Dr.WEB

CureIt!

Руководство пользователя

Dr.Web CureIt!
Руководство пользователя
23.09.2021

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «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

1. Условные обозначения

В данном руководстве используются следующие условные обозначения:

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

2. О продукте

Dr.Web CureIt! — 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.

Вы можете использовать Dr.Web CureIt! бесплатно для проверки персонального компьютера. Для коммерческого использования Dr.Web CureIt! требуется лицензия. Подробную информацию о лицензии и покупке программы вы можете получить на официальном сайте проекта Dr.Web CureIt!.

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 Windows® (начиная с Microsoft Windows XP и заканчивая Microsoft Windows 11) и Windows Server® и постоянно обновляется и дополняется актуальными 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 серверы компании «Доктор Веб» общую информацию о проверяемом компьютере и состоянии информационной безопасности на нем. При использовании платной версии Dr.Web CureIt! вы можете отказаться от передачи статистики.

Для использовании бесплатной версии Dr.Web CureIt! требуются административные привилегии и доступ к интернету.

2.1. 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 более поздними; • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7 с пакетом обновлений SP1 или более поздними; • Windows 8; • Windows 8.1; • Windows 10; • Windows Server 2003 с пакетом обновлений SP1; • Windows Server 2008 с пакетом обновлений SP2 или более поздними. Для 64-разрядных операционных систем: • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7 с пакетом обновлений SP1 или более поздними; • Windows 8; • Windows 8.1; • Windows 10; • Windows 11; • Windows Server 2008 с пакетом обновлений SP2 или более поздними; • Windows Server 2008 R2 с пакетом обновлений SP1 или более поздними; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019.
Место на жестком диске	160 МБ свободного дискового пространства.

Компонент	Требование
Свободная оперативная память	Не менее 360 МБ.
Процессор	С поддержкой системы команд i686 и набором инструкций SSE2.

Поскольку компания Microsoft прекратила поддержку алгоритма хеширования SHA-1, перед установкой программы Dr.Web CureIt! на Windows Vista или Windows 7, Windows Server 2008 или Windows Server 2008 R2 убедитесь, что система поддерживает алгоритм хеширования SHA-256. Для этого установите все рекомендуемые обновления из Центра обновления Windows. Подробную информацию о необходимых пакетах обновлений вы можете найти на официальном сайте компании «Доктор Веб».

2.2. Проверка антивируса

Вы можете проверить работоспособность Dr.Web CureIt! с помощью тестового файла EICAR — European Institute for Computer Anti-Virus Research.

Для этого вы можете использовать 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 вредоносна, 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 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».

2.3. Методы обнаружения угроз

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

Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он выполняется путем проверки содержимого анализируемого объекта на предмет наличия в нем сигнатур уже известных угроз. *Сигнатурой* называется непрерывная конечная последовательность байтов, 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 применяется 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 кода. 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 программ 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.

2.4. Отправка статистики

Чтобы получить данные о вирусной обстановке в мире и на основе этих данных улучшать механизмы проверки и обезвреживания угроз, Dr.Web CureIt! передает обезличенную статистику 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 https://company.drweb.com/policy.

3. Начало работы

Dr.Web CureIt! проверяет загрузочные секторы, память, а также отдельные файлы и файлы в составных объектах (архивах, файлах электронной почты или файловых контейнерах). При проверке используются все методы обнаружения угроз.

Лицензионное соглашение бесплатной версии Dr.Web CureIt! не позволяет проверять почтовые файлы.

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 применить действия по умолчанию ко всем обнаруженным угрозам или выбрать необходимые действия для отдельных объектов.

Действия по умолчанию оптимальны для большинства применений, но при необходимости вы можете изменить их в настройках 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.

В ходе проверки Dr.Web CureIt! передает на серверы компании «Доктор Веб» общую информацию о проверяемом компьютере. При использовании платной версии Dr.Web CureIt! вы можете отказаться от передачи статистики.

Язык интерфейса

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

3.1. Обновление Dr.Web CureIt!

Dr.Web CureIt! не содержит 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 загрузить последнюю версию Dr.Web CureIt!, которая всегда доступна на официальном сайте проекта Dr.Web CureIt! и снабжена самыми последними вирусными базами и современным механизмом обнаружения вирусных угроз.

Чтобы загрузить последнюю версию Dr.Web CureIt!

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

   В окне интернет-браузера по умолчанию откроется официальный сайт проекта Dr.Web CureIt!, откуда вы сможете загрузить обновленную версию программы.

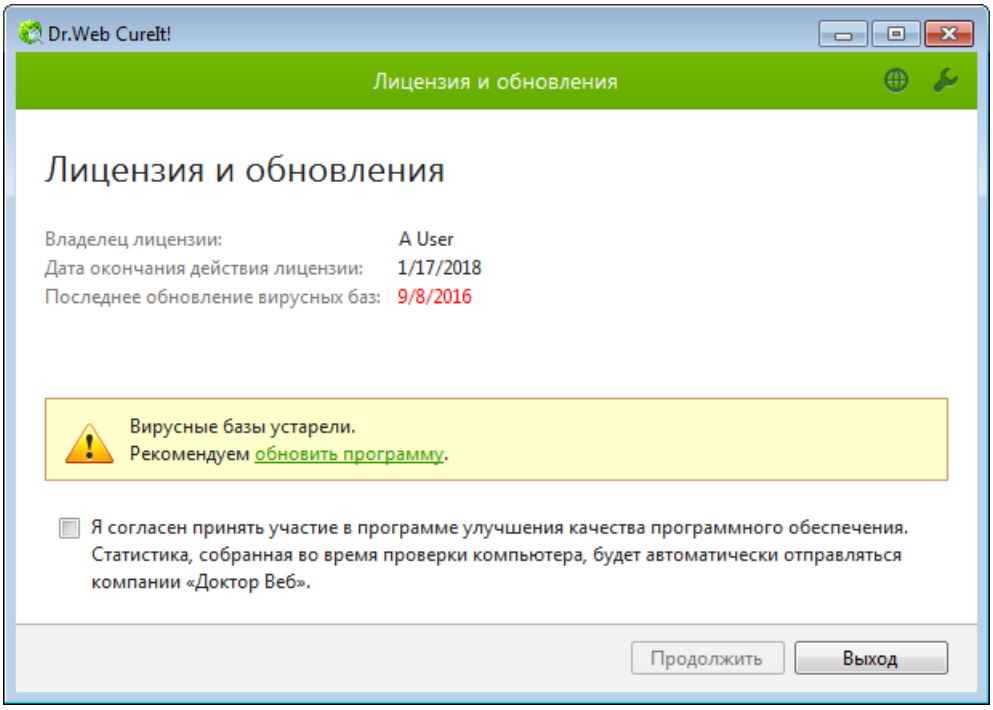

Рисунок 1. Обновление Dr.Web.

3.2. Быстрая проверка

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

В этом 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;

- руткиты.

При необходимости более гибкой настройки вы можете провести выборочную проверку.

Чтобы провести быструю проверку

1. Запустите Dr.Web CureIt!.
2. В первом окне **Лицензия и обновление** ознакомьтесь с условиями отправки статистики. Нажмите кнопку **Продолжить**.
3. В окне выбора типа проверки нажмите кнопку **Начать проверку**.

Рисунок 2. Выбор проверки Dr.Web.

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

   При необходимости вы можете выполнить следующее:

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

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

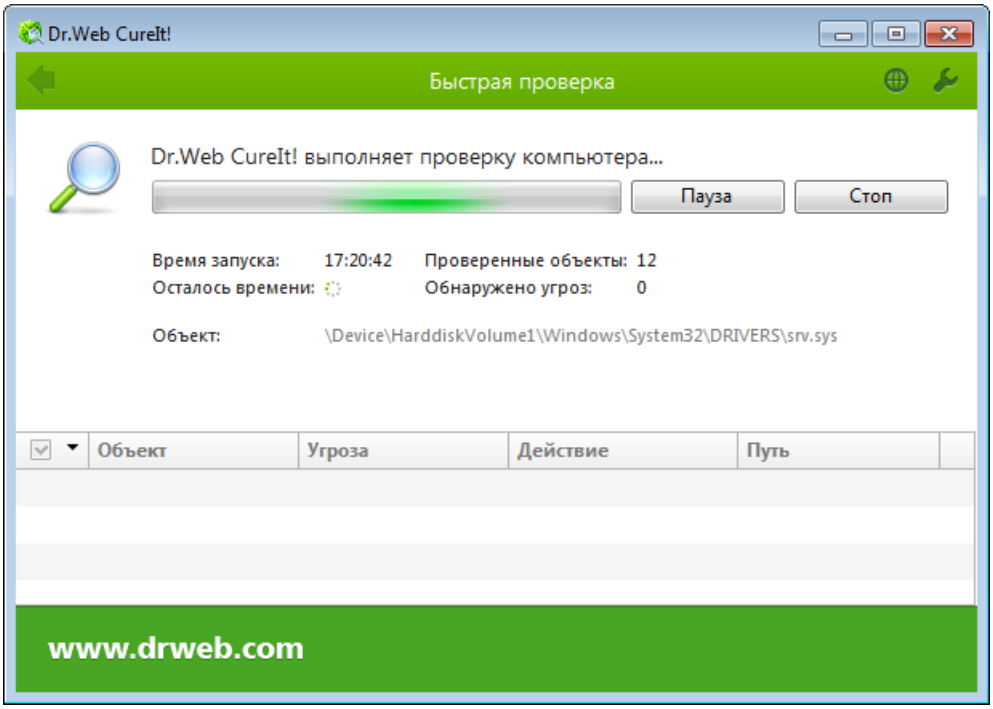

Рисунок 3. Быстрая проверка Dr.Web.

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**.

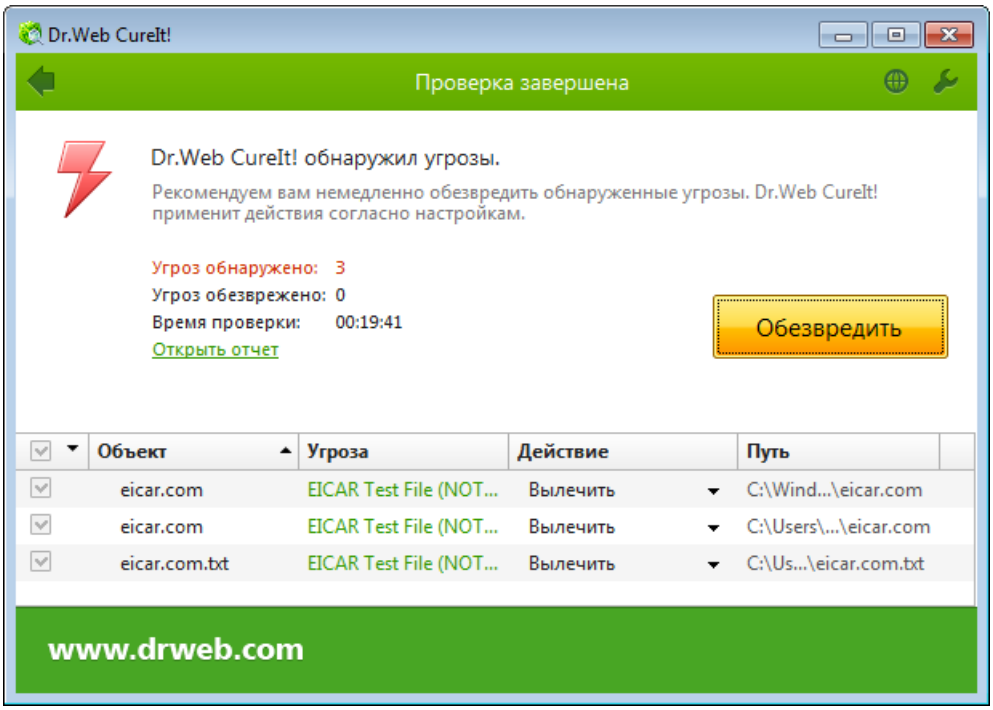

Рисунок 4. Результаты быстрой проверки Dr.Web.

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

3.3. Менеджер Карантина

В окне Менеджера Карантина отображаются данные о содержимом Карантина Dr.Web CureIt!. В Карантине хранятся подозрительные файлы и резервные копии файлов, обработанных Dr.Web CureIt!.

Каталог Карантина создается в каталоге `%USERPROFILE%\Doctor Web\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! нажмите значок **Параметры проверки** и выберите пункт **Менеджер Карантина**.

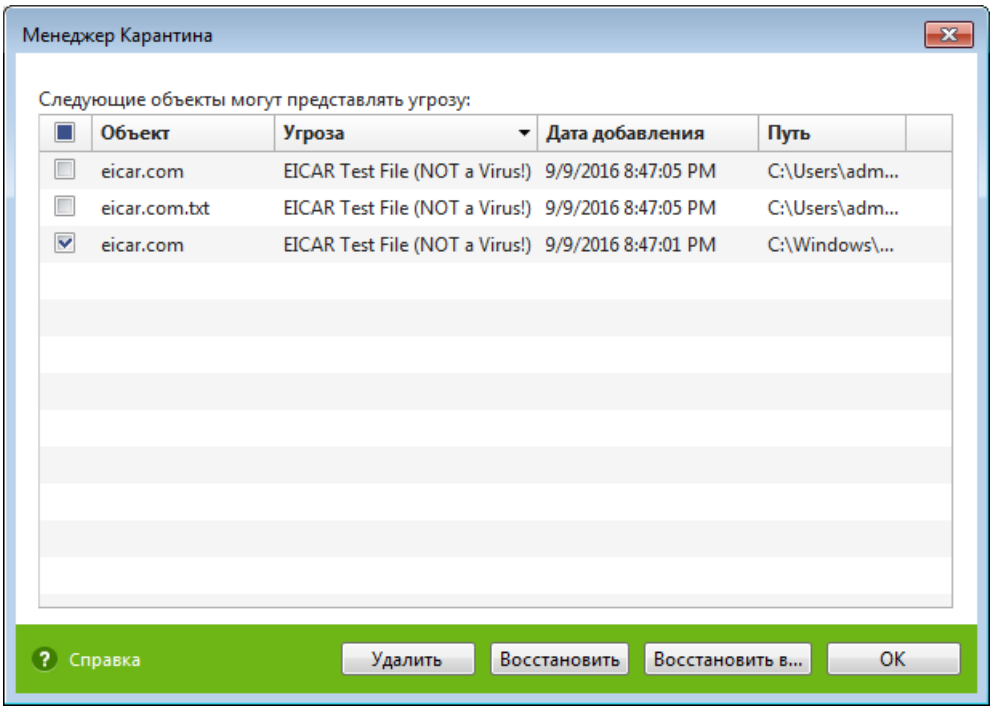

Рисунок 5. Менеджер карантина Dr.Web.

В центральной части окна отображается таблица с информацией о состоянии Карантина со следующими полями:

- **Объект** — имя объекта, находящегося 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.

Файлы в окне Карантина 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 эту 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.

4. Дополнительные возможности

В большинстве случаев чтобы обезвредить угрозы на компьютере, 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 командной строки.

4.1. Выборочная проверка

Кроме быстрой проверки наиболее уязвимых объектов операционной системы, в Dr.Web CureIt! предусмотрен гибкий пользовательский режим. С его помощью вы можете настроить проверку под свои нужды.

При выборе этого 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. Для начала проверки выбранных объектов нажмите кнопку **Запустить проверку**. В случае полной или быстрой проверки выбирать объекты не требуется.

Вы можете выбирать вид проверки при каждом запуске Dr.Web CureIt! на шаге **Выбор проверки**.

Рисунок 6. Выбор проверки Dr.Web.

Чтобы запустить выборочную проверку

1. Запустите Dr.Web CureIt!.
2. В первом окне **Лицензия и обновление** ознакомьтесь с условиями отправки статистики. 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, нажмите ссылку 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.

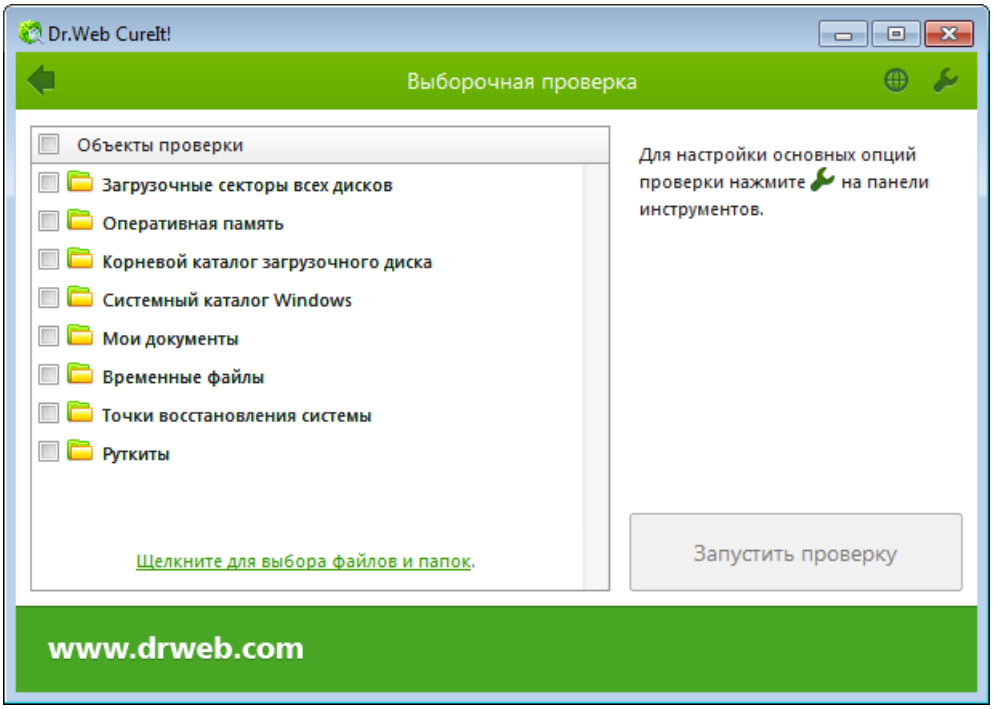

Рисунок 7. Выбор файлов для проверки Dr.Web.

При необходимости перед началом проверки настройте параметры работы Dr.Web CureIt!. Для этого на панели инструментов нажмите кнопку **Параметры проверки**.

5. Нажмите кнопку **Запустить проверку**.
6. 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.

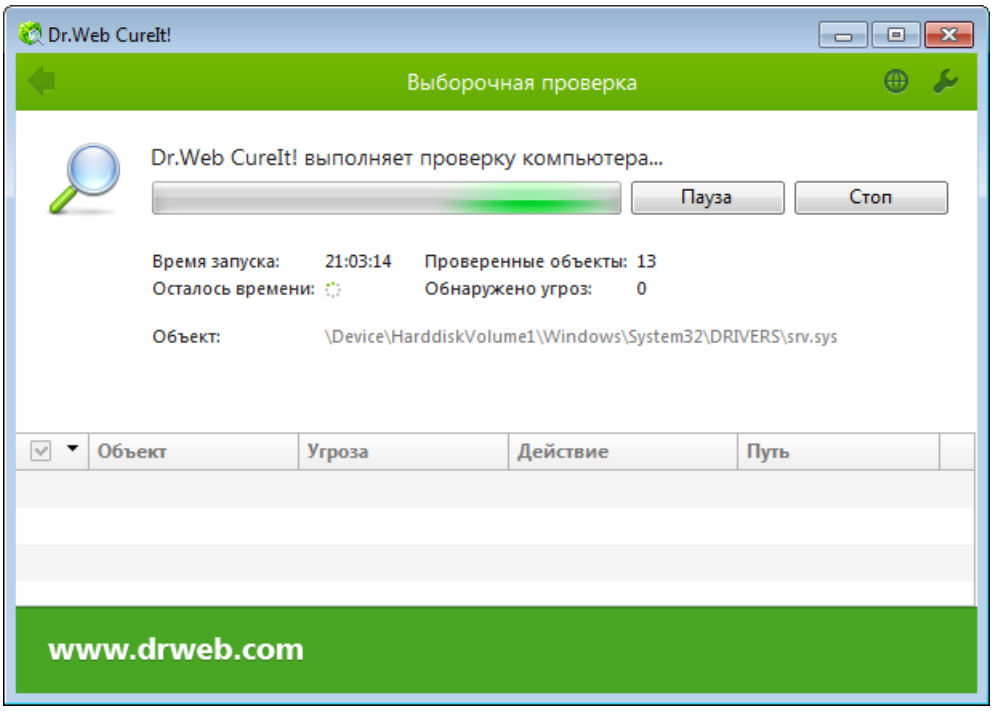

Рисунок 8. Выборочная проверка Dr.Web.

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**.

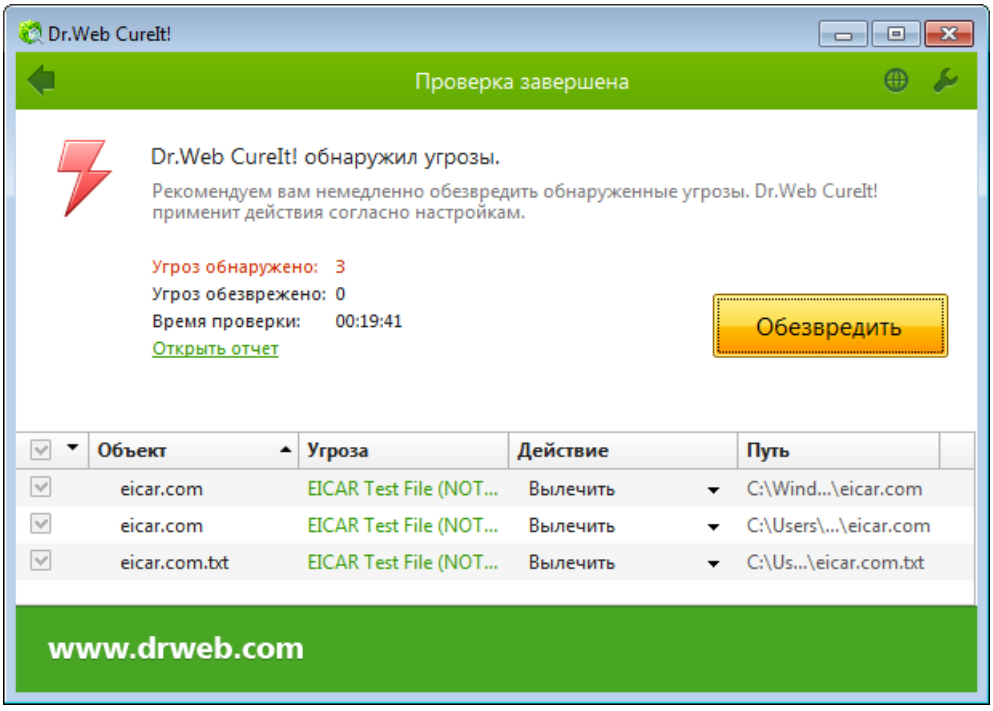

Рисунок 9. Результаты выборочной проверки Dr.Web.

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

4.2. 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, к которым по нажатию кнопки **Обезвредить** будут применены действия. Для этого используйте флажки рядом с названиями объектов или выпадающее меню в заголовке таблицы.

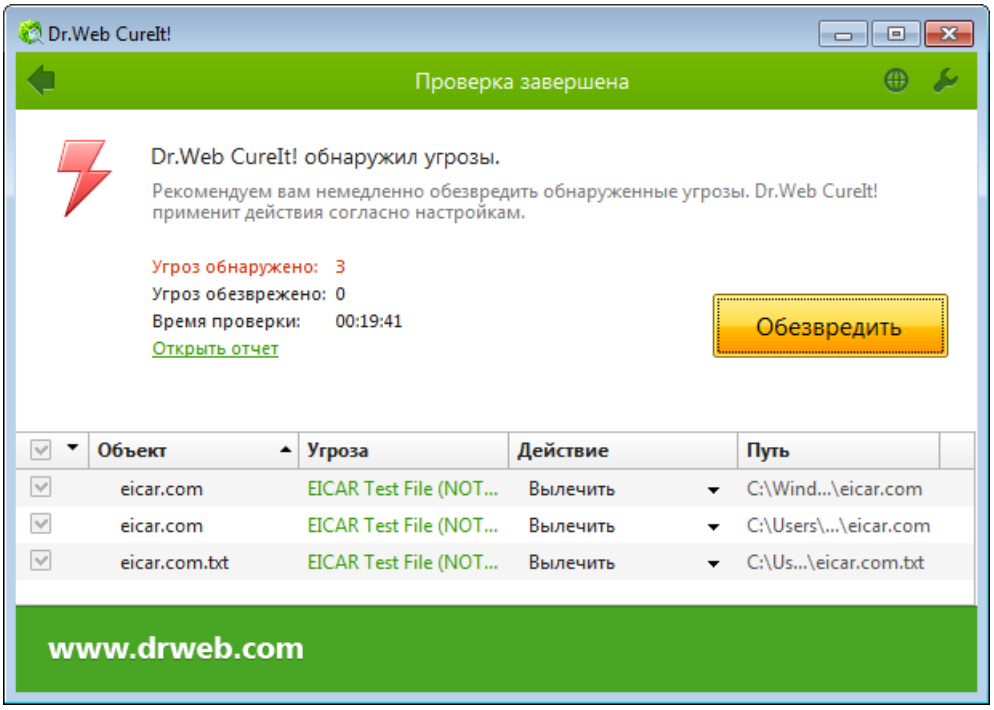

Рисунок 10. Выбор действия после проверки Dr.Web.

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).

Чтобы выбрать действие для угрозы

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`.

4.3. Настройка проверки

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

Чтобы изменить настройки Dr.Web CureIt!

1. Запустите Dr.Web CureIt!. Откроется главное окно Dr.Web CureIt!.
2. На панели инструментов нажмите значок **Параметры проверки** и выберите пункт **Настройки**. Откроется окно настроек со следующими вкладками:
   - Основные, в которой задаются общие параметры работы Dr.Web CureIt!.
   - Действия, в которой задается реакция Dr.Web CureIt! на обнаружение зараженных или подозрительных файлов и вредоносных программ.
   - Исключения, в которой задаются дополнительные ограничения на состав файлов, подлежащих проверке.
   - Отчет, в которой задается режим ведения файла отчета Dr.Web CureIt!.
3. Чтобы получить информацию о настройках, нажмите кнопку **Справка**.
4. По окончании редактирования настроек нажмите кнопку **OK** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

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

4.3.1. Вкладка Основные

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

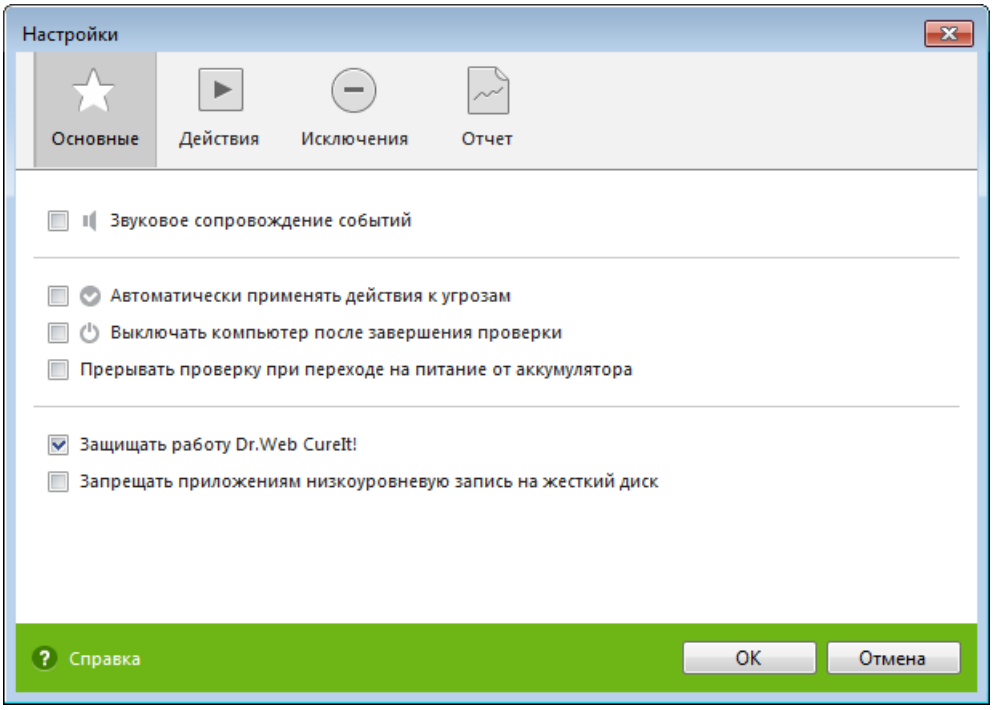

Рисунок 11. Настройка Dr.Web. Вкладка Основные.

Вы можете включить звуковое сопровождение событий, а также настроить автоматические действия к обнаруженным угрозам и взаимодействие программы с операционной системой.

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

4.3.2. Вкладка Действия

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

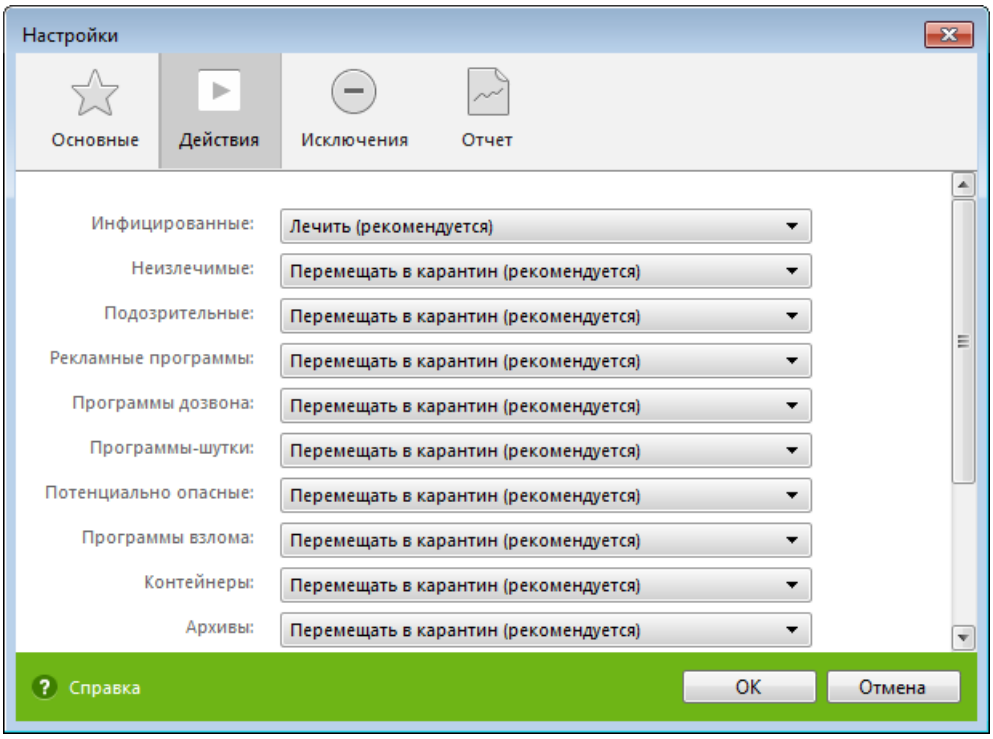

Рисунок 12. Настройка Dr.Web. Вкладка Действия.

Оптимальной реакцией на обнаружение излечимых угроз (например, зараженных вирусами файлов) является лечение, в ходе которого восстанавливается исходное состояние объекта, имевшееся до заражения. Угрозы других типов рекомендуется перемещать в карантин, таким образом вы предотвратите случайную потерю ценных данных.

Вы можете выбрать следующие реакции:

Действие	Описание
Лечить	Восстановить состояние объекта, имевшееся до заражения. Если вирус неизлечим или попытка лечения не была успешной, будет выполнено действие, заданное для неизлечимых объектов. Лечение 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. Лечение — это единственное действие, доступное для зараженных загрузочных секторов.

Действие	Описание
Перемещать в карантин	Переместить объект в специальную папку для временного хранения подозрительных объектов. По умолчанию карантин расположен в скрытой папке `%USERPROFILE%\Doctor Web\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. Это 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 (архивов, файлов электронной почты или файловых контейнеров) 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.

4.3.3. Вкладка Исключения

На этой вкладке вы можете задать дополнительное ограничение на состав файлов, которые будут проверяться в соответствии с заданием на проверку, а также указать, требуется ли проводить проверку содержимого архивов и инсталляционных пакетов.

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

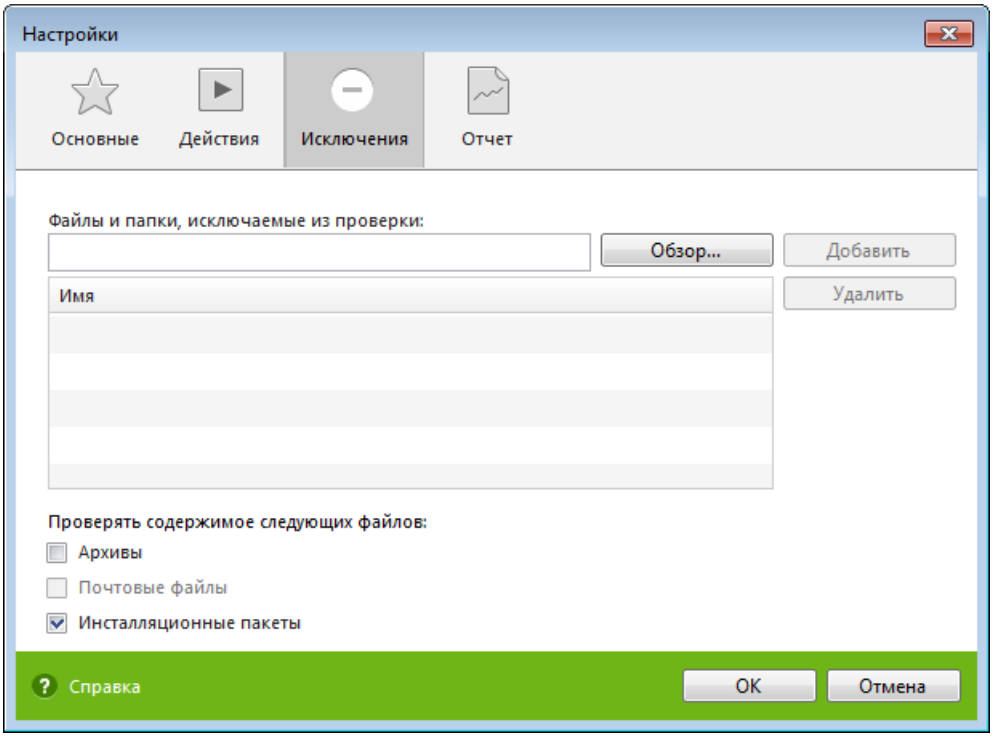

Рисунок 13. Настройка Dr.Web. Вкладка Исключения.

Список исключаемых файлов

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

Чтобы задать список исключаемых файлов

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:

  - 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.
- Чтобы удалить какой-либо объект из списка, выберите его в списке и нажмите кнопку **Удалить**. Файл будет допущен к последующей проверке.

4.3.4. Вкладка Отчет

На этой вкладке 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.

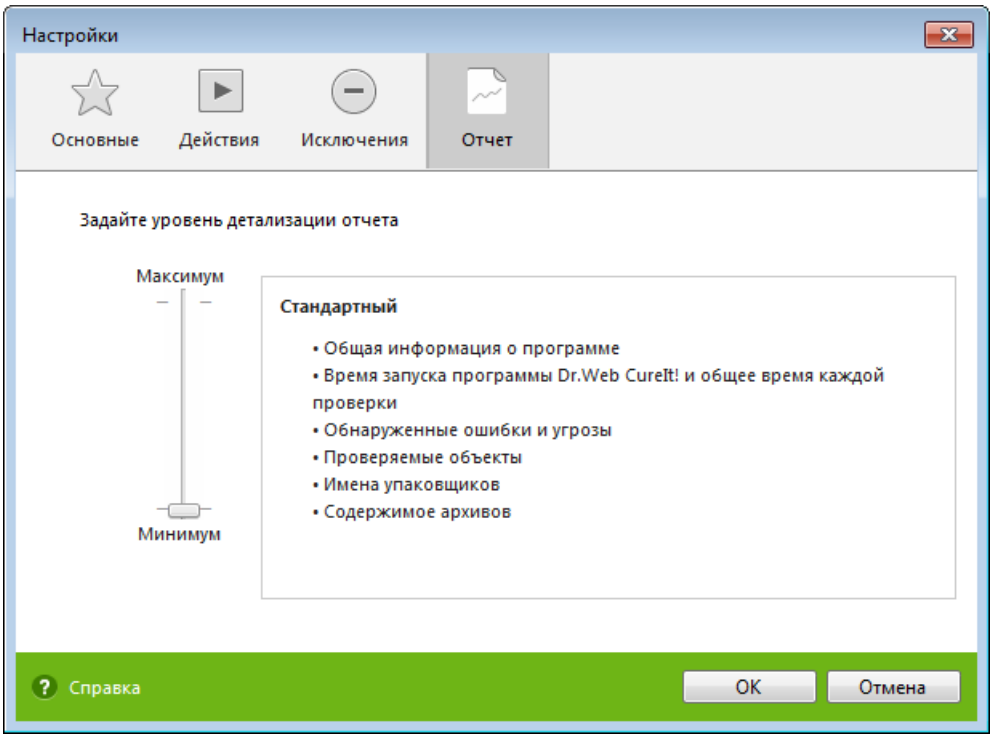

Рисунок 14. Настройка Dr.Web. Вкладка Отчет.

Вы можете задать одну из следующих степеней детальности ведения отчета:

- **Стандартный** — в этом режиме в отчете фиксируются только наиболее значимые события, такие как запуск и остановка Dr.Web CureIt! и обнаруженные угрозы;
- **Отладочный** — в этом 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».

4.4. Запуск из командной строки

Вы можете запускать Dr.Web CureIt! в режиме командной строки. Так вы можете задать дополнительные настройки текущего сеанса проверки и перечень проверяемых объектов в качестве параметров вызова.

Чтобы использовать интерфейс командной строки в бесплатной версии Dr.Web CureIt!, требуется подтвердить согласие на отправку анонимной статистики в компанию «Доктор Веб». При использовании платной версии Dr.Web CureIt! такое согласие не требуется.

Синтаксис команды запуска:

```
[<путь_к_программе>][<имя_CureIt!-файла>] [<объекты>] [<ключи>]
```

Список объектов на проверку может быть пуст или содержать несколько элементов, разделенных пробелами. Если путь к объектам не указан, поиск осуществляется в папке, где расположен файл Dr.Web CureIt!.

Наиболее распространенные варианты указания режимов проверки:

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

Ключи — параметры командной строки, которые задают настройки программы. При их отсутствии проверка выполняется с ранее сохраненными настройками (или настройками по умолчанию, если вы не меняли их). Ключи начинаются с символа / и разделяются пробелами, как и остальные параметры командной строки. 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 проверки:

- `*` — проверять все жесткие диски;
- `C:` — проверять диск `C`;
- `D:\games` — проверять файлы в каталоге;
- `C:\games\*` — проверять все файлы и подкаталоги каталога `C:\games`.

Ключи командной строки

Список всех ключей 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 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 инсталляционных пакетов в проверку необходимо установить флажок **Инсталляционные пакеты** в разделе Исключения 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. Если размер архива превышает максимальный, Dr.Web CureIt! не распакует и не проверит его. 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 проверять директории (проверять поддиректории). По умолчанию опция включена.

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

/FAST — провести быструю проверку системы.

/FL:<*имя_файла*> — проверить пути, указанные в файле.

/FM:<*маска*> — проверить файлы по маске. По умолчанию проверяются все файлы.

/FR:<*регулярное_выражение*> — проверять файлы по регулярному выражению. По умолчанию проверяются 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 проверяются оперативная память и загрузочные секторы всех дисков, а также проводится поиск руткитов. Использование этого ключа отменяет режимы **/FAST** и **/FULL**.

/LN — проверять файлы, на которые указывают ярлыки. По умолчанию опция отключена.

/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 проверки и системный приоритет задачи на проверку. По умолчанию — без ограничений.

/NOREBOOT — отменяет перезагрузку и выключение после проверки.

/NT — проверять NTFS-потоки. По умолчанию опция включена.

/OK — выводить полный список проверяемых объектов, сопровождая незараженные пометкой OK. По умолчанию опция отключена.

/P:<*приоритет*> — приоритет запущенной проверки в общей очереди задач на проверку:

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 — проверять по символьным ссылкам. По умолчанию опция отключена.

/SCC — выводить содержимое составных объектов (архивов, файлов электронной почты или файловых контейнеров). По умолчанию опция отключена.

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

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

/SST — выводить время проверки файла. По умолчанию опция отключена.

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

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

/TR — проверять системные точки восстановления. По умолчанию опция отключена.

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

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

Задание действий для различных угроз

Используйте следующие модификаторы, чтобы выбрать подходящее действие для каждого типа угроз (*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).

- **/ARW:**<*действие*> — действия с потенциально опасными файлами (возможные действия: DQI).
- **/ASU:**<*действие*> — действия с подозрительными файлами (возможные действия: DQI).

Модификаторы ключей

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

/AC- — режим явно отключается.

/AC или **/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**, **/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**, если в качестве модификатора <*число*> указано значение **0**, ключ используется без ограничений.

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