Dr.WEB®
CureIt!®

Защити созданное

Руководство пользователя

Dr.Web® CureIt!®
Руководство пользователя
27.07.2015

«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

Используемые обозначения

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

Таблица 1. Условные обозначения.

Обозначение	Комментарий
Полужирное начертание	Названия элементов графического интерфейса и примеры ввода, который необходимо выполнить в точности так, как он приведен в руководстве.
Зеленое и полужирное начертание	Наименования продуктов **«Доктор Веб»** или их компонентов.
Зеленое и подчеркнутое начертание	Ссылки на страницы руководства и веб-сайты.
`Моноширинный шрифт`	Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением.
Курсив	Термины и замещающий текст (приводится вместо информации, которую необходимо ввести пользователю). В случае примеров ввода командной строки курсив указывает на значения параметров.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Знак плюса (+)	Указывает на одновременность нажатия клавиш клавиатуры. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
Восклицательный знак	Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях.

Dr.Web CureIt!

Dr.Web® CureIt!® представляет собой антивирусный сканер на основе **Dr.Web Scanning Engine**, стандартного сканирующего ядра продуктов семейства **Dr.Web**. Несмотря на некоторые ограничения по сравнению с **Антивирусом Dr.Web для Windows** (отсутствие резидентного монитора, консольного сканера и модуля автоматического обновления и так далее), **Dr.Web CureIt!** способен эффективно проверять систему и выполнять необходимые действия для обезвреживания обнаруженных угроз.

Dr.Web CureIt! обнаруживает и обезвреживает следующие типы вредоносных программ:

- черви;
- вирусы;
- трояны;
- руткиты;
- шпионские программы;
- программы дозвона;
- рекламные программы;
- программы взлома;
- программы-шутки;
- потенциально опасные программы.

Dr.Web CureIt! идеально подходит для ситуаций, когда установка антивируса оказывается невозможной в результате действий вирусов или по какой-либо другой причине, потому что он не требует установки, работает под 32- и 64-битными операционными системами семейств Microsoft® Windows® и Microsoft® Windows Server® (начиная с Microsoft Windows XP и заканчивая Microsoft Windows 8.1) и постоянно обновляется и дополняется свежими вирусными базами, что обеспечивает эффективную защиту от вирусов и прочих вредоносных программ. Помимо этого, **Dr.Web CureIt!** автоматически определяет язык, который использует операционная система. Если язык вашей операционной системы не поддерживается, то **Dr.Web CureIt!** будет использовать английский язык по умолчанию.

В ходе проверки **Dr.Web CureIt!** передает на сервера компании **«Доктор Веб»** общую информацию о проверяемом компьютере и состоянии информационной безопасности на нем. При использовании платной версии **Dr.Web CureIt!** передача статистики является опциональной.

Рекомендуется запускать **Dr.Web CureIt!** от имени пользователя, обладающего правами администратора. В противном случае те файлы и папки, к которым непривилегированный пользователь не имеет доступа (в том числе и системные папки), не будут подвергнуты проверке.

Системные требования

Использование **Dr.Web CureIt!** возможно на компьютере, удовлетворяющем следующим требованиям:

Компонент	Требование
Операционная система	Для 32-разрядных операционных систем: • Windows XP с пакетом обновлений SP2 или SP3; • Windows Vista; • Windows 7; • Windows 8; • Windows 8.1 • Windows 10; • Windows Server 2003 с пакетом обновлений SP1; • Windows Server 2008. Для 64-разрядных операционных систем: • Windows Vista; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10; • Windows Server 2008; • Windows Server 2008 R2; • Windows Server 2012; • Windows Server 2012 R2.
Место на жестком диске	160 МБ свободного дискового пространства.
Свободная оперативная память	Не менее 360 МБ.
Процессор	Поддерживающий систему команд i686 и старше.

Проверка антивируса

Вы можете проверить работоспособность антивирусных программ, обнаруживающих вирусы по их сигнатурам, с использованием тестового файла EICAR- European Institute for Computer Anti-Virus Research.

Многими разработчиками антивирусов принято для этой цели использовать одну и ту же стандартную программу test.com. Эта программа была специально разработана для того, чтобы пользователь, не подвергая свой компьютер опасности, мог посмотреть, как установленный антивирус будет сигнализировать об обнаружении вируса. Программа test.com не является сама по себе вредоносной, но специально обрабатывается большинством антивирусных программ как вирус. **Dr.Web® CureIt!®** называет этот «вирус» следующим образом: `EICAR Test File (Not a Virus!)`. Примерно так его называют и другие антивирусные программы.

Программа test.com представляет собой 68-байтный COM-файл, в результате исполнения которого на консоль выводится текстовое сообщение EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

Файл test.com состоит только из текстовых символов, которые формируют следующую строку:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Если вы создадите файл, содержащий приведенную выше строку и сохраните его под именем test.com, то в результате получится программа, которая и будет описанным «вирусом».

Методы обнаружения угроз

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

Методы обнаружения угроз

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.

Отправка статистики

Для проведения анализа вирусной обстановки в мире и дальнейшего совершенствования механизмов проверки и обезвреживания угроз **Dr.Web CureIt!** предоставляет возможности по отправке обезличенной статистики об антивирусной проверке на сервера компании **«Доктор Веб»**. Данные передаются в ходе проверки и содержат только следующие общие сведения:

- характеристики процессора (имя, техническое описание, текущая и максимальная скорость, количество ядер и количество логических процессоров);
- характеристики оперативной памяти (общее и свободное на момент проверки количество физической и виртуальной памяти);
- параметры операционной системы (имя, версия и номер сборки, установленные пакеты дополнений (service pack), режим загрузки, привилегии учетной записи – пользовательские или административные, региональные настройки);
- сведения об установленном антивирусе, антишпионе и брандмауэре;
- информация об отдельных найденных угрозах (тип и название угрозы, тип и название зараженного объекта, примененное к объекту действие, при необходимости – хеш-сумма зараженного файла);
- сводная информация о проверке (время окончания проверки, количество проверенных файлов и объектов, количество подозрительных объектов, количество обнаруженных угроз каждого типа);
- сводная информация о примененных действиях (количество объектов, к которым действия не применялись, а также количество вылеченных, удаленных, перемещенных, переименованных и проигнорированных объектов).

Вы можете ознакомиться с политикой конфиденциальности компании **«Доктор Веб»** на официальном сайте по адресу http://company.drweb.com/policy/.

Если вы хотите принять участие в сборе статистики для компании **«Доктор Веб»**, то выберите соответствующий вариант при запуске программы.

Начало работы

Dr.Web CureIt! предназначен для проведения антивирусной проверки загрузочных секторов, памяти, а также как отдельных файлов, так и файлов в составных объектах(архивы, файлы электронной почты, инсталляционные пакеты). Проверка производится с использованием всех методов обнаружения угроз.

По умолчанию **Dr.Web CureIt!** не проверяет архивы. Вы можете включить проверку архивов в настройках **Dr.Web CureIt!**.

В случае обнаружения вредоносного объекта **Dr.Web CureIt!** только предупреждает вас об угрозе. Отчет о результатах проверки приводится в таблице. Вы можете как применить действия по умолчанию ко всем обнаруженным угрозам, так и выбрать необходимый метод обработки для отдельных объектов.

Действия по умолчанию являются оптимальными для большинства применений, но при необходимости вы можете изменить их в окне настройки параметров работы **Dr.Web CureIt!**. Если действие для отдельного объекта вы можете выбрать по окончании проверки, то общие настройки по обезвреживанию конкретных типов угроз необходимо задавать до начала проверки.

Изменение языка интерфейса

Чтобы выбрать язык интерфейса **Dr.Web CureIt!**, нажмите иконку **Язык** на панели инструментов и выберите необходимый пункт.

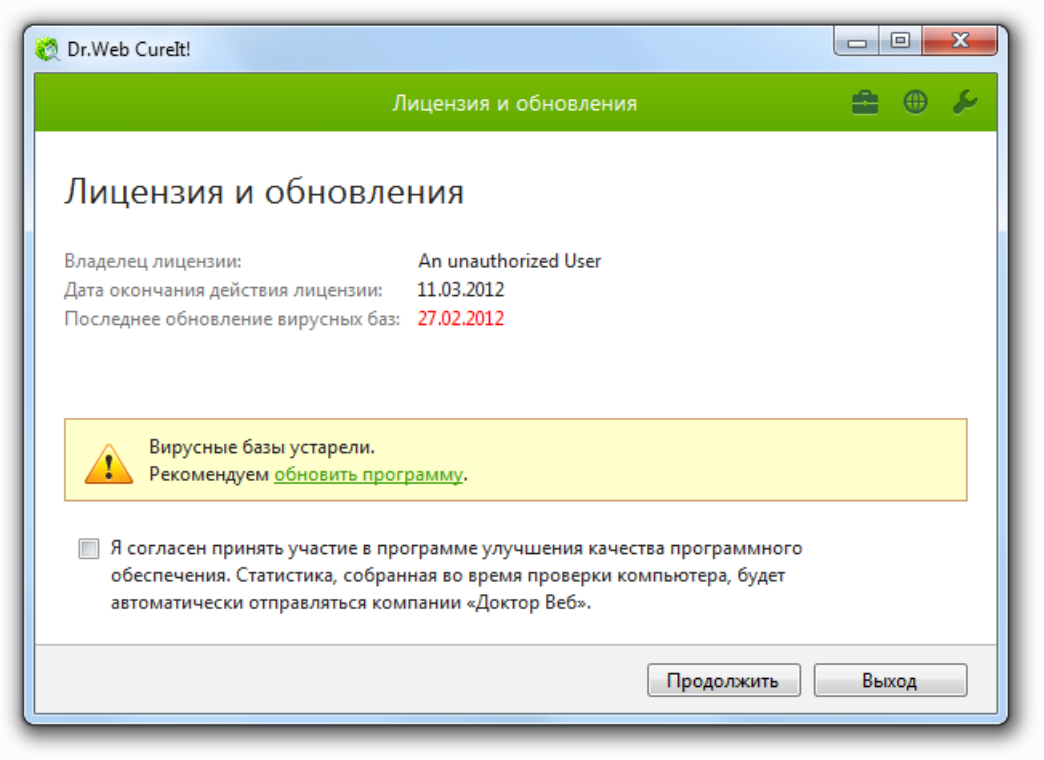
Обновление Dr.Web CureIt!

Dr.Web CureIt! не включает встроенного модуля автоматического обновления, поэтому он остается максимально надежным только до ближайшего выпуска новых дополнений антивирусных баз (который происходит примерно каждый час). После этого для эффективного обнаружения угроз необходимо повторно загружать последнюю версию **Dr.Web CureIt!**, которая всегда доступна на вашей персональной странице на **официальном сайте компании «Доктор Веб»** и снабжена самыми последними вирусными базами и наиболее современным механизмом детектирования вирусных угроз.

Загрузка последней версии Dr.Web CureIt!

1. Запустите **Dr.Web CureIt!**.
2. При необходимости обновления в первом окне **Лицензия и обновление** отображается соответствующее оповещение. Чтобы обновить программу, пройдите по ссылке **обновить программу** в оповещении.

   В окне интернет-браузера по умолчанию откроется ваша персональная страница на **официальном сайте компании «Доктор Веб»**, откуда вы сможете загрузить обновленную версию программы при наличии действительной лицензии или продлить срок действия лицензии.



Быстрая проверка

Dr.Web CureIt! предоставляет предустановленный шаблон быстрой проверки наиболее уязвимых объектов операционной системы.

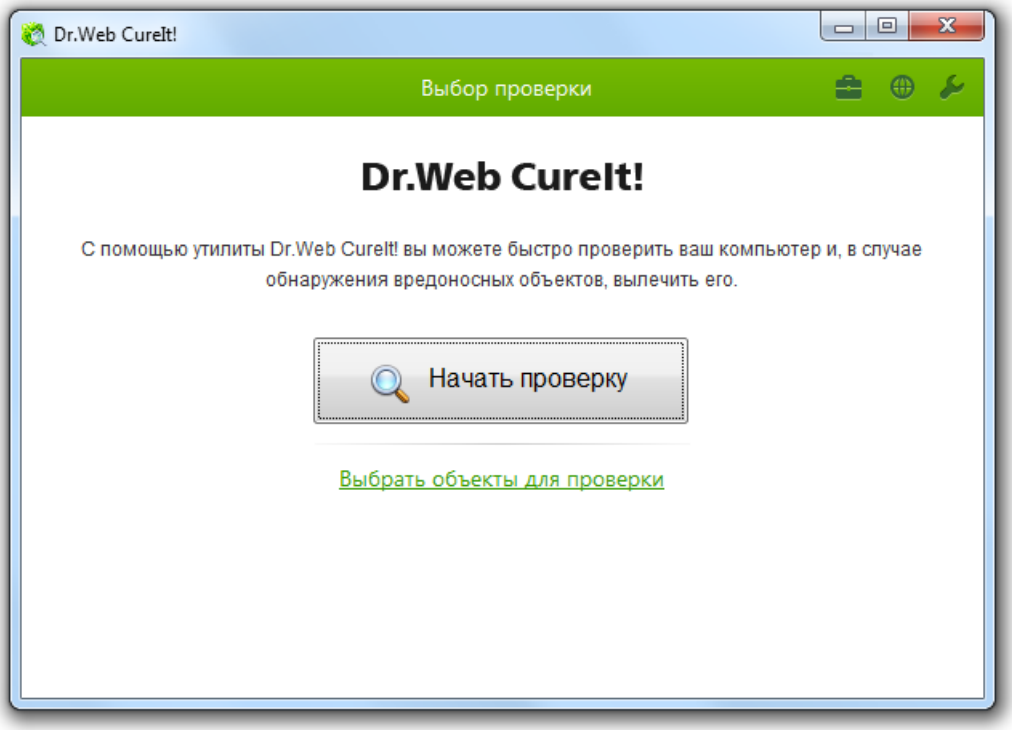
В данном режиме производится проверка следующих объектов:

- оперативная память;
- загрузочные секторы всех дисков;
- корневой каталог загрузочного диска;
- корневой каталог диска установки Windows;
- системный каталог Windows;
- папка Мои Документы;
- временный каталог системы;
- временный каталог пользователя;
- наличие руткитов (если процесс проверки запущен от имени администратора).

При необходимости более гибкой настройки вы можете провести выборочную проверку.

Проведение быстрой проверки

1. Запустите **Dr.Web CureIt!**.
2. В первом окне **Лицензия и обновление** ознакомьтесь с условиями отправки статистики. При желании вы можете присоединиться к программе улучшения качества программного обеспечения. Для этого установите соответствующий флажок. Нажмите кнопку **Продолжить**.
3. В окне выбора типа проверки нажмите кнопку **Начать проверку**.

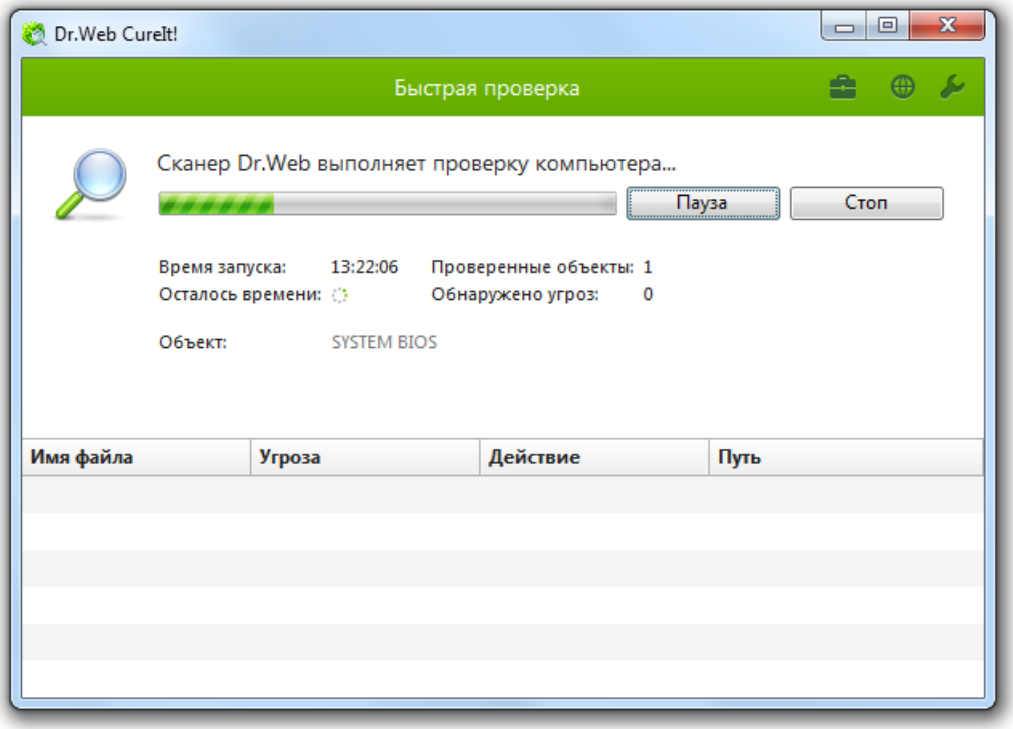


4. В процессе проверки в окне отображается общая информация о ее ходе, а также список обнаруженных угроз.

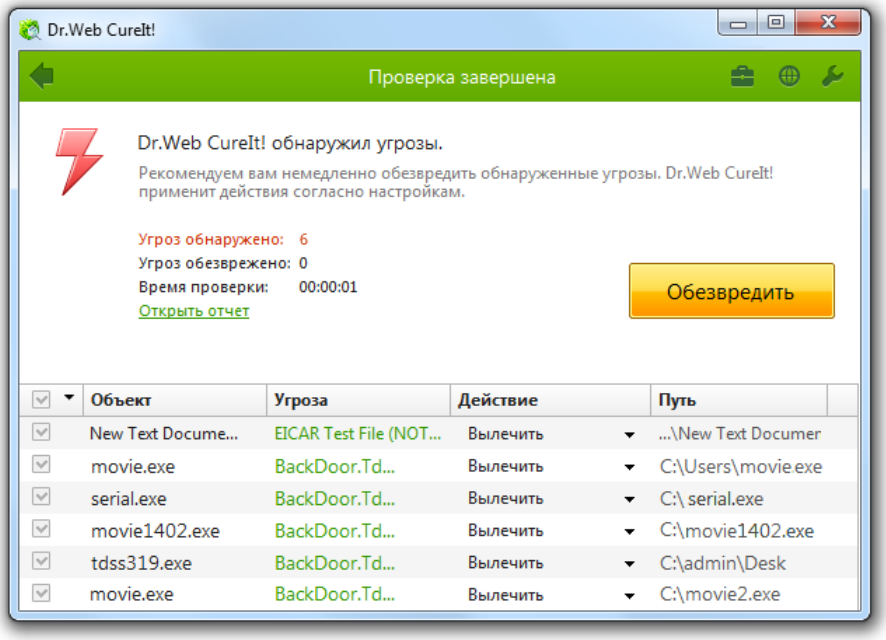
   При необходимости вы можете выполнить следующее:

- чтобы приостановить проверку, нажмите кнопку **Пауза**;
- чтобы возобновить проверку после паузы, снова нажмите кнопку **Продолжить**;
- чтобы полностью остановить проверку, нажмите кнопку **Стоп**.

Кнопка **Пауза** недоступна во время проверки оперативной памяти и процессов.



5. По завершении проверки информация об обнаруженных угрозах приводится в окне отчета. Ознакомьтесь с результатами проверки. При необходимости вы можете просмотреть файл отчета о проверке. Для этого нажмите **Открыть отчет**.



6. Если в ходе проверки были обнаружены вирусы или угрозы других типов, их необходимо

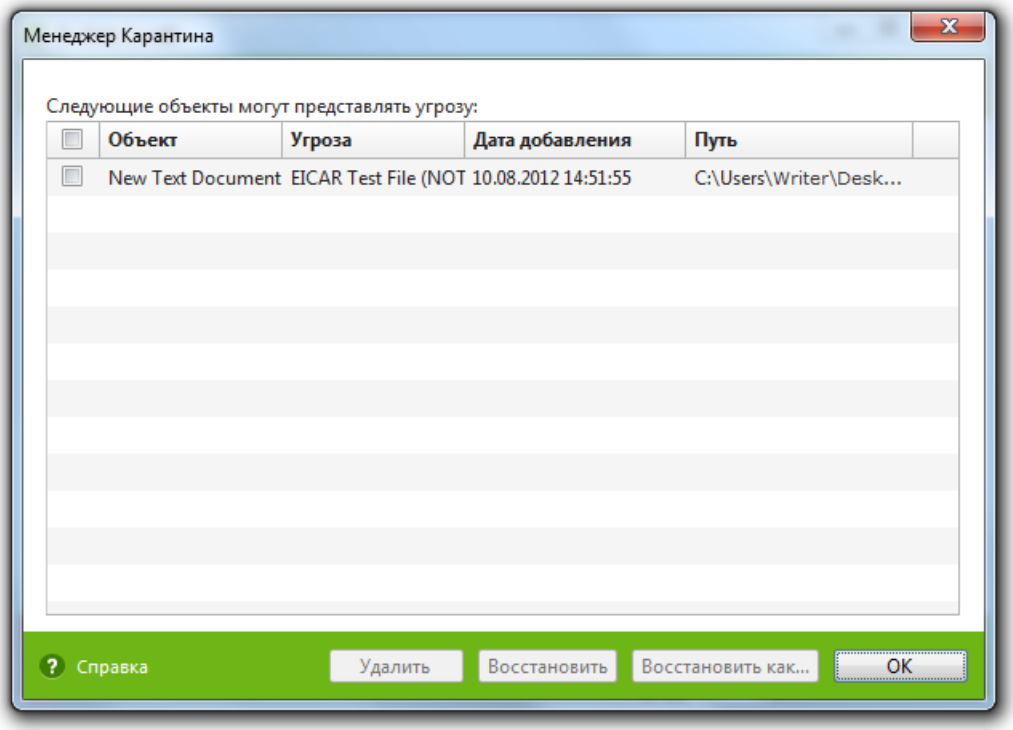
нейтрализовать. Чтобы применить предустановленные действия, нажмите кнопку **Обезвредить**. При необходимости вы можете настроить разные действия для конкретных угроз.

Менеджер Карантина

Это окно содержит данные о содержимом **Карантина Dr.Web CureIt!**, который служит для изоляции файлов, подозрительных на наличие вредоносных объектов. Также в **Карантин** помещаются резервные копии файлов, обработанных **Dr.Web CureIt!**.

Каталог **Карантина** создается в каталоге %USERPROFILE%\Doctor Web\DrWeb CureIt Quarantine. Зараженный объект переносится в соответствующую папку **Карантина** и, если файл находится не на съемном носителе, шифруется.

Чтобы открыть окно **Карантина**, на панели инструментов в окне **Dr.Web CureIt!** щелкните по иконке **Параметры проверки** и выберите пункт **Менеджер Карантина**.



В центральной части окна отображается таблица с информацией о состоянии карантина, включающая следующие поля:

- **Объект** – список имен объектов, находящихся в карантине;
- **Угроза** – классификация вредоносной программы, определяемая **Dr.Web CureIt!** при автоматическом перемещении объекта в карантин;
- **Дата добавления** – дата, когда объект был перемещен в **Карантин**;
- **Путь** – полный путь, по которому находился объект до перемещения в карантин.

В окне **Карантина** файлы могут видеть только те пользователи, которые имеют к ним доступ.

Чтобы отобразить скрытые объекты, запустите **Dr.Web CureIt!** под административной учетной записью.

В окне карантина доступны следующие кнопки управления:

- **Восстановить** – переместить файл из карантина и восстановить первоначальное местоположение файла на компьютере (восстановить файл под тем же именем и в папку, в которой он находился до перемещения в карантин).
- **Восстановить в** – переместить файл под заданным именем в нужную папку;

Используйте данную функцию только в том случае, если вы уверены, что объект безопасен.

- **Удалить** – удалить файл из карантина и из системы.

Для одновременной работы с несколькими файлами установите флажки рядом с названиями объектов, а затем выберите необходимое действие.

Дополнительные возможности

В большинстве случаев для полного излечения компьютера от заражения достаточно провести быструю проверку. В редких случаях, когда необходима тонкая настройка процедуры проверки вы можете воспользоваться следующими дополнительными возможностями:

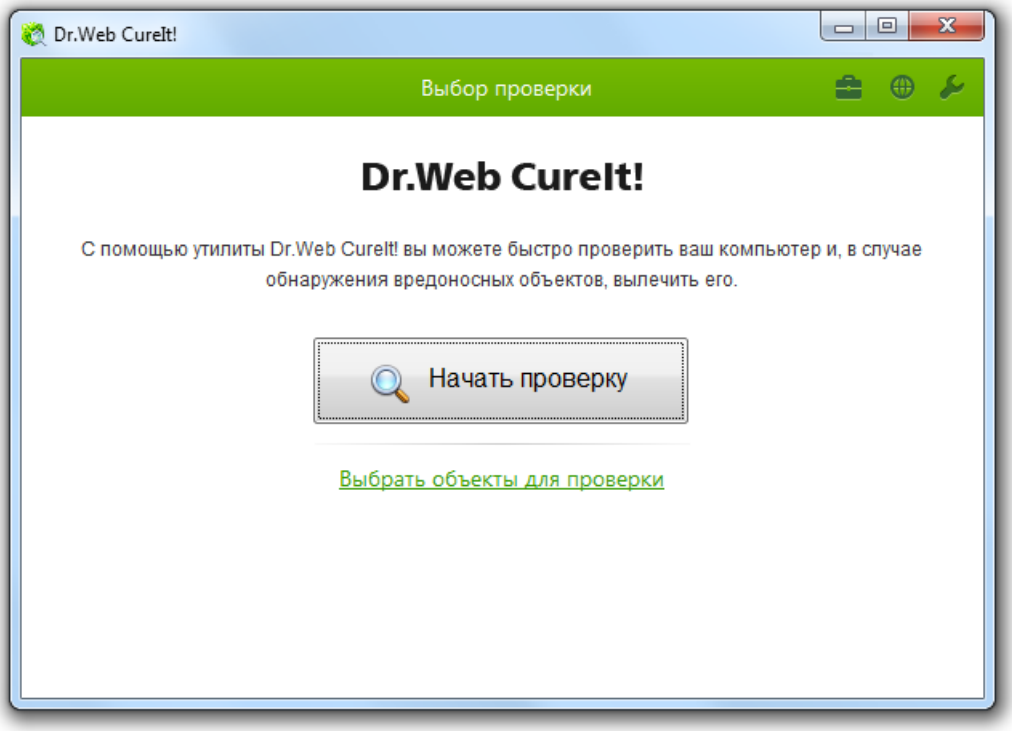
- проведение выборочной проверки, в ходе которой можно указать конкретные объекты операционной системы и отдельные папки и файлы для проверки;
- выбор действий по обезвреживанию обнаруженных угроз;
- общая настройка антивирусной проверки;
- запуск **Dr.Web CureIt!** с параметрами из командной строки.

Выборочная проверка

Помимо предустановленного шаблона быстрой проверки наиболее уязвимых объектов операционной системы **Dr.Web CureIt!** также предоставляет гибкий пользовательский режим, в котором вы можете настроить проверку под свои нужды.

При выборе данного режима перед началом настройки в окне **Dr.Web CureIt!** вы можете задать объекты для проверки: любые файлы и папки, а также такие объекты, как оперативная память, загрузочные секторы и т.п.). В случае быстрой проверки выбирать объекты не требуется.

Выбор вида проверки осуществляется при каждом запуске **Dr.Web CureIt!** на шаге **Выбор проверки**.



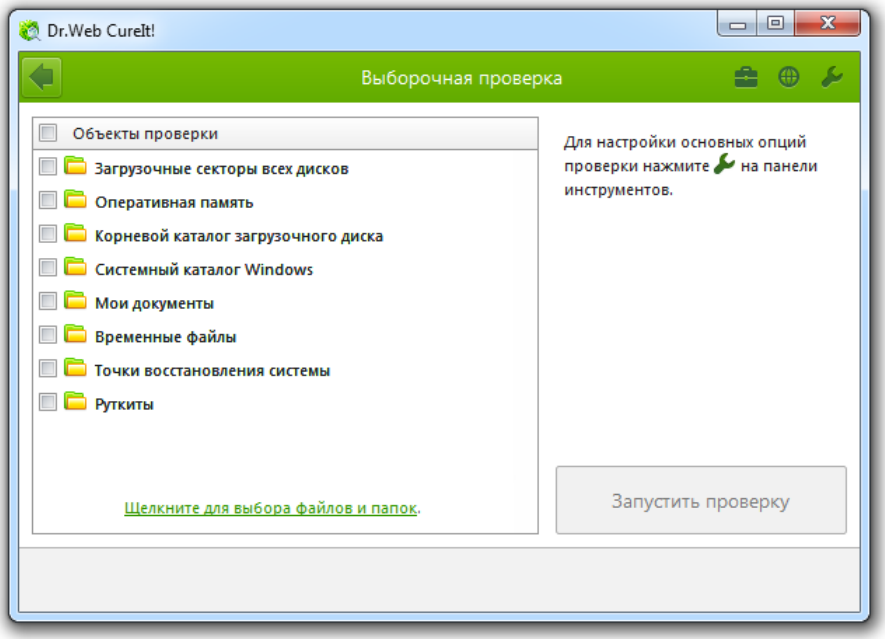
Выборочная проверка

1. Запустите **Dr.Web CureIt!**.
2. В первом окне **Лицензия и обновление** ознакомьтесь с условиями отправки статистики. При желании вы можете присоединиться к программе улучшения качества программного

обеспечения. Для этого установите соответствующий флажок. Нажмите кнопку **Продолжить**.

3. В окне выбора типа проверки нажмите **Выбрать объекты для проверки**.
4. В таблице в центре окна выберите объекты для проверки. Чтобы добавить в список конкретный файл или папку, щелкните по ссылке в нижней части поля таблицы и выберите нужный объект в окне **Обзор**.

   Чтобы выбрать все указанные в таблице объекты, установите флажок **Объекты проверки** в заголовке таблицы.

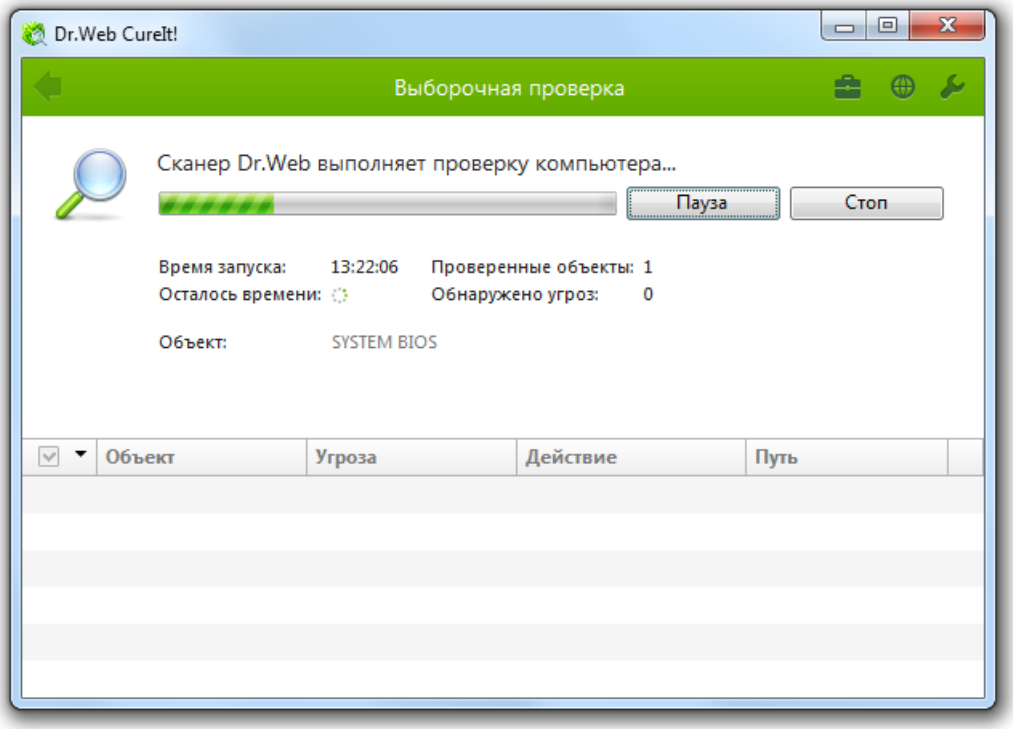


5. При необходимости перед началом проверки настройте параметры работы **Dr.Web CureIt!**. Для этого на панели инструментов нажмите кнопку **Параметры проверки**.
6. Нажмите кнопку **Запустить проверку**.
7. В процессе проверки в окне отображается общая информация о ее ходе, а также список обнаруженных угроз.

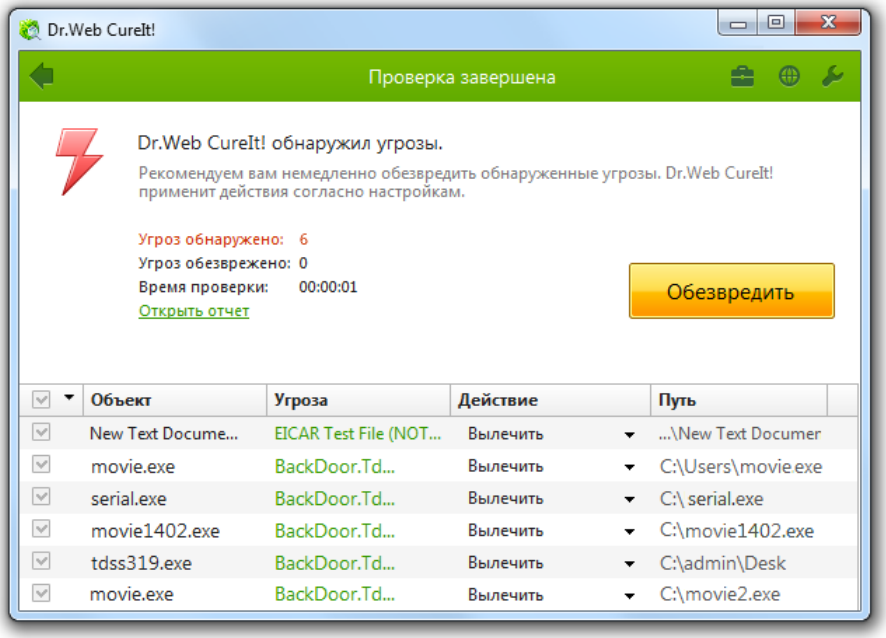
   При необходимости вы можете выполнить следующее:

   - чтобы приостановить проверку, нажмите кнопку **Пауза**;
   - чтобы возобновить проверку после паузы, снова нажмите кнопку **Продолжить**;
   - чтобы полностью остановить проверку, нажмите кнопку **Стоп**.

Кнопка **Пауза** недоступна во время проверки оперативной памяти и процессов.



8. По завершении проверки информация об обнаруженных угрозах приводится в окне отчета. Ознакомьтесь с результатами проверки. При необходимости вы можете просмотреть файл отчета о проверке. Для этого нажмите **Открыть отчет**.

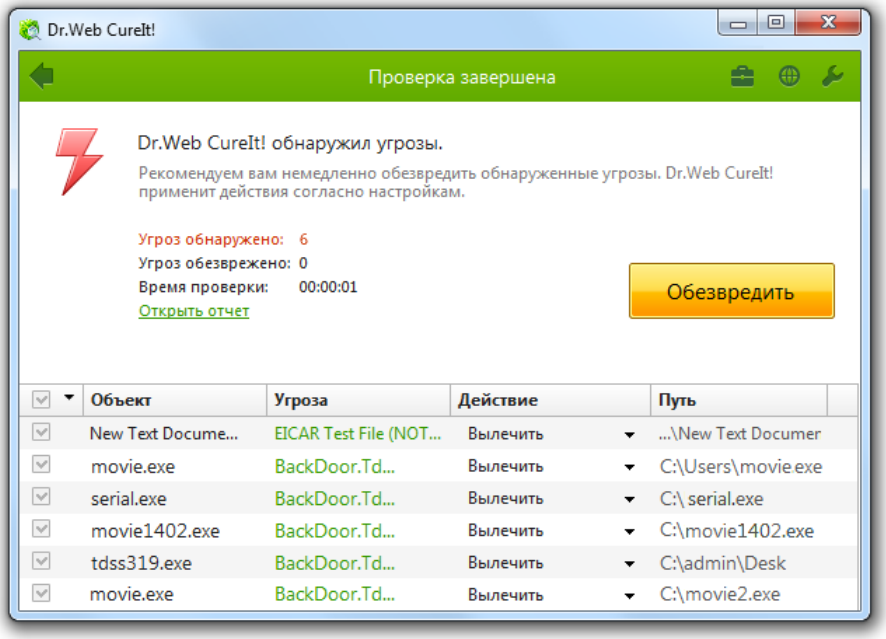


9. Если в ходе проверки были обнаружены вирусы или угрозы других типов, их необходимо нейтрализовать. Чтобы применить предустановленные действия, нажмите кнопку **Обезвредить**. При необходимости вы можете настроить разные действия для конкретных угроз.

Настройка обезвреживания угроз

По окончании проверки **Dr.Web CureIt!** лишь информирует об обнаруженных угрозах и предлагает применить к ним наиболее оптимальные действия по обезвреживанию. Вы можете обезвредить все обнаруженные угрозы одновременно. Для этого после завершения проверки нажмите кнопку **Обезвредить**, и **Dr.Web CureIt!** применит оптимальные действия по умолчанию для всех обнаруженных угроз.

По нажатию кнопки **Обезвредить** действия применяются к выбранным объектам в таблице. По умолчанию после окончания проверки для обезвреживания выбраны все объекты. При необходимости вы можете вручную выбрать конкретные объекты или группы объектов, для которых требуется применить действия по нажатию кнопки **Обезвредить**. Для этого используйте флажки рядом с названиями объектов или выпадающее меню в заголовке таблицы.



Вы также можете применить действие для каждой угрозы по отдельности. Вы можете восстановить функциональность зараженного объекта (*вылечить* его), а при невозможности – устранить исходящую от него угрозу (*удалить* объект).

Выбор действия

1. В поле **Действие** в выпадающем списке выберите необходимое действие для каждого объекта (по умолчанию **Dr.Web CureIt!** предлагает оптимальное значение).
2. Нажмите кнопку **Обезвредить**. **Dr.Web CureIt!** одновременно применит выбранные действия ко всем угрозам.

Подозрительные файлы, перемещенные в карантин, рекомендуется передавать для дальнейшего анализа в антивирусную лабораторию **«Доктор Веб»**.

Существуют следующие ограничения:

- лечение подозрительных объектов невозможно;
- невозможно перемещение или удаление объектов, не являющихся файлами (например, загрузочных секторов);

- любые действия для отдельных файлов внутри архивов, контейнеров или в составе писем невозможны – действие в таких случаях применяется только ко всему объекту целиком.

Подробный отчет о работе **Dr.Web CureIt!** сохраняется в виде файла CureIt.log в каталоге %USERPROFILE%\Doctor Web.

Настройка проверки

Настройки по умолчанию являются оптимальными для большинства применений **Dr.Web CureIt!**, их не следует изменять без необходимости.

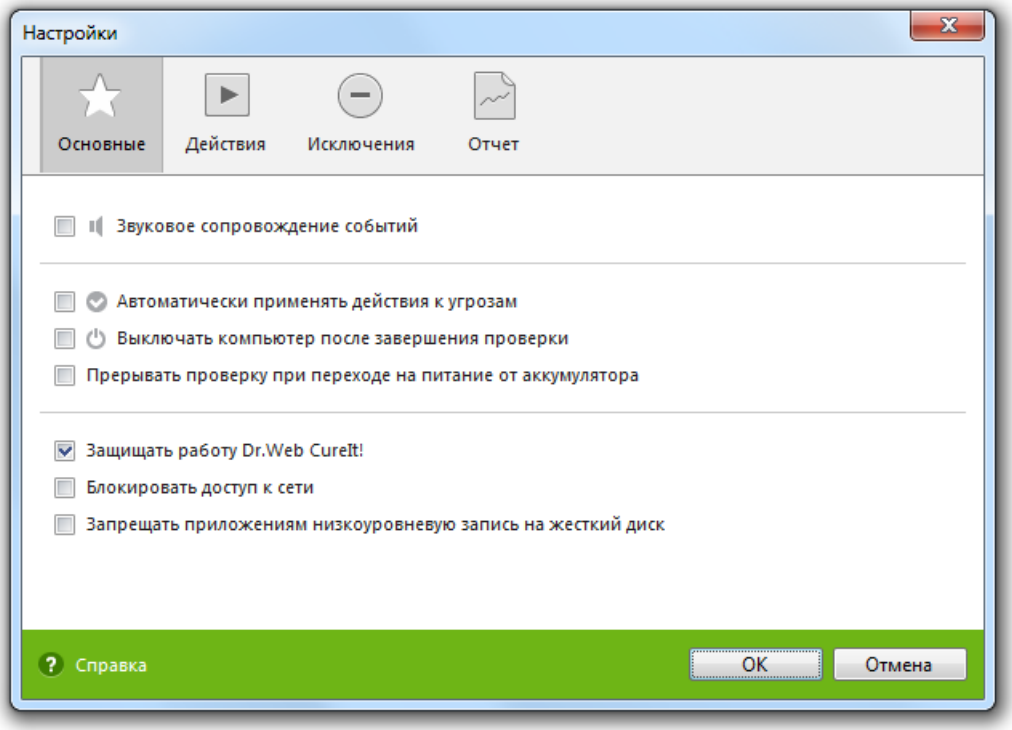
Изменение настроек Dr.Web CureIt!

1. Если **Dr.Web CureIt!** не запущен, запустите его. Откроется главное окно **Dr.Web CureIt!**.
2. На панели инструментов щелкните по иконке **Параметры проверки** и выберите пункт **Настройки.** Откроется окно настроек, содержащее следующие разделы:
   - раздел Основные, в котором задаются общие параметры работы **Dr.Web CureIt!**;
   - раздел Действия, в котором задается реакция **Dr.Web CureIt!** на обнаружение зараженных или подозрительных файлов и вредоносных программ;
   - раздел Исключения, в котором задаются дополнительные ограничения на состав файлов, подлежащих проверке;
   - раздел Отчет, в котором задается режим ведения файла отчета **Dr.Web CureIt!**.
3. Чтобы получить информацию о настройках, нажмите кнопку **Справка**.
4. По окончании редактирования настроек нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

Изменение настроек имеет силу только в данном сеансе работы **Dr.Web CureIt!**. При повторном запуске утилиты все настройки автоматически возвращаются к первоначальным значениям.

Раздел Основные

На этой вкладке задаются основные параметры работы **Dr.Web CureIt!**.



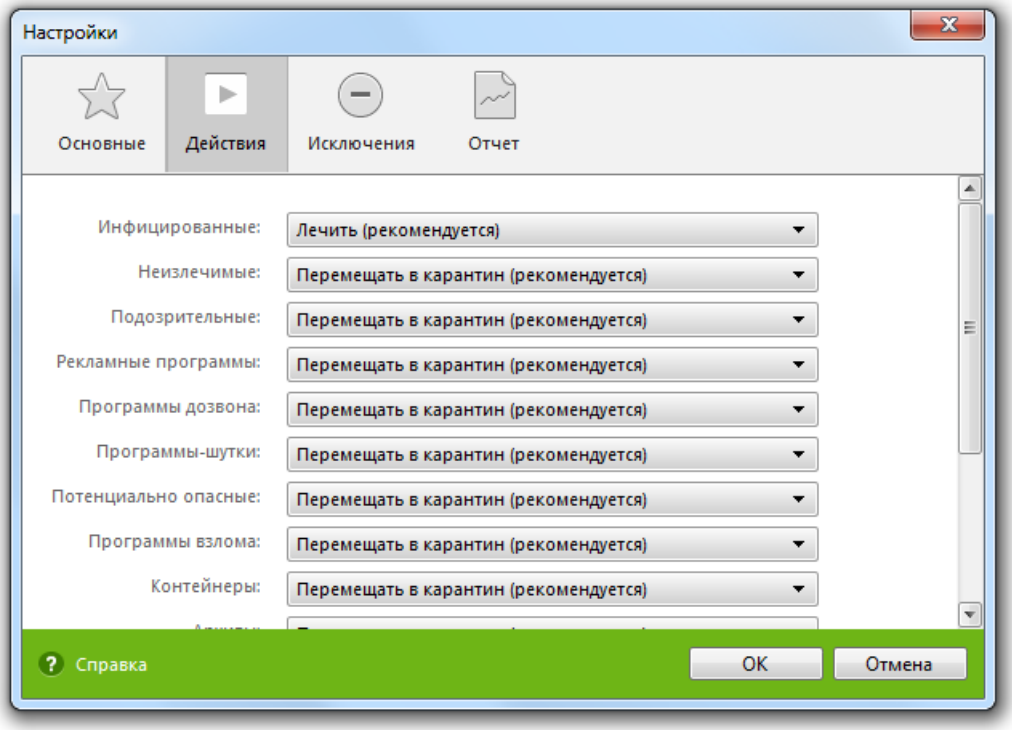
Вы можете включить звуковое сопровождение событий, а также указать **Dr.Web CureIt!** автоматически применять действия к угрозам и настроить взаимодействие программы с операционной системой.

В данном разделе вы также можете настроить параметры самозащиты, а также запретить некоторые действия, которые могут привести к заражению вашего компьютера.

Рекомендуется запускать **Dr.Web CureIt!** от имени пользователя, обладающего правами администратора. В противном случае те файлы и папки, к которым непривилегированный пользователь не имеет доступа (в том числе и системные папки), не будут подвергнуты проверке.

Раздел Действия

По окончании проверки **Dr.Web CureIt!** лишь информирует об обнаруженных угрозах и предлагает применить к ним наиболее оптимальные действия по обезвреживанию. Данные действия выбираются автоматически в соответствии с настройками на данной вкладке.



Оптимальной реакцией на обнаружение излечимых угроз (например, зараженных вирусами файлов) является лечение, в ходе которого восстанавливается исходного состояния объекта до заражения. Угрозы других типов рекомендуется перемещать в карантин, что позволяет предотвратить случайную потерю ценных данных. Вы можете выбрать следующие реакции:

Действие	Описание
Лечить	Восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, будет отработана реакция, заданная для неизлечимых объектов. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов(архивов, файлов электронной почты или файловых контейнеров). Троянские программы при обнаружении удаляются. Это единственное действие, доступное для зараженных загрузочных секторов.
Перемещать в карантин	Переместить объект в специальную папку для изоляции. По умолчанию карантин расположен в скрытой папке %USERPROFILE%\Doctor Web\DrWeb CureIt Quarantine\ и становится доступен после окончания проверки. Для загрузочных секторов никаких действий производиться не будет.
Удалять	Полностью удалить объект из системы. Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Пропустить объект без выполнения каких-либо действий и не выводить информацию в отчете. Данное действие возможно только для вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

При обнаружении вирусов или подозрительного кода внутри составных объектов(архивы, файлы электронной почты, файловые контейнеры) действия по отношению к угрозам внутри таких объектов выполняются над всем объектом, а не только над зараженной его частью. По умолчанию во всех этих случаях предусмотрено перемещение объекта в карантин.

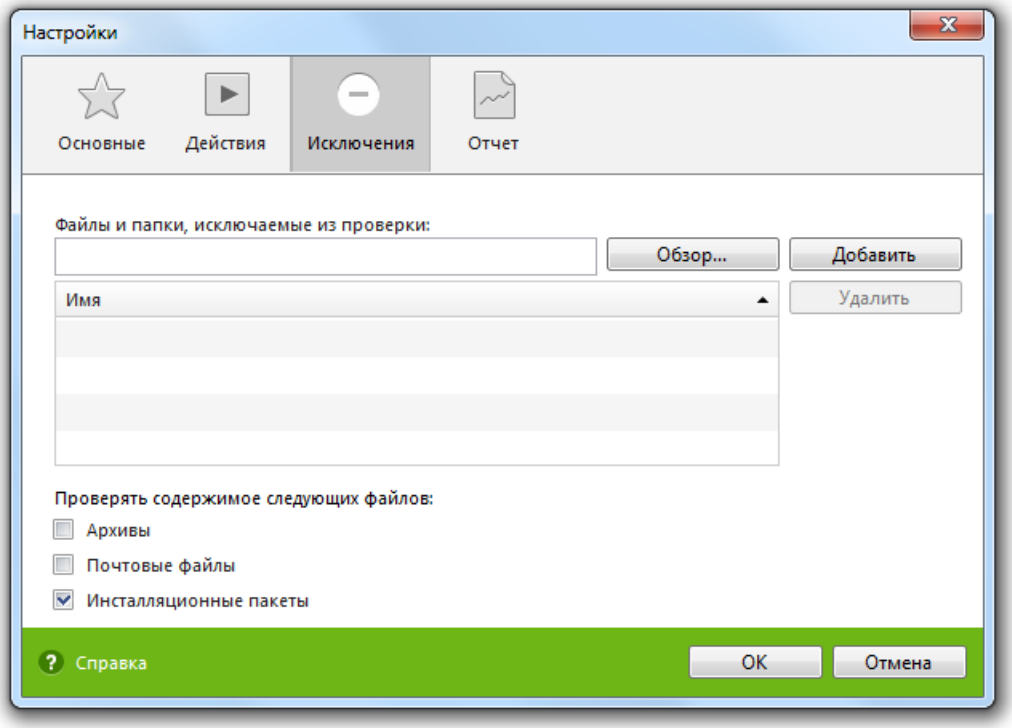
Для успешного завершения лечения некоторых зараженных (инфицированных) файлов требуется перезагрузка операционной системы. Вы можете выбрать один из вариантов:

- **Предлагать перезагрузку**;
- **Перезагружать компьютер автоматически**. Этот режим может привести к потере несохраненных данных.

Раздел Исключения

На этой вкладке задается дополнительное ограничение на состав файлов, которые должны быть подвергнуты проверке в соответствии с заданием на сканирование, а также указывается, требуется ли проводить проверку содержимого архивов, почтовых файлов и инсталляционных пакетов.

Лицензионное соглашение бесплатной версии **Dr.Web CureIt!** не предоставляет возможности проверять почтовые файлы, данный вид проверки доступен только в коммерческой версии утилиты и других продуктах семейства **Dr.Web**.



Список исключаемых файлов

Здесь можно задать список файлов (масок файлов), которые не будут сканироваться (из проверки будут исключены все файлы с данным именем.) В таком качестве могут выступать временные файлы (файлы подкачки) и т. п.

Задание списка исключаемых файлов

Чтобы задать список, выполните одно из следующих действий:

- введите имя (маску) файла, который должен быть исключен из проверки. Если вводится имя существующего файла, можно воспользоваться кнопкой **Обзор** и выбрать объект в стандартном окне открытия файла. Также вы можете использовать ‣маски;

Маска задает общую часть имени объекта при этом:

- символ «*» заменяет любую, возможно пустую последовательность символов;
- символ «?» заменяет любой, но только один символ;
- остальные символы маски ничего не заменяют и означают, что на этом месте в имени должен находиться именно этот символ.

Примеры:

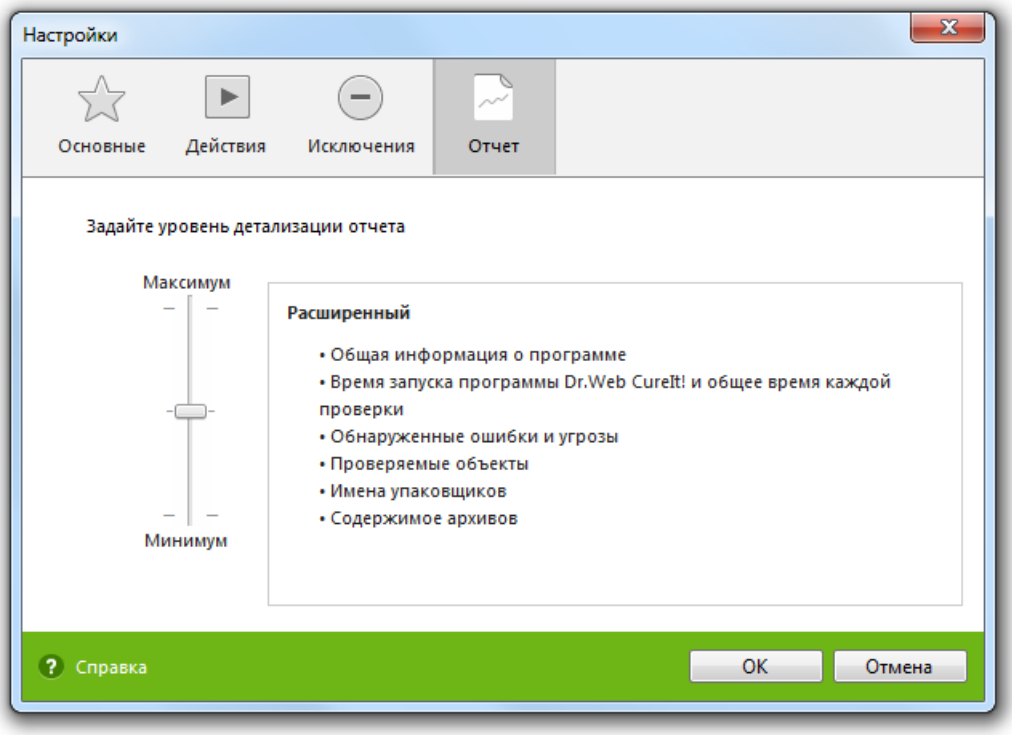
- **отчет*.doc** – маска, задающая все документы Microsoft Word, название которых начинается с подстроки «отчет», например, файлы отчет-февраль.doc, отчет121209.doc и т.д.;
- ***.exe** – маска, задающая все исполняемые файлы с расширением EXE, например, setup.exe, iTunes.exe и т.д.;
- **photo????09.jpg** – маска, задающая все файлы изображений формата JPG, название которых начинается с подстроки «photo» и заканчивается подстрокой «09», при этом между двумя этими подстроками в названии файла стоит ровно четыре произвольных символа, например, photo121209.jpg, photomama09.jpg или photo----09.jpg.

- нажмите кнопку **Добавить**, расположенную справа. Файл (маска файла) будет добавлен в список, расположенный ниже;
- для того чтобы удалить какой-либо объект из списка, выберите его в списке и нажмите кнопку **Удалить**. Файл будет допущен к последующей проверке.

Раздел Отчет

В этом разделе задается режим ведения файла отчета.

Отчет **Dr.Web CureIt!** хранится в файле CureIt.log, расположенном в каталоге %USERPROFILE%\Doctor Web. Рекомендуется периодически анализировать файл отчета.



Вы можете задать одну из следующих степеней детальности ведения отчета:

- **Стандартный** – в данном режиме в отчете фиксируются только наиболее значимые события, такие как запуск и остановка **Dr.Web CureIt!** и обнаруженные угрозы;
- **Расширенный** – в данном режиме в отчете помимо общих событий фиксируются данные о именах упаковщиков и содержимом проверяемых архивов. При необходимости вы можете добавить такие объекты в список исключений, что может снизить нагрузку на компьютер. Данный режим ведения отчета установлен по умолчанию для **Dr.Web CureIt!**;
- **Отладочный** – в данном режиме в отчете фиксируется максимальное количество информации о работе **Dr.Web CureIt!**, что может привести к значительному увеличению файла отчета. Рекомендуется использовать этот режим только при возникновении проблем в работе **Dr.Web CureIt!** или по просьбе технической поддержки компании **«Доктор Веб»**.

Запуск из командной строки

Вы можете запускать **Dr.Web CureIt!** в режиме командной строки. Такой способ позволяет задать дополнительные настройки текущего сеанса сканирования и перечень проверяемых объектов в качестве параметров вызова.

Синтаксис команды запуска следующий:
[<*путь_к_программе*>][*имя_CureIt!-файла*] [<*объекты*>] [<*ключи*>]

Список объектов сканирования может быть пуст или содержать несколько элементов, разделенных пробелами. Если путь к объектам сканирования не указан, поиск осуществляется в папке, где расположен файл **Сканера Dr.Web** (обычно – временная папка, куда распаковывается **Dr.Web CureIt!**).

Наиболее распространены следующие варианты указания объектов сканирования:

- **/LITE** – произвести стартовую проверку системы, при которой проверяются оперативная память и загрузочные секторы всех дисков, а также провести проверку на наличие руткитов.
- **/FAST** – произвести быструю проверку системы.
- **/FULL** – произвести полную проверку всех жестких дисков и сменных носителей (включая загрузочные секторы).

Параметры – ключи командной строки, которые задают настройки программы. При их отсутствии сканирование выполняется с ранее сохраненными настройками (или настройками по умолчанию, если вы не меняли их). Ключи начинаются с символа «/» и, как и остальные параметры командной строки, разделяются пробелами. Ключи начинаются с символа «/» и, как и остальные параметры командной строки, разделяются пробелами. Параметры, включающие пробелы, необходимо заключать в кавычки. Например:

- 636frs47.exe /tm-
- 45hlke49.exe /tm- D:\test\
- 10sfr56g.exe /OK- "D:\Program Files\"

Наиболее распространенные варианты указания объектов сканирования:

- * сканировать все жесткие диски;
- C: – сканировать диск C;
- D:\games – сканировать файлы в каталоге;
- C:\games* – сканировать все файлы и подкаталоги каталога C:\games.

Ключи командной строки

/AA – автоматически применять действия к обнаруженным угрозам.

/AR – проверять архивы. По умолчанию опция отключена.

Для включения архивов в проверку необходимо явно указать ключ **/AR**.

Если вы запускаете проверку из графического интерфейса, то для включения архивов в проверку необходимо установить флажок **Архивы** в разделе Исключения настроек **Dr.Web CureIt!**.

/AC – проверять инсталляционные пакеты. По умолчанию опция отключена.

Для включения инсталляционных пакетов в проверку необходимо явно указать ключ **/AC**.

Если вы запускаете проверку из графического интерфейса, то для включения архивов в проверку необходимо установить флажок **Инсталляционные пакеты** в разделе Исключения настроек **Dr.Web CureIt!**.

/AFS – использовать прямой слеш при указании вложенности внутри архива. По умолчанию опция отключена.

/ARC:*<число>* – максимальный уровень сжатия. Если сканер определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка не производится. По умолчанию – без ограничений.

/ARL:*<число>* – максимальный уровень вложенности проверяемого архива. По умолчанию – без ограничений.

/ARS:*<число>* – максимальный размер проверяемого архива, в килобайтах. По умолчанию – без ограничений.

/ART:*<число>* – порог проверки уровня сжатия (минимальный размер файла внутри архива, начиная с которого будет производиться проверка коэффициента сжатия), в килобайтах. По умолчанию – без ограничений.

/ARX:*<число>* – максимальный размер проверяемых объектов в архивах, в килобайтах. По умолчанию – без ограничений.

/BI – вывести информацию о **вирусных базах Dr.Web**. По умолчанию опция включена.

/DR – рекурсивно сканировать директории (проверять поддиректории). По умолчанию опция включена.

/E:*<число>* – использовать указанное количество движков.

/FAST – произвести быструю проверку системы.

/FL:*<имя_файла>* – сканировать пути, указанные в файле.

/FM:*<маска>* – сканировать файлы по маске. По умолчанию сканируются все файлы.

/FR:*<регулярное_выражение>* – сканировать файлы по регулярному выражению. По умолчанию сканируются все файлы.

/FULL – произвести полную проверку всех жестких дисков и сменных носителей (включая загрузочные секторы).

/HA – производить эвристический анализ файлов и поиск в них неизвестных угроз. По умолчанию опция включена.

/LITE – произвести стартовую проверку системы, при которой сканируются оперативная память и загрузочные секторы всех дисков, а также проводится поиск руткитов. Использование этого ключа отменяет режимы **/FAST** и **/FULL**.

/LN – сканировать файлы, на которые указывают ярлыки. По умолчанию опция отключена.

/MA – проверять почтовые файлы. По умолчанию опция включена.

/MC:<*число*> – установить максимальное число попыток вылечить файл. По умолчанию – без ограничений.

/NB – не создавать резервные копии вылеченных или удаленных файлов. По умолчанию опция отключена.

/NI[:X] – уровень использования ресурсов системы, в процентах. Определяет количество памяти используемой для сканирования и системный приоритет задачи сканирования. По умолчанию – без ограничений.

/NOREBOOT – отменяет перезагрузку и выключение после сканирования.

/NT – сканировать NTFS-потоки. По умолчанию опция включена.

/OK – выводить полный список сканируемых объектов, сопровождая незараженные пометкой **Ok**. По умолчанию опция отключена.

/P:<*приоритет*> – приоритет запущенной задачи сканирования в общей очереди задач на сканирование:

0 – низший.

L – низкий.

N – обычный. Приоритет по умолчанию.

H – высший.

M – максимальный.

/PAL:<*число*> – уровень вложенности упаковщиков. По умолчанию – 1000.

/RA:<*имя файла*> – дописать отчет о работе программы в указанный файл. По умолчанию – отчет не создается.

/RP:<*имя файла*> – записать отчет о работе программы в указанный файл. По умолчанию – отчет не создается.

/QNA – выводить пути в двойных кавычках.

/QUIT – закрыть **Dr.Web CureIt!** после проверки (вне зависимости от того, были ли применены действия к обнаруженным угрозам).

/REP – сканировать по символьным ссылкам. По умолчанию опция отключена.

/SCC – выводить содержимое составных объектов(архивы, файлы электронной почты или файловые контейнеры). По умолчанию опция отключена.

/SCN – выводить название инсталляционного пакета. По умолчанию опция отключена.

/SPN – выводить название упаковщика. По умолчанию опция отключена.

/SST – выводить время сканирования файла. По умолчанию опция отключена.

/TB – выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска. По умолчанию опция отключена.

/TM – выполнять поиск вирусов в оперативной памяти (включая системную область Windows). По умолчанию опция отключена.

/TR – сканировать системные точки восстановления. По умолчанию опция отключена.

/W:<*число*> – максимальное время сканирования, в секундах. По умолчанию – без ограничений.

/X:S[:R] – по окончании сканирования перевести машину в указанный режим: выключение/ перезагрузка/ждущий режим/спящий режим.

Задание действий с различными объектами (C – вылечить, Q – переместить в карантин, D – удалить, I – игнорировать):

- **/AAD:**<*действие*> – действия для рекламных программ (возможные действия: DQI)
- **/AAR:**<*действие*> – действия с инфицированными архивами (возможные действия: DQI)
- **/ACN:**<*действие*> – действия с инфицированными инсталляционными пакетами (возможные действия: DQI)
- **/ADL:**<*действие*> – действия с программами дозвона (возможные действия: DQI)
- **/AHT:**<*действие*> – действия с программами взлома (возможные действия: DQI)
- **/AIC:**<*действие*> – действия с неизлечимыми файлами (возможные действия: DQ)
- **/AIN:**<*действие*> – действия с инфицированными файлами (возможные действия: CDQ)
- **/AJK:**<*действие*> – действия с программами-шутками (возможные действия: DQI)
- **/AML:**<*действие*> – действия с инфицированными почтовыми файлами (возможные действия: QI)
- **/ARW:**<*действие*> – действия с потенциально опасными файлами (возможные действия: DQI)
- **/ASU:**<*действие*> – действия с подозрительными файлами (возможные действия: DQI)

Модификаторы параметров

Некоторые ключи могут иметь модификаторы, с помощью которых режим явно включается либо отключается. Например:

/AC- режим явно отключается,
/AC, **/AC+** режим явно включается.

Такая возможность может быть полезна в случае, если режим включен/отключен по умолчанию. Список ключей, допускающих применение модификаторов: **/AR**, **/AC**, **/AFS**, **/BI**, **/DR**, **/HA**, **/LN**, **/MA**, **/NB**, **/NT**, **/OK**, **/QNA**, **/REP**, **/SCC**, **/SCN**, **/SPN**, **/SST**, **/TB**, **/TM**, **/TR**.

Для ключа **/FL** модификатор «-» означает: проверить пути, перечисленные в указанном файле, и удалить этот файл.

Для ключей **/ARC**, **/ARL**, **/ARS**, **/ART**, **/ARX**, **/NI[:X]**, **/PAL**, **/W**, принимающих в качестве значения параметра <*число*>, «0» означает, что параметр используется без ограничений.

Если в командной строке встречаются несколько взаимоисключающих ключей, то действует последний из них.

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, настоятельно рекомендуется попробовать найти решение одним из следующих способов:

- Ознакомиться с последними версиями описаний и руководств по адресу http://download.drweb.com/doc
- 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.