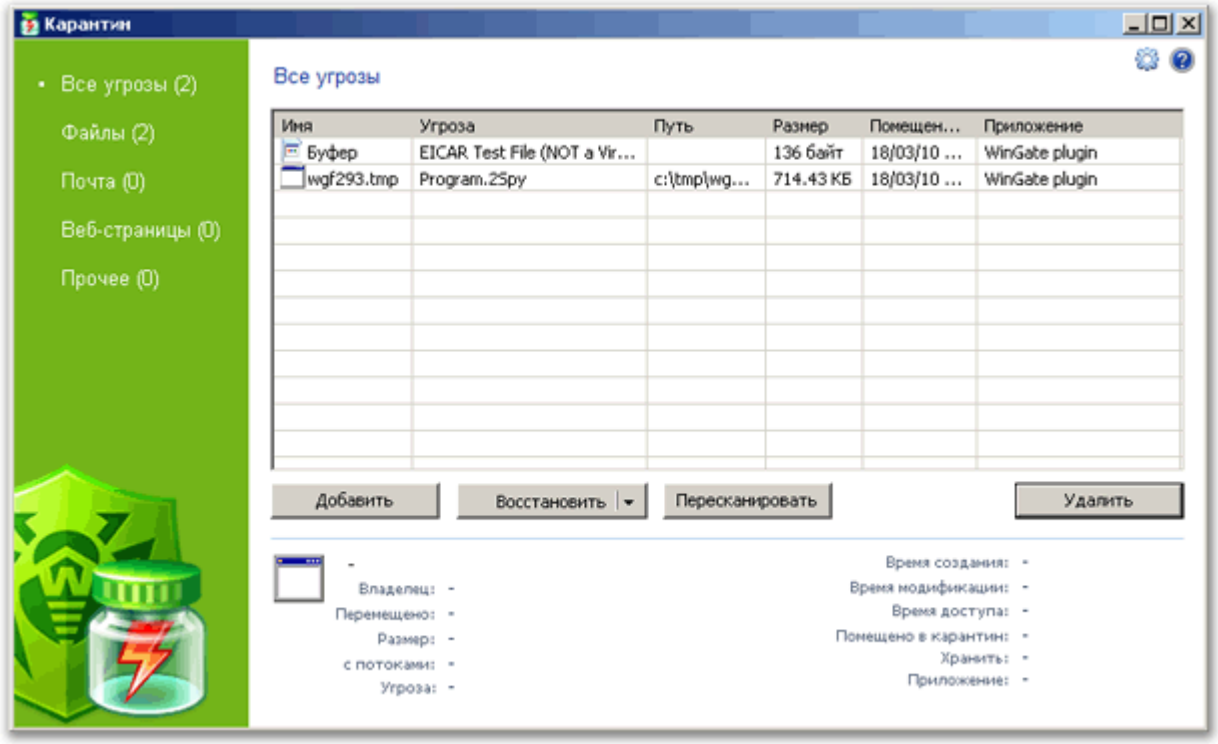

Рисунок 7. Карантин Dr.Web

Для каждого объекта в списке содержится информация об имени и размере зараженного файла, имени вируса, а также путь к папке хранения объекта. 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.

Действия над объектами в карантине

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

1. Выберите один или несколько объектов в списке.
2. Для удаления объекта(ов) нажмите кнопку **Удалить.**
3. Для восстановления объекта(ов) нажмите кнопку **Восстановить** и выберите пункт **Восстановить в,** после чего выберите папку для восстановления объекта(ов).

С помощью кнопки **Пересканировать** можно повторно проверить находящиеся в карантине объекты, в частности, подозрительные файлы, после обновления вирусных баз Dr.Web.

Можете добавить в карантин файлы с локального диска и сменных носителей с помощью кнопки **Добавить,** после чего осуществить антивирусную проверку этих файлов.

Свойства карантина

Для доступа к свойствам карантина нажмите кнопку **Свойства** в верхней части окна **Карантин.** В открывшемся окне **Свойства карантина** (рис. 8) можно изменить следующие настройки:

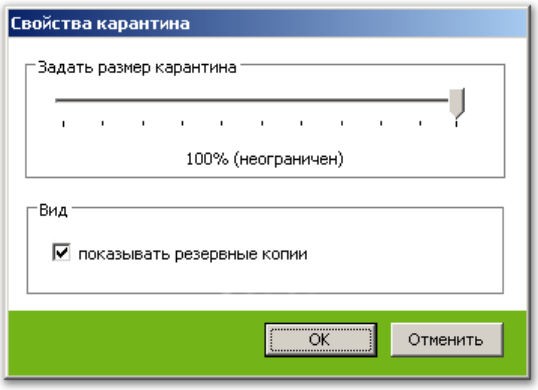

Рисунок 8. Свойства карантина

1. Настроить размер карантина. Для этого установите 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**.

Антиспам

Антиспам позволяет фильтровать электронные сообщения, обрабатываемые службами SMTP server и POP3 proxy server, предотвращая тем самым получение нежелательных сообщений, например, рекламных рассылок.

Предусмотрено три категории спама, для каждой из которых можно задать одно из четырех действий – пропустить, переместить в карантин, удалить, пропустить с пометкой о возможном спаме.

В разделе **Антиспам** (рис. 9) можно включить или выключить проверку почты на спам и определить действия программы для трех категорий спама – писем с высокой, средней и низкой вероятностью спама.

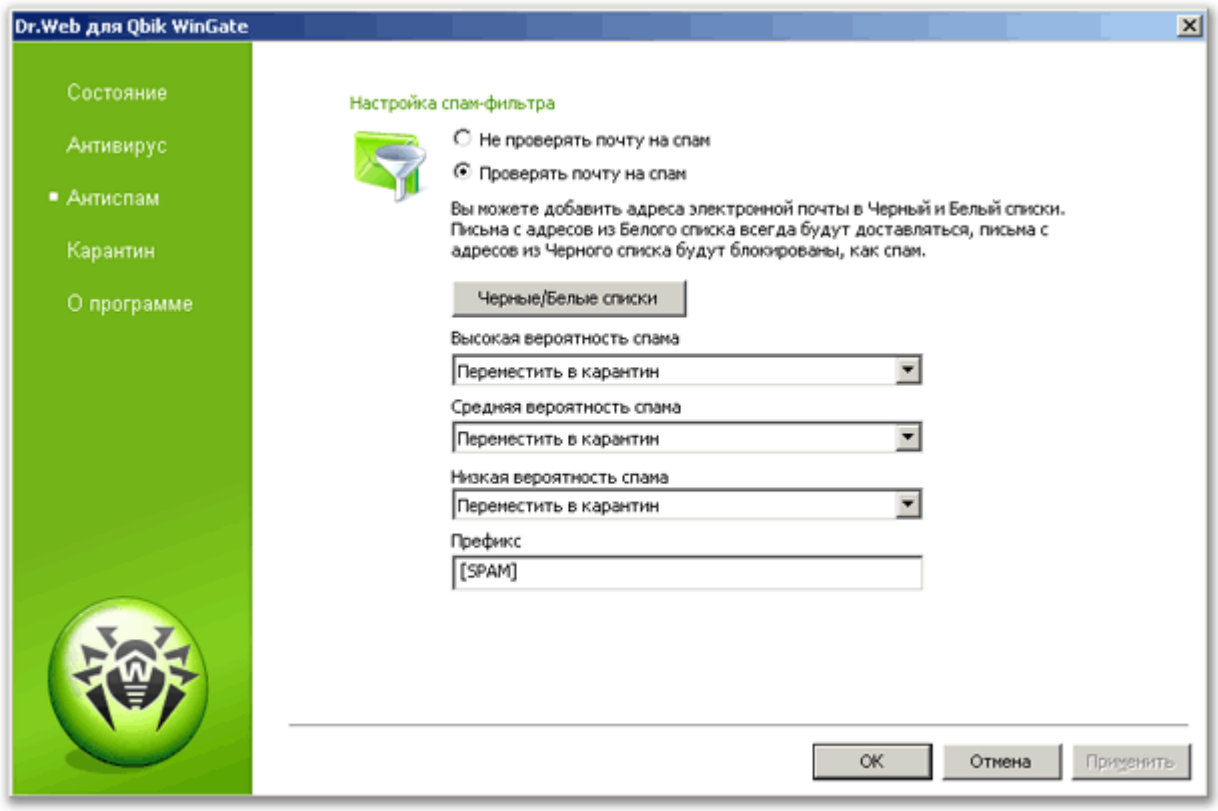

Рисунок 9. Раздел Антиспам

Настройки в разделе **Антиспам** доступны, только если ключевой файл поддерживает использование компонента **Антиспам**. Информацию о ключевом файле можно проверить в разделе **О программе** в окне настроек **Dr.Web для Qbik WinGate**.

Если поддержка **Антиспама** не предусмотрена лицензией, настройки проверки на спам будут недоступны, и сама проверка сообщений на спам осуществляться не будет.

Для каждой категории спама можете задать одно из следующих действий:

- **Пропустить –** письмо будет пропущено и доставлено получателю.
- **Переместить в карантин –** письмо будет перемещено в карантин в соответствии с настройками карантина и не будет доставлено получателю.
- **Удалить –** письмо будет удалено.
- **Добавить префикс в тему письма и доставить –** в тему письма будет добавлен

префикс, указанный в поле **Префикс,** и письмо будет доставлено получателю.

В поле **Префикс** можно указать текст, который будет добавляться к теме письма при выборе соответствующей настройки.

Если **Антиспам** неправильно распознал некоторые письма, следует отправить их на специальные почтовые адреса для анализа и повышения качества работы фильтра:

- письма, ошибочно принятые за спам, следует отправлять на адрес vrnonspam@drweb.com.
- нераспознанные и пропущенные спам-сообщения следует отправлять на адрес vrspam@drweb.com.

Все сообщения необходимо высылать только в виде вложения (а не в теле письма).

Черные/Белые списки

Черный и белый списки используются для дополнительной фильтрации сообщений. Можете добавить электронные адреса, которым доверяете, в белый список. К письмам с данных адресов не будут применяться никакие действия вне зависимости от их содержания. Если же добавить адрес в черный список, то все письма с этого адреса попадут в категорию **Высокая вероятность спама,** и к ним будут применены соответствующие действия.

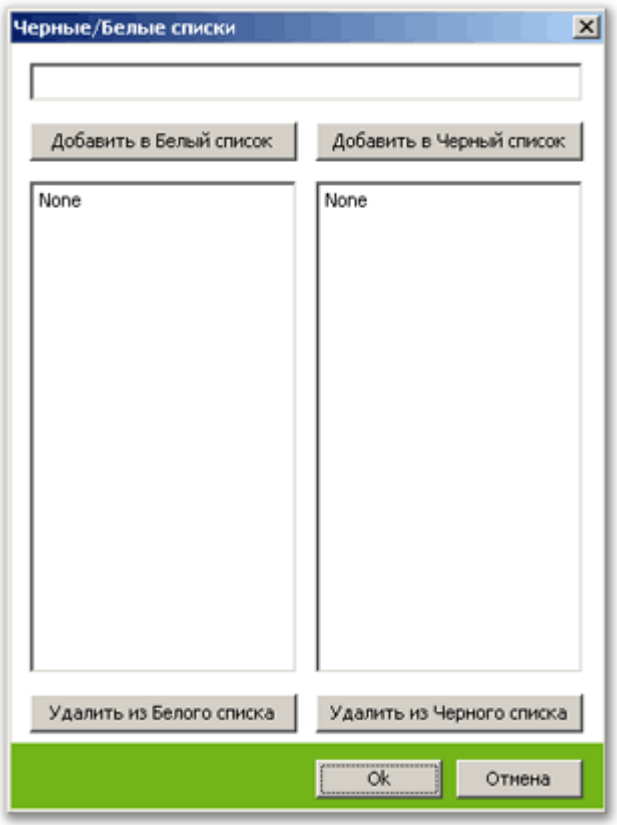

Рисунок 10. Черные/Белые списки

Для работы с черным и белым списками нажмите кнопку **Черные/Белые списки** в разделе **Антиспам** (см. рис. 9). Для добавления адреса в черный или белый список, укажите его в текстовом поле в окне **Черные/Белые списки** и нажмите кнопку **Добавить в Белый список** или **Добавить в Черный список** соответственно (см. рис. 10, ниже).

Для удаления адреса из черного или белого списка, выделите его и нажмите кнопку **Удалить из Черного списка** или **Удалить из Белого списка** соответственно.

При внесении адреса в список можете использовать подстановочный символ «*» вместо части адреса (например, запись вида `*@domain.org` означает все адреса в домене **domain.org**).

Обновление вирусных баз

Модуль обновления (drwebupw.exe) может быть запущен сразу после установки **Dr.Web для Qbik WinGate** 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 Qbik WinGate** 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.

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

По умолчанию при установке **Dr.Web для Qbik WinGate** создается задание по обновлению вирусных баз, в котором задан оптимальный интервал запроса обновлений с сервера Всемирной системы обновлений компании **«Доктор Веб»**. При желании можно отредактировать данное расписание при помощи планировщика заданий Windows. Также настроить работу модуля обновления можно, используя параметры командной строки (Приложение 1).

Редактирование расписания обновлений

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

Обновление без подключения к сети Интернет

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

   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.
   Список доступных к обновлению компонентов можно просмотреть в файле drweb32.lst, расположенном в каталоге установки **Dr.Web для Qbik WinGate** (обычно %ProgramFiles% \DrWeb for Qbik WinGate).
3. На локальном компьютере, где вы хотите настроить обновление через центральный каталог, откройте Планировщик заданий.
4. В контекстном меню задания **Dr.Web Update for Qbik WinGate Plugin** выберите пункт **Свойства.**

5. В диалоговом окне Dr.Web Update for Qbik WinGate 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 **OK**.

Регистрация событий

Dr.Web для Qbik WinGate регистрирует ошибки и происходящие события в следующих журналах регистрации:

- журнале регистрации событий операционной системы Event Log;
- текстовом файле журнала отладки Dr.Web.

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

Журнал операционной системы

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

- сообщения о запуске и остановке программы (запуске и остановке службы WinGate с установленным приложением Dr.Web для Qbik WinGate);
- сообщения об отсутствии или недействительности ключевого файла;
- информация об обнаружении вирусов;
- информация о перемещениях заблокированных объектов в карантин WinGate и/или **Карантин Dr.Web** (при соответствующих настройках проверки);
- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 день до окончания срока).

Включение/выключение регистрации событий в журнале операционной системы

1. В разделе **Антивирус** нажмите кнопку **Дополнительно** для доступа к дополнительным настройкам сканирования, далее выберите/снимите флажок **Уведомления в Windows Event log.**
2. Перезапустите службу WinGate.

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 Qbik WinGate** является приложение Dr.Web для Qbik WinGate.

Журнал отладки

В журнал отладки **Dr.Web для Qbik WinGate** заносится отладочная информация, которая используется при поиске и анализе ошибок работы программы.

Включение/выключение регистрации событий в журнале отладки

1. В разделе **Антивирус** нажмите кнопку **Дополнительно** для доступа к дополнительным настройкам сканирования, далее выберите/снимите флажок **Журнал отладки программы.**
2. Перезапустите службу WinGate.

Включение регистрации событий в отладочный журнал программы **Dr.Web для Qbik WinGate** снижает производительность системы.

Журнал отладки drwebforwingate.log создается в каталоге установки программы **Dr.Web для**

Qbik WinGate (обычно %ProgramFiles%\DrWeb for Qbik WinGate\).

Диагностика

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

- проверка корректности установки
- проверка работы программы
- проверка работы модуля обновления

Проверка установки

Чтобы проверить корректность установки:

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

Имя файла	Описание
drwebupw.exe	Исполняемый файл модуля обновления
update.drl	Список URL-адресов для обновления
drweb32.key	Лицензионный ключевой файл
DrWebQuarantine.exe	Утилита для доступа к **Карантину Dr.Web**
locale.ini	Файл локализации
drwmsg.dll	Служебная библиотека
drwebforwingate.dll	Библиотека приложения **Dr.Web для Qbik WinGate**
drweb32.ini	Файл конфигурации приложения и модуля обновлений
DrWebForWingateConfigurator.exe	Графический интерфейс **Dr.Web для Qbik WinGate**

   - %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

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 Qbik WinGate**.

Проверка работоспособности

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

Проверка работы программы

Для проверки способности **Dr.Web для Qbik WinGate** обнаруживать вирусы в HTTP-трафике выполните следующие действия:

1. Убедитесь, что в разделе **Состояние защиты** (см. рис. 3) включена защита службы WWW Proxy Server.
2. Настройте браузер на работу через прокси-сервер Qbik WinGate с установленным приложением **Dr.Web для Qbik WinGate**.
3. 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://ru.wikipedia.org/wiki/EICAR-Test-File. Загрузка файла eicar.com не должна начаться, а в браузере должна отобразиться страница с информацией о том, что файл инфицирован. Обнаруженный файл с тестовым вирусом EICAR появится в **Карантине Dr.Web**.

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 Qbik WinGate Plug-in** создано.
2. Запустите задание **Dr.Web Update for Qbik WinGate Plug-in.**
3. Откройте журнал обновлений приложения **Dr.Web для Qbik WinGate** drwebupw.log, расположенный в каталоге %AllUsersProfile%\Application Data\Doctor Web\Logs\, и убедитесь, что он не содержит ошибок.

Приложения

Приложение 1. 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 Qbik WinGate**, откройте Планировщик Заданий.
2. В контекстном меню задания **Dr.Web Update for Qbik WinGate Plug-in**  выберите **Свойства.**
3. К тексту команды в поле **Выполнить** добавьте выбранные параметры командной строки.

Допустимые параметры

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)
/DIR:*<каталог>*	Указывает каталога для установки файлов обновления По умолчанию используется каталог, из которого запущен модуль обновления.
/GO	Включает пакетный режим работы, при котором не выводятся диалоговые окна
/INI:*<путь>*	Указывает альтернативный конфигурационный файл
/LNG:*<файл>*	Указывает имя файла языковых ресурсов По умолчанию используется английский язык.
/NI	Запрещает использование параметров, записанных в конфигурационном файле drweb32.ini
/NR	Запрещает создание журнала регистрации обновлений
/PASS:*<пароль>*	Указывает пароль для подключения к серверу обновлений
/ PPASS:*<пароль>*	Указывает пароль для подключения к прокси-серверу
/PURL:*<адрес>*	Указывает адрес прокси-сервера
/PUSER:*<имя>*	Указывает имя пользователя для подключения к прокси-серверу
/QU	Включает режим принудительного закрытия модуля обновления по завершении обновления вне зависимости от результата Код результата записывается в переменную ERRORLEVEL окружения операционной системы: • нулевое значение указывает на успех; • ненулевое значение указывает на неудачу.
/REG	Включает режим регистрации продукта и получения регистрационного ключа
/RP*<файл>* или **/RP+***<файл>*	Включает запись отчет о работе программы в указанный файл По умолчанию используется %AllUsersProfile%\Application Data\Doctor Web\Logs \drwebupw.log.

Параметр	Комментарий
	Используйте параметр **/RP+** для включения режима добавления в существующий файл. Используйте параметр **/RP** для включения режима перезаписи существующего файла.
/SO	Включает звуковое оповещение об ошибках
/ST	Включает режим невидимого обновления, при котором модуль обновления запускается в невидимом окне (stealth mode)
/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 Режим предназначен для получения полной локальной копии серверной области обновления **Dr.Web**. Этот режим нельзя использовать для обновления антивируса, установленного на компьютере.
/UPD	Включает режим обычного обновления Используйте этот режим вместе с режимом **/REG** для загрузки обновлений сразу же после регистрации продукта.
/UPM:*<режим>*	Включает режим использования прокси-сервера при подключении к сети Интернет Параметр *<режим>* может принимать следующие значения: • direct – не использовать прокси-сервер; • ieproxy – использовать системные настройки прокси-сервера; • userproxy – использовать настройки, заданные пользователем.
/URL:*<url>*	Указывает сервер обновлений Допускаются только пути в формате UNC.
/URM:*<режим>*	Включает режим перезагрузки компьютера после обновления Параметр *<режим>* может принимать следующие значения: • 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.
/USER:*<имя>*	Указывает имя пользователя для подключения к серверу обновлений
/UVB	Включает режим обновления только вирусных баз и ядра drweb32.dll Этот параметр отменяет действие ключа **/UA.**

Приложение 2. Действия в случае возникновения проблем

В случае возникновения проблем при использовании программы **Dr.Web для Qbik WinGate** 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 в службу технической поддержки или в систему учета ошибок Dr.Web вместе с вашим запросом.

Рекомендации

1. Сохраните конфигурационный файл drweb32.ini с настройками программы **Dr.Web для Qbik WinGate**, расположенный в каталоге установки программы (обычно %ProgramFiles% \DrWeb for Qbik WinGate).
2. Сохраните файл-отчет со сведениями о системе в формате NFO. Для этого выполните следующие действия:
   - откройте **Пуск** -> **Выполнить** и выполните команду `msinfo32`;
   - в меню **Файл** выберите **Сохранить;**
   - укажите имя файла и нажмите кнопку **ОК.**
3. Сохраните журналы операционной системы **Приложение** и **Система** в формате EVT. Для этого выполните следующие действия:
   - откройте **Пуск** -> **Выполнить** и 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 дождитесь ее проявления. После этого журнал отладки можно отключить. Текстовый журнал отладки drwebforwingate.log будет создан по умолчанию в каталоге %ProgramFiles%\DrWeb for Qbik WinGate.

Если проблемы возникли на этапе установки или удаления приложения:

1. Укажите версию установочного файла **Dr.Web для Qbik WinGate**, с которым возникли проблемы (например, 5.00.2.02190). Для просмотра версии установочного файла выполните следующие действия:
   - найдите в проводнике установочный файл **Dr.Web для Qbik WinGate**, например, drweb-QbikWinGate-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 Qbik WinGate**. Для этого выполните следующие действия:
   - найдите в проводнике установочный файл **Dr.Web для Qbik WinGate** (например, drweb-QbikWinGate-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-qbikwingate-setup.log, расположенный во временном каталоге. Для этого откройте каталог временных файлов %Temp% через меню **Пуск** -> **Выполнить** и в открывшемся окне скопируйте файл drweb-qbikwingate-setup.log.
4. Приложите следующую информацию из используемого лицензионного файла:
   - значение параметров `Applications`, `Created` и `Expired`, например:
     ```
     Applications=Update, Scheduler, WinGatePlugin
     Created=2010-01-05 (12:00) UTC
     Expires=2010-07-05 (12:00) UTC
     ```
   - секцию `[Settings]`, например:
     ```
     FileServer=No
     InetGateway=No
     SpamFilter=No
     LotusSpamFilter=No
     EmailAddresses=Unlimited
     TrafficLimit=Unlimited
     ```