Dr.WEB

CureNet!

Руководство администратора

Dr.Web CureNet!
Версия 11.0.0
Руководство администратора
12.04.2024

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 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. Используемые 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. Dr.Web CureNet!

Dr.Web предназначен для проведения централизованной антивирусной проверки по сети удаленных компьютеров и серверов под управлением операционной системы Windows. Данный продукт не требует установки и выполняет проверку и лечение обнаруженных вредоносных объектов, даже если на проверяемых компьютерах (далее – станциях) установлены антивирусы других производителей. Скорость распространения и проверки станций, равно как и скорость сбора статистики не зависят от состояния связи. Проверку можно проводить даже в сетях, полностью изолированных от Интернета.

Dr.Web предоставляет вам следующие преимущества:

- централизованная проверка станций под управлением Windows в сети;
- централизованное управление реакцией на обнаружение угроз;
- лечение зараженных объектов;
- проверка почтовых файлов и файлов в архивах и контейнерах;
- регулярное обновление вирусных баз и компонентов антивируса;
- высокая скорость проверки;
- сбор статистики антивирусной проверки;
- сохранение отчета о проверке удаленных станций в формате CSV или XML.

2.1. Системные требования

Системные требования для компьютера администратора

Использование Dr.Web CureNet! возможно на компьютерах, удовлетворяющих следующим требованиям:

Компонент	Требование
Операционная система	• Windows XP Professional с пакетом обновлений SP2 или более поздним; • Windows Server 2003 с пакетом обновлений SP1 или более поздним; • Windows Vista (только редакции Business, Enterprise или Ultimate) с пакетом обновлений SP1 или более поздним; • Windows Server 2008; • Windows 7 (только редакции Профессиональная/Professional, Корпоративная/Enterprise или Максимальная/Ultimate); • Windows Server 2008 с пакетом обновлений SP2;

Компонент	Требование
	• Windows 8 и 8.1 (только редакции Профессиональная/Professional и Корпоративная/Enterprise); • Windows Server 2012; • Windows 10.
Место на жестком диске	200 МБ свободного дискового пространства.
Свободная оперативная память	Не менее 360 МБ.
Процессор	С поддержкой системы команд i686 и набором инструкций SSE2.
Прочее	Подключение к сети Интернет для обновления вирусных баз и компонентов Dr.Web. Подключение ко всем проверяемым станциям по протоколу TCP/IP.

Системные требования для станций

Системные требования для станций совпадают с требованиями для компьютера, на котором запускается Консоль администрирования, за исключением следующего:

- **Операционная система:** Windows XP Professional SP2 и более поздние версии, кроме следующих версий для 64-разрядных систем: Windows Server 2003 x64 Edition и Windows XP Professional SP2 x64 Edition.
- **Прочее:** подключение к сети Интернет не требуется.

2.2. Подготовка станций

Для антивирусной проверки станций требуется одновременное выполнение следующих условий:

- опция **Сетевое обнаружение** должна быть включена на компьютере, на котором запущена Консоль администрирования, если вы планируете искать станции в сети этим методом;
- станция должна быть доступна по сети;
- используемая для подключения учетная запись должна существовать и обладать необходимыми правами;
- если для защиты удаленного компьютера используется брандмауэр, необходимо провести дополнительные настройки;

  При использовании брандмауэра Windows в его настройках перейдите на вкладку **Дополнительные параметры**, выберите **Правила для входящих подключений** и включите следующие исключения: **Служба входа в сеть (NP-In)** и **Общий доступ к**

файлам и принтерам (SMB-In). Исключения должны быть включены для профиля брандмауэра **Private**. Если станция находится в домене, исключения должны быть включены для профиля **Domain**.

При использовании других брандмауэров необходимо открыть 445 порт.

- должна быть выполнена дополнительная настройка (см. Дополнительная настройка).

Перед началом работы убедитесь, что у вас имеется информация об учетных данных администраторов на всех станциях, подлежащих проверке.

Все действия по подготовке операционной системы станции к проверке Dr.Web CureNet! необходимо проводить под учетной записью с правами администратора.

Дополнительная настройка

Для проведения проверки станций требуется одновременное выполнение следующих дополнительных условий:

- ограничения системы контроля учетных записей (UAC) должны быть отключены, если станция работает под управлением Windows Vista или более поздней операционной системы. Если вы работаете под встроенным аккаунтом администратора, то данную настройку проводить не нужно. Перейдите к следующему пункту;

  Откройте редактор реестра операционной системы.

  1. Найдите и выберите ветку HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM.
  2. Если в данной ветке отсутствует ключ **LocalAccountTokenFilterPolicy**, создайте его:
     a. В меню **Правка** выберите команду **Создать**, а затем выберите **Параметр DWORD**.
     b. Введите в качестве имени ключа **LocalAccountTokenFilterPolicy**.
  3. В контекстном меню ключа **LocalAccountTokenFilterPolicy** выберите **Изменить**.
  4. В поле **Значение** введите **1**.
  5. Нажмите кнопку **OK** и выйдите из редактора реестра.
  6. Перезагрузите станцию.
  7. Повторите операцию для всех станциях, подлежащих проверке.

  

  Данную операцию рекомендуется выполнять только администратору или опытному пользователю системы. Неверные действия при изменении реестра могут серьезно повредить систему. Специалисты компании Microsoft рекомендуют перед изменением реестра создать резервную копию всех важных данных, имеющихся на компьютере.

- все необходимые для работы сети службы должны быть установлены и настроены;

Проверка сетевых настроек

1. Запустите Панель управления на станции.
   - при настройке поддерживаемых систем старше Windows Vista, выберите раздел **Сетевые подключения** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**).
   - при настройке Windows Vista выберите режим просмотра по категории. В категории **Сеть и Интернет** выберите **Просмотр состояния сети и задач** → **Управление сетевыми подключениями**.
   - при настройке Windows 7 или Windows Server 2008 выберите режим просмотра по категории. В категории **Сеть и Интернет** выберите **Просмотр состояния сети и задач** → **Изменение параметров адаптера**.
   - при настройке Windows 8, Windows 10 или Windows Server 2012 в категории **Сеть и Интернет** выберите **Центр управления сетями и общим доступом** → **Изменение параметров адаптера**.
   - при настройке Windows 10 в категории **Сеть и Интернет** перейдите в любую из вкладок **VPN**, **Ethernet** или **Набор номера**, выберите **Центр управления сетями и общим доступом** → **Изменение параметров адаптера**.
2. Щелкните правой кнопкой мыши по необходимому подключению и выберите пункт **Свойства**.
3. Проверьте, что для выбранного подключения установлены и настроены следующие службы:
   - клиент для сетей Microsoft;
   - служба доступа к файлам и принтерам сетей Microsoft;
   - протокол Интернета версии 4 (TCP/IPv4) или версии 6 (TCP/IPv6).
4. Сохраните изменения и закройте окно настроек.

- параметры общего доступа должны допускать расширенную настройку;

Настройка общего доступа

1. Запустите Панель управления на станции.
   - при настройке Windows XP или Windows Server 2003 выберите пункт **Брандмауэр Windows** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**);
   - при настройке Windows Vista выберите режим просмотра по категории. В категории **Сеть и Интернет** выберите **Настройка общего доступа к файлам**;
   - при настройке Windows 7 или Windows Server 2008 выберите режим просмотра по категории. В категории **Сеть и Интернет** выберите **Центр управления сетями и общим доступом** и затем выберите **Изменить дополнительные параметры общего доступа**;

- при настройке Windows 8, Windows 10 или Windows Server 2012 в категории **Сеть и Интернет** выберите **Центр управления сетями и общим доступом** и затем выберите **Изменить дополнительные параметры общего доступа**.

2. В открывшемся окне выполните одно из следующих действий:
   - при настройке Windows XP или Microsoft Windows Server 2003 перейдите на вкладку **Исключения** и включите настройку **Общий доступ к файлам и принтерам**;
   - при настройке Windows Vista установите **Сетевое обнаружение** и выберите **Общий доступ к файлам**;
   - при настройке Microsoft Windows Server 2008, Windows 7, Windows 8, Windows 10 или Microsoft Windows Server 2012 выберите **Включить сетевое обнаружение** и **Включить общий доступ к файлам и принтерам**.
3. Сохраните изменения и закройте окно настроек.

- для локальных учетных записей должна использоваться обычная модель совместного доступа и безопасности.

Настройка модели совместного доступа и безопасности

1. Запустите Панель управления на станции.
   - при настройке поддерживаемых систем старше Windows Vista выберите пункт **Администрирование** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**) и запустите утилиту **Локальная политика безопасности**.
   - при настройке Windows Vista и более поздних систем выберите режим просмотра по категории. В категории **Система и безопасность** выберите группу **Администрирование** и запустите утилиту **Локальная политика безопасности**.

   

   Для запуска утилиты по настройке локальных политик безопасности вы также можете набрать в поле поиска ОС Windows команду **secpol.msc** и нажать клавишу ENTER.

2. В дереве консоли выберите группу **Локальные политики**, а затем – группу **Параметры безопасности**.
3. Щелкните правой кнопкой мыши по параметру **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей**, выберите пункт **Свойства** и задайте значение **Обычная – локальные пользователи удостоверяются как они сами**.

   

   По умолчанию, подключение к удаленному компьютеру не может быть установлено, если используемая учетная запись содержит пустой пароль. Чтобы подключиться, задайте непустой пароль.

4. Закройте консоль.

2.3. Настройка контроллера домена Active Directory

Если в организации используется контроллер домена Active Directory, следует настроить

- параметры общего доступа к файлам и принтерам;
- параметры безопасности.

Вы можете создать новый объект групповой политики (GPO) для применения данных настроек или же изменить параметры уже существующего объекта.

Создание нового объекта групповой политики

1. В окне командной строки введите в текстовое поле **gpmc.msc** и запустите консоль управления групповыми политиками **GPMC**.
2. Создайте новый объект групповой политики, например **GPO-CureNet**. Для этого в дереве консоли **GPMC** правой кнопкой мыши щелкните **Объекты групповой политики** в соответствующем лесу и домене. Нажмите **Создать**. В открывшемся диалоговом окне укажите имя нового объекта и нажмите **OK**.
3. Привяжите созданный объект к нужному домену.
4. Правой кнопкой мыши нажмите на созданный объект, выберите **Изменить** и скорректируйте необходимые настройки в соответствие с описанием, приведенным ниже.

Если вы решили не создавать новый объект, а изменить параметры уже существующего объекта, то откройте окно с соответствующими настройками.

1. На компьютере, где установлена консоль управления групповыми политиками GPMC, нажмите **Пуск** → **Администрирование** → **Управление групповой политикой**.
2. Если появится диалоговое окно контроля учетных записей, поверьте данные и нажмите кнопку **Продолжить**.
3. В области навигации найдите и разверните узел **Лес: Имя леса**, затем разверните узел **Объекты групповой политики** и щелкните правой кнопкой мыши имя того объекта, для которого вы хотите задать разрешение.
4. В открывшемся меню выберите **Изменить**.

Настройка общего доступа к файлам и принтерам

Разрешите входящие запросы на доступ к файлам от клиентских компьютеров. Включение данного исключения брандмауэра открывает для IP-адресов, указанных в данном правиле, UDP-порты 137 и 138, а также TCP-порт 445.

Разрешение общего доступа к файлам и принтерам

1. В области навигации открывшегося окна разверните следующие узлы: **Конфигурация компьютера → Политики → Административные шаблоны → Сеть → Сетевые подключения → Брандмауэр Windows → Профиль домена**.
2. В области сведений дважды щелкните по настройке **Брандмауэр Windows: Разрешает исключение для входящего общего доступа к файлам и принтерам** и включите данное правило на вкладке настроек.
3. В текстовом поле **Разрешить незапрошенные входящие сообщения с этих IP-адресов** укажите нужный диапазон.
4. Нажмите **ОК**, чтобы сохранить изменения.

Настройка параметров безопасности

Настройте политику **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** так, чтобы при входе в сеть с учетными данными локальной учетной записи проверка подлинности производилась по этим данным.

Разрешение сетевого доступа по учетным записям пользователей

1. В области навигации открывшегося окна разверните следующие пункты: **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Локальные политики → Параметры безопасности**.
2. Для политики **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** установите режим **Обычная – локальные пользователи удостоверяются как они сами**.

Применение изменений в домене

Для того, чтобы применить изменения групповых политик в домене, в обоих случаях (и при создании нового объекта, и при изменении политик уже существующего объекта) в окне командной строки укажите команду **gpupdate /force**.

2.4. Лицензирование

Приобретение лицензии

Для работы Dr.Web требуется лицензия, которая позволяет полноценно использовать все возможности приложения. Приобрести лицензию вы можете на официальном сайте компании «Доктор Веб». Лицензия имеет два ограничения: срок действия и количество станций, которые могут быть одновременно выбраны для проверки. Параметры вашей лицензии хранятся в ключевом файле. Для того, чтобы просмотреть их, нажмите кнопку **Справка** и выберите пункт **О программе**.

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

- период, в течение которого разрешено использование продукта;
- перечень компонентов, разрешенных к использованию;
- период, в течение которого разрешено обновление (срок подписки; может не совпадать со сроком использования);
- другие ограничения (в частности, максимальное количество станций, которые разрешается проверять одновременно, и разрешение на проведение лечения).

При работе Dr.Web ключевой файл должен находиться в той же папке, в которую вы распаковали файлы программы. Если в ней одновременно расположены несколько ключевых файлов, Dr.Web выберет именно тот, который позволяет выполнить запрошенную операцию. Информацию об использовании лицензии можно просмотреть в файле журнала `CureNet.log`.

Изменение параметров лицензии

При необходимости, вы можете расширить допустимое количество станций или продлить срок действия лицензии. Для этого

1. Запустите Консоль администрирования.
2. На 1 шаге нажмите на **Мой Dr.Web** или на любом другом шаге нажмите кнопку **Справка** и выберите пункт **Мой Dr.Web**.

   В окне интернет-браузера по умолчанию откроется ваша персональная страница на сайте компании Dr.Web, где вы сможете не только изменить параметры лицензии, но и просмотреть всю необходимую информацию о ней, а также задать вопрос службе технической поддержки.
3. Загрузите обновленную версию дистрибутива Dr.Web, в котором содержится ваш новый ключевой файл.

Получение демонстрационного периода

Если перед приобретением лицензии вы хотите ознакомиться с продуктом, активируйте демонстрационный период. Для этого заполните специальную форму на официальном сайте компании «Доктор Веб». В демонстрационном режиме Dr.Web CureNet! не содержит функции лечения, но вы сможете ознакомиться с тем, как происходит распространение сканирующих процессов на станции в локальной сети, проверить станции на наличие угроз информационной безопасности и получить отчет об обнаруженных (но не вылеченных) вирусах и вредоносных программах. Для лечения станций необходимо приобрести коммерческую лицензию.

3. Запуск Dr.Web

Dr.Web не требует установки на проверяемых станциях. Для начала работы с программой и запуска первой проверки необходимо выполнить следующие действия:

- Скопировать на компьютер администратора дистрибутив Dr.Web и запустить его, после чего файлы программы распаковываются в папку Dr.Web, автоматически создается репозиторий Dr.Web и запускается Консоль администрирования.
- Убедиться в возможности доступа на станции, подлежащие проверке.
- Убедиться, что станции подготовлены к проверке.

Консоль администрирования запускается автоматически после распаковки дистрибутива Dr.Web.

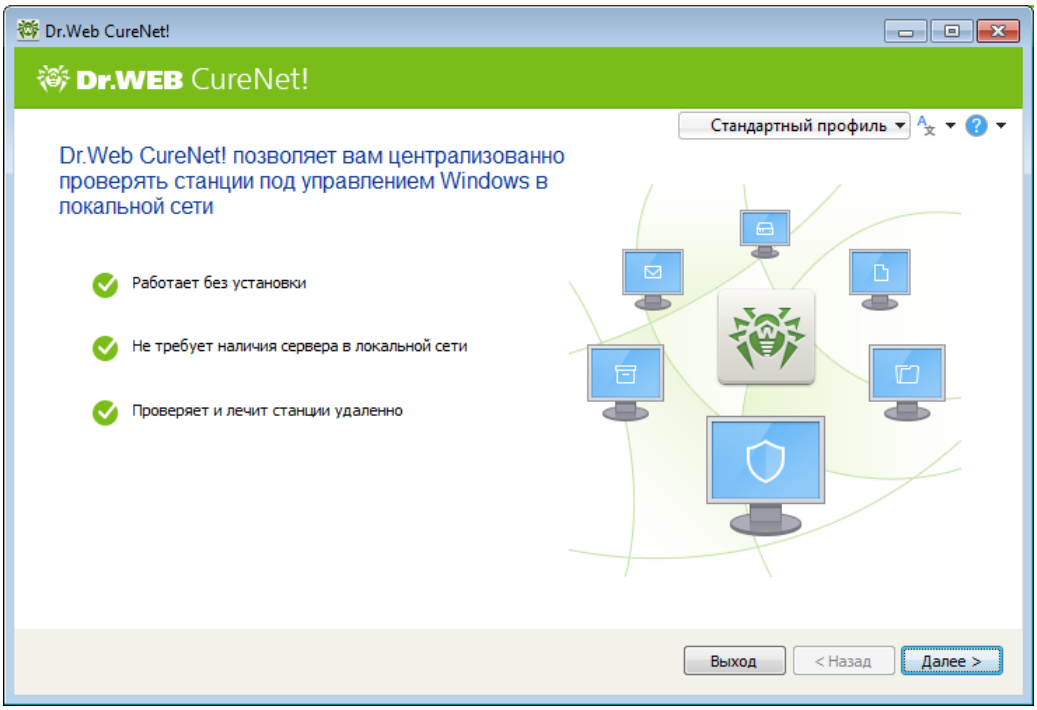

Рисунок 1. Консоль администрирования Dr.Web.

4. Обновление

Настоятельно рекомендуется устанавливать все обновления, выпускаемые компанией «Доктор Веб». Обновления вирусных баз позволяют обнаруживать ранее неизвестные вирусы, блокировать их распространение, а в ряде случаев – излечивать ранее неизлечимые зараженные файлы. Время от времени совершенствуются антивирусные алгоритмы, реализованные в виде исполняемых файлов и программных библиотек. Благодаря опыту эксплуатации антивирусов Dr.Web исправляются обнаруженные в программах ошибки, обновляется система помощи и документация.

Программа Dr.Web разработана специально для проведения централизованной проверки, поэтому для обеспечения максимальной защиты с ее помощью не требуется поводить обновление на каждой отдельной станции. Вирусные базы Dr.Web распространяются на проверяемые станции из репозитория Dr.Web, поэтому для поддержания актуальности информации о вредоносных программах и методах воздействия достаточно регулярно обновлять компоненты репозитория. При значительном устаревании вирусных баз Dr.Web в Консоли администрирования отображается соответствующее предупреждение.

Создание или обновление репозитория вручную не допускается.

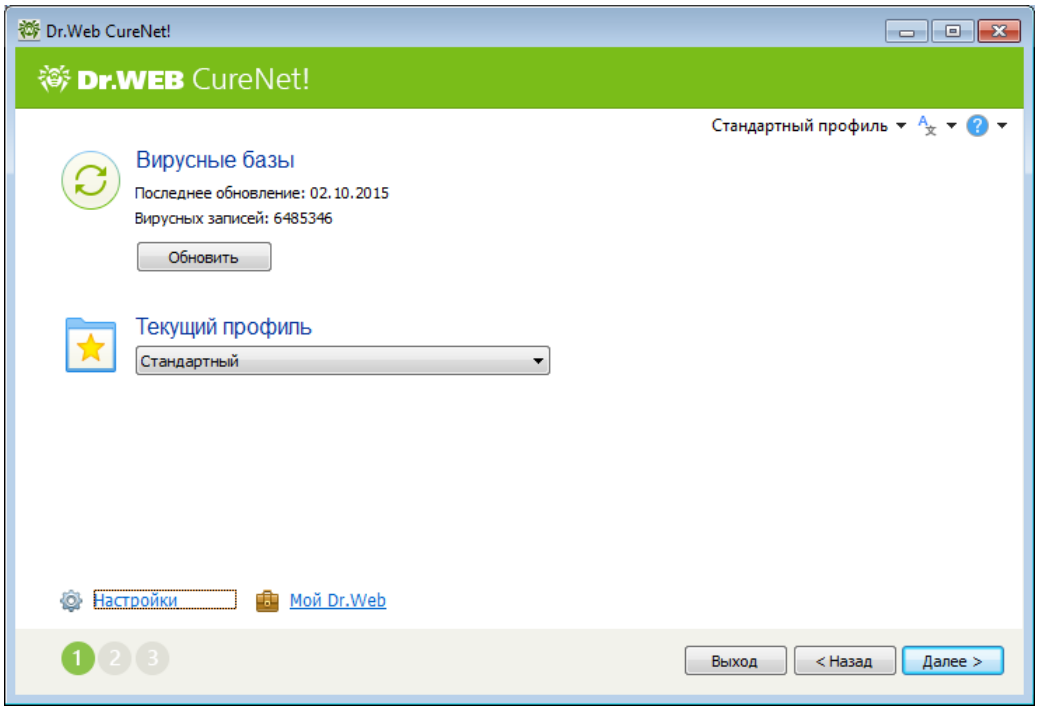

Рисунок 2. Обновление Dr.Web.

Для проведения обновления необходимо иметь доступ в сеть Интернет.

Обновление репозитория Dr.Web CureNet!

1. Dr.Web проверяет, не является ли ключевой файл заблокированным на сайте компании «Доктор Веб». Если действительный ключевой файл не найден, пользователю выдается соответствующее сообщение, обновление не производится, а компоненты программы могут быть заблокированы. В таком случае приобретите лицензию или обратитесь к службе технической поддержки компании «Доктор Веб».
2. Если действительный ключевой файл найден, запускается процесс обновления, во время которого Dr.Web загружает все обновленные файлы, соответствующие программной версии. Дождитесь завершения процесса.

Консоль администрирования и другие программные компоненты могут быть обновлены автоматически во время обновления репозитория или дистрибутива Dr.Web. При обновлении репозитория, Dr.Web проверяет наличие файла с новой версией консоли. При наличии новой версии пользователю будет предложено перезапустить программу, чтобы обновить Консоль администрирования. В противном случае консоль будет обновлена автоматически при следующем запуске программы.

Обратите внимание, что при таком методе обновления консоли, Dr.Web не загружает ключевой файл. Для того чтобы обновить лицензию в программе, необходимо выполнить обновление дистрибутива через Мой Dr.Web.

Обновление дистрибутива Dr.Web через Мой Dr.Web

Количество обновлений дистрибутива программы во время срока действия лицензии не ограничено.

1. Запустите Консоль администрирования.
2. В окне выбора профилей проверки нажмите **Мой Dr.Web** или на любой другом шаге нажмите кнопку **Справка** и выберите пункт **Мой Dr.Web**.

   В окне интернет-браузера по умолчанию откроется ваша персональная страница на сайте компании «Доктор Веб», откуда вы сможете загрузить обновленную версию дистрибутива Dr.Web при наличии действительной лицензии или продлить срок ее действия.
3. Сохраните обновленный дистрибутив Dr.Web.
4. Запустите дистрибутив Dr.Web, чтобы распаковать файлы программы и запустить обновленную Консоль администрирования.

5. Функции Dr.Web

Работа Dr.Web настраивается с компьютера администратора при помощи Консоли администрирования.

Во избежание прерывания работы Dr.Web рекомендуется временно отключать автоматическое обновление операционной системы.

Начало работы

1. Запустите Консоль администрирования и нажмите кнопку **Далее**.
2. В открывшемся окне вы можете выбрать необходимый профиль.
3. При значительном устаревании вирусных баз Dr.Web отображается соответствующее предупреждение. В таком случае настоятельно рекомендуется запустить процесс обновления, нажав на кнопку **Обновить**. Для продолжения работы нажмите **Далее**.
4. Выберите необходимые станции. Сформируйте список учетных записей, под которыми Dr.Web будет подключаться к указанным станциям. Нажмите **Далее**. Откроется окно выбора режимов работы.

Вы также сможете добавить новые станции позже: в ходе проверки или во время работы с карантином.

Запуск и проведение проверки

1. Укажите один из режимов проверки.
2. Нажав на ссылку **Настройки**, вы можете просмотреть и, при необходимости, изменить следующие параметры работы Сканера Dr.Web:
   - общие настройки работы станций при проверке (оповещение пользователей и перезагрузка проверенных станций и т.п.);
   - проверка архивов и контейнеров;
   - реакция на обнаружение определенных типов угроз;
   - режим работы сети во время сканирования и проверка доступности станций перед началом копирования файлов Dr.Web;
   - параметры сетевого подключения, которое используется для обновления репозитория Dr.Web.
3. Для запуска проверки нажмите кнопку **Начать**.

Во время проверки вы можете добавить новые станции, а также приостановить, возобновить или прекратить проверку определенной станции. Для этого нажмите на имя станции в таблице и в открывшемся контекстном меню выберите необходимое действие.

Обратите внимание на следующие особенности проверки:

- Действия над некоторыми зараженными или подозрительными объектами (например, ключами реестра, файлами, используемыми другими приложениями Windows) не могут быть выполнены немедленно. При обнаружении таких файлов Сканер Dr.Web помечает их как подлежащие обработке (в зависимости от заданного действия) после перезагрузки станции и выводит соответствующее оповещение в отчете. Для корректной обработки подобных объектов вы можете разрешить Сканеру Dr.Web перезагружать операционные системы проверенных станций при необходимости или выключать их автоматически после окончания сканирования. При этом пользователю станции будет выводиться соответствующее предупреждение и выделяться время на завершение текущей работы и сохранение информации. Подробнее о настройке действий над вредоносными объектами см. раздел Дополнительная настройка.
- При обнаружении вирусов в главной загрузочной записи операционной системы (MBR) Сканер Dr.Web применяет обязательную перезагрузку станции непосредственно после обнаружения вируса и восстановления записи (так называемая «жесткая» перезагрузка). Перезагрузка выполняется вне зависимости от того, установлен флажок **Перезагрузить станцию** или нет.

Процесс проверки станций не зависит от Консоли администрирования. Для выхода из Консоли администрирования нажмите кнопку **Выход**. При этом процесс проверки не прекращается, но статистика работы становится недоступной.

Просмотр результатов проверки

Процесс и общие результаты проверки отображаются в отчете о работе Dr.Web. Вы можете сохранить отчет в файле формата CSV или XML.

Также вы можете просмотреть подробные сведения о проверке конкретной станции.

Работа с карантином

1. В окне выбора режимов работы укажите режим **Менеджер карантина**.
2. Нажмите **Начать**.
3. Откроется окно работы с карантином, где вы можете просмотреть информацию о состоянии карантина на каждой выбранной станции, восстановить изолированные объекты в нужную папку, удалить их или скачать на свой компьютер.

5.1. Профили

Dr.Web позволяет сохранять все настройки проверки в файлах профилей: язык программы, список проверяемых станций, учетные данные для доступа к ним, реакцию Сканера Dr.Web на обнаружение угроз, а также другие настройки.

Создание нового профиля

1. На любом шаге проверки нажмите название профиля в верхней части окна (по умолчанию, **Стандартный профиль**) и выберите пункт **Сохранить**.
2. В открывшемся окне введите имя нового профиля проверки и при необходимости пароль доступа к нему. Пароль доступа требуется только при сохранении паролей для подключения к станциям.

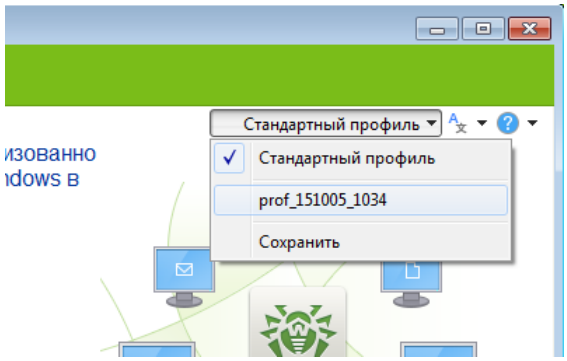

Рисунок 3. Профили.

3. Нажмите кнопку **Сохранить**.
4. Перейдите к следующим шагам проверки или нажмите кнопку **Выход**.

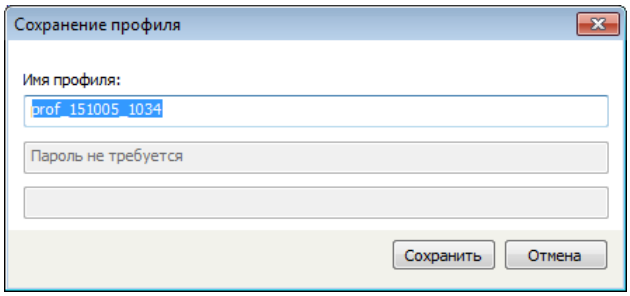

Рисунок 4. Сохранение профиля.

Изменения в настройках не сохраняются автоматически. Чтобы сохранить измененные настройки профиля, повторно сохраните его под тем же именем.

Вход в существующий профиль

1. На любом шаге проверки до выбора режима работы нажмите название профиля в верхней части окна (по умолчанию, **Стандартный профиль**) и выберите профиль, который вы хотите использовать. На шаге обновления вы можете также выбрать профиль непосредственно в окне Консоли администрирования.
2. Если требуется, введите пароль доступа к профилю.

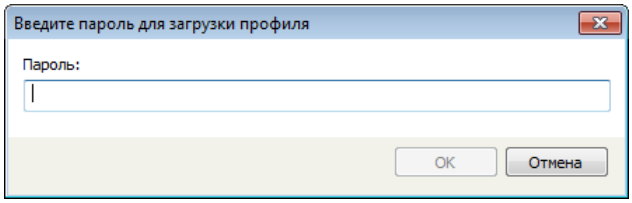

Рисунок 5. Загрузка профиля.

3. Консоль администрирования устанавливает все настройки проверки согласно информации, сохраненной в выбранном профиле. При необходимости измените настройки проверки на соответствующих шагах.

Удаление профиля

Профили не удаляются средствами Dr.Web. Чтобы удалить профиль проверки, удалите файл с его именем в подкаталоге Profiles каталога Dr.Web.

5.2. Выбор станций

На этом шаге вы можете выбрать станции для проверки или работы с карантином, а также указать параметры подключения к ним.

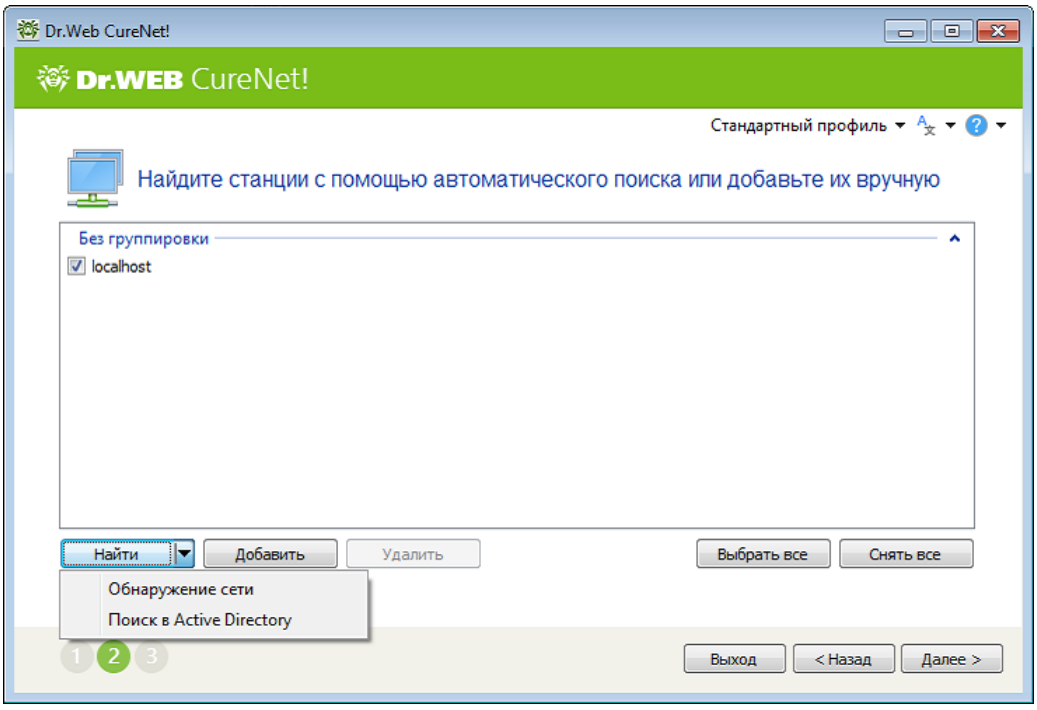

Рисунок 6. Выбор станций.

Dr.Web позволяет добавлять станции как вручную, так и при помощи автоматического поиска во всех сетях, доступных с компьютера, на котором запущена Консоль администрирования.

В результате поиска Dr.Web обнаруживает только те сети и станции, которые видимы для учетной записи, под которой запущена Консоль администрирования.

Автоматический поиск станций

1. Нажмите кнопку **Найти** и выберите нужный режим поиска.

   Если в вашей организации используется контроллер домена Active Directory, рекомендуется выбрать опцию **Поиск в Active Directory**. В этом случае обнаружение всех станций обычно занимает меньший промежуток времени и в списке отобразятся даже те станции, которые на момент поиска выключены.

   При выборе опции **Обнаружение сети** поиск всех станций может занять длительное время. В любой момент вы можете нажать кнопку **Прервать поиск**. Все станции, обнаруженные на этот момент, будут добавлены в список. Если в процессе поиска станция не была найдена, добавьте ее вручную.
2. Выберите необходимые станции из списка:
   - чтобы добавить определенную станцию, установите флажок рядом с ее именем или IP-адресом в списке;
   - чтобы добавить все станции из списка, нажмите кнопку **Выбрать все**;
   - чтобы снять выделение со всех станций и начать выбор заново, нажмите кнопку **Снять все**.

Добавление станций вручную

1. Для добавления одной или нескольких станций вручную нажмите кнопку **Добавить**.
2. В окне **Добавление станций** введите одно из следующих значений:
   - IP-адрес станции или ее сетевое имя;
   - диапазон IP-адресов станций через дефис («-») или с использованием маски (подробнее см. Приложение В. Сетевые маски).

При добавлении станций убедитесь, что указанный IP-адрес не является широковещательным (предназначенным для передачи широковещательных пакетов по сети).

3. Нажмите кнопку **ОК**.
4. Станции, добавленные в список вручную, автоматически выбираются для дальнейшей работы с ними. Для того, чтобы исключить станции из списка, снимите соответствующие флажки.
5. После завершения выбора сформируйте список учетных записей, под которыми Dr.Web будет подключаться к указанным станциям. По умолчанию подключение происходит с правами учетной записи, под которой запущена Консоль администрирования. Если подключение под этой учетной записью невозможно, то используются записи из списка.

Удаление станций из списка

1. Выделите те станции, которые вы хотите удалить из списка. Для быстрого выделения всех станций, нажмите на название соответствующей группы.
2. Нажмите кнопку **Удалить**.

После завершения выбора сформируйте список учетных записей, под которыми Dr.Web будет подключаться к указанным станциям. По умолчанию подключение происходит с правами учетной записи, под которой запущена Консоль администрирования. Если подключение под этой учетной записью невозможно, то используются записи из списка.

Настройка списка учетных записей

1. Чтобы сформировать или отобразить список учетных записей, нажмите **Учетные данные**. Откроется окно **Учетные записи и пароли**.

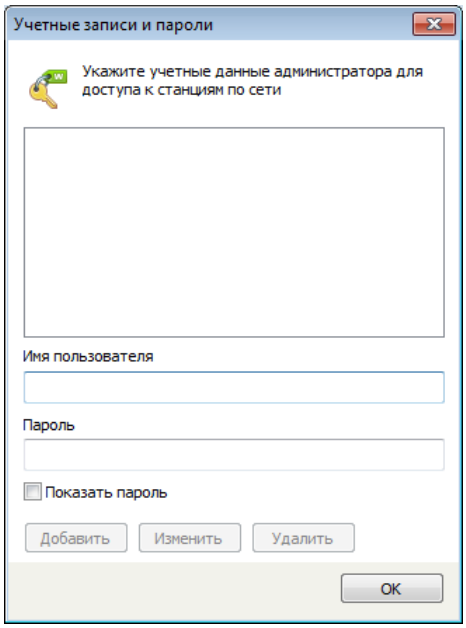

Рисунок 7. Управление учетной записью.

2. Отредактируйте список. При этом обратите внимание на особенности добавления учетных записей.
   - Имя пользователя необходимо указывать в одном из следующих форматов:

     <домен>\<имя пользователя>, где *<домен>* – имя домена, имеющего указанную учетную запись;

     <станция>\<имя пользователя>, где *<станция>* – сетевое имя станции, имеющей указанную учетную запись.
   - Если все станции, которые вы хотите добавить, находятся вне доменов и имеют одинаковую учетную запись, то для ускорения подключение рекомендуется добавить к списку только эту общую учетную запись, опустив при этом имя станции. Dr.Web автоматически попытается подключиться ко всем станциям под этой учетной записью.

Данный способ подходит только для сетей с корректной конфигурацией.

3. Нажмите кнопку **ОК**.

Добавление станций во время проверки

1. Нажмите правой кнопкой мыши внутри таблицы и в открывшемся меню выберите **Добавить станцию**.
2. Введите IP-адрес или сетевое имя станции.
3. Нажмите **ОК**. Станция, соответствующая указанным данным, добавится в список проверяемых.

5.3. Выбор режима работы

На этом шаге задается режим работы Сканера Dr.Web на станциях и его реакция на обнаружение зараженных или подозрительных файлов, вредоносных программ, а также инфицированных архивов и почтовых сообщений.

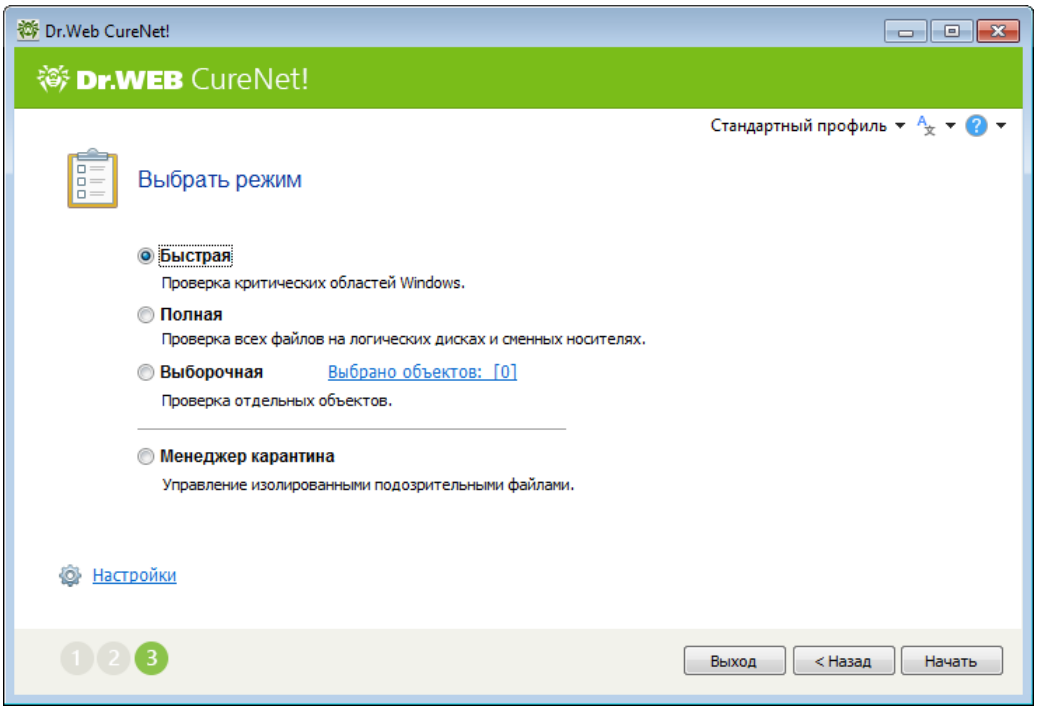

Рисунок 8. Выбор режима работы.

Режимы проверки

По умолчанию после копирования файлов Dr.Web запускает на станции Сканер Dr.Web, который выполняет быструю проверку (режим **Быстрая проверка**).

В данном режиме проверяются следующие объекты:

- оперативная память;

- загрузочные секторы всех дисков;
- корневая папка загрузочного диска;
- системная папка Windows;
- папка Мои Документы;
- временная папка системы;
- временная папка пользователя.

Папка Мои документы и папка с временными файлами пользователя проверяются для всех учетных записей на станции.

Архивированные файлы в данном режиме не проверяются.

Вы можете изменить режим проверки, выбранный по умолчанию, на один следующих:

- **Полная проверка**, при которой сканируются оперативная память и все жесткие диски, включая их загрузочные секторы, а также осуществляется проверка на наличие руткитов.
- **Выборочная проверка**, при которой на всех выбранных станциях сканируются только указанные объекты. Чтобы выбрать объекты для сканирования, нажмите ссылку **Выбрано объектов**. В появившемся окне укажите необходимые объекты для сканирования. Они добавятся в профиль при сохранении.

Режим Менеджер карантина

Данный режим позволяет просматривать и редактировать содержимое карантина, созданного на станциях, а также копировать на свой компьютер изолированные файлы для дальнейшей работы с ними. Карантин служит для изоляции файлов, подозрительных на наличие вредоносных объектов. Также в него помещаются резервные копии файлов, обработанных Dr.Web.

5.4. Дополнительная настройка

Настройки программы по умолчанию являются оптимальными для большинства случаев.

При необходимости вы можете добавить проверку архивов и почтовых файлов, изменить реакцию Сканера Dr.Web на обнаружение вредоносных объектов и задать некоторые другие дополнительные настройки.

Дополнительная настройка проверки

1. Чтобы открыть окно с настройками, нажмите на **Настройки**.
2. Задайте нужные параметры на следующих вкладках:

- Общие
- Исключения
- Действия
- Сеть
- Обновление

При необходимости нажимайте кнопку **Применить**.

3. По окончании редактирования настроек нажмите кнопку **OK** для сохранения внесенных изменений или кнопку **Отмена** для отказа от них.

Изменение настроек имеет силу только в данном сеансе работы Dr.Web. При повторном запуске утилиты все настройки автоматически возвращаются к первоначальным значениям. Используйте профили для сохранения настроек.

5.4.1. Вкладка Общие

На этой вкладке вы можете указать общие настройки работы станций при проверке с помощью Dr.Web.

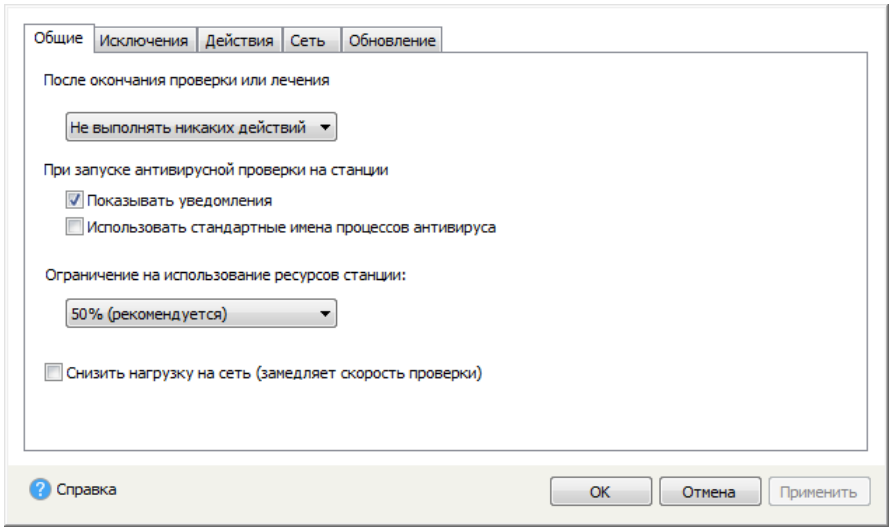

Рисунок 9. Настройка Dr.Web. Вкладка Общие.

Для успешного завершения лечения некоторых инфицированных файлов (например, файлов, которые используются другими приложениями, или ключей реестра) требуется перезагрузка операционной системы. На этой вкладке задаются дополнительные настройки лечения таких инфекций.

Режимы **Перезагрузить станцию** и **Выключить станцию** предписывают выполнение соответствующего действия на станции автоматически, при этом ее пользователю выводится соответствующее предупреждение и выделяется время на завершение работы и сохранение информации. Перезагрузка выполняется один раз после завершения сканирования.

Режим **Не выполнять никаких действий** позволяет пользователям продолжать работу без перезагрузки, но не гарантирует успешного завершения лечения некоторых инфекций.

При обнаружении вирусов в главной загрузочной записи операционной системы (MBR) Сканер Dr.Web применяет обязательную перезагрузку станции непосредственно после обнаружения вируса и восстановления записи (так называемая «жесткая» перезагрузка). Такая перезагрузка выполняется вне зависимости от выбранного режима.

Dr.Web по умолчанию оповещает пользователей станций о начале проверки при помощи сообщений, появляющихся в виде всплывающего окна в области уведомлений Windows. Чтобы не оповещать пользователей, снимите флажок **Показывать уведомления**.

По умолчанию при копировании на проверяемую станцию файлов Dr.Web для них генерируются случайные имена. Если на станции установлен антивирус с брандмауэром, то администратору может понадобиться при каждой проверке задавать для него исключения. В таком случае рекомендуется включить режим **Использовать стандартные имена процессов антивируса**, чтобы файлы Dr.Web копировались на станции под своими именами. При этом администратору понадобится прописать исключение брандмауэра на проверяемой станции только один раз.

Вы можете также установить ограничение на использование ресурсов проверяемой станции. По умолчанию выбрано значение равное 50%. Чтобы изменить это значение или полностью снять ограничение, выберите соответствующий пункт выпадающего списка под заголовком **Ограничение на использование ресурсов станции**.

В условиях высокой загруженности сети вы можете включить настройку **Снизить нагрузку на сеть (замедляет скорость проверки)**. В этом режиме Dr.Web копирует программные файлы на станции по очереди, а также увеличивает временной интервал, по истечении которого станция отправляет данные администратору. Обратите внимание, что данная настройка замедляет скорость проверки.

5.4.2. Вкладка Исключения

На этой вкладке вы можете задать список файлов и папок, которые должны быть исключены из проверки Сканером Dr.Web на станции. Из проверки могут быть исключены папки карантина антивируса, рабочие папки некоторых программ, временные файлы (файлы подкачки) и т. п. По умолчанию этот список пуст.

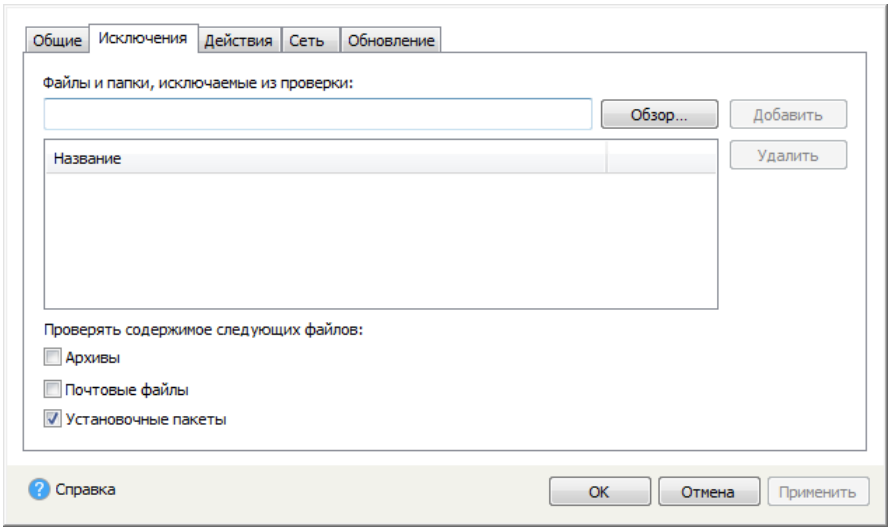

Рисунок 10. Настройка Dr.Web. Вкладка Исключения.

Формирование списка исключений

1. Чтобы добавить папку или файл к списку исключений, выполните одно из следующих действий:
   - чтобы указать конкретный существующий файл или папку, нажмите кнопку **Обзор** и выберите папку или файл в стандартном окне открытия файла. Вы можете вручную ввести полный путь к файлу или папке в поле ввода, а также отредактировать запись в поле ввода перед добавлением ее в список;
   - чтобы исключить из проверки все файлы или папки с определенным именем, введите это имя в поле ввода. Указывать путь к папке или файлу при этом не требуется;
   - чтобы исключить из проверки файлы или папки определенного вида, введите определяющую их маску в поле ввода. Подробнее о масках:

   Маска задает общую часть имени объекта, при этом:

   - символ «`*`» заменяет любую, возможно пустую, последовательность символов;
   - символ «`?`» заменяет любой, но только один 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`, `photoмама09.jpg` или `photo----09.jpg`.

2. Нажмите кнопку **OK**. Выбранный файл или папка появится в списке.

Примеры задания исключений:

- `C:\folder` или `C:\folder\**` – исключает из проверки все файлы в папке C:\folder. В подпапках файлы будут проверяться.
- `C:\folder\*` – исключает из проверки все файлы в папке C:\folder и всех подпапках на любом уровне.
- `C:\folder\*.txt` – исключает из проверки файлы *.txt в папке C:\folder. В подпапках файлы *.txt будут проверяться.
- `C:\folder\*\*.txt` – исключает из проверки файлы *.txt только в подпапках первого уровня папки C:\folder.
- `C:\folder\**\*.txt` – исключает из проверки файлы *.txt в подпапках любого уровня папки C:\folder. В самой папке C:\folder файлы *.txt будут проверяться.

При необходимости вы можете выбрать следующие объекты для проверки:

- **Архивы** – поставьте этот флажок, чтобы проверять файлы в архивах;
- **Почтовые файлы** – поставьте этот флажок, чтобы проверять файлы почтовых клиентов;
- **Установочные пакеты** – поставьте этот флажок, чтобы проверять файлы установочных пакетов.

При обнаружении инфицированного объекта в архиве предписанное действие выполняется для всего архива целиком, а не только для вредоносного объекта.

Обратите внимание, что включение данных режимов сканирования может значительно замедлить процесс проверки.

5.4.3. Вкладка Действия

Действия над зараженными или подозрительными объектами выполняются только при работе в основном режиме (при наличии действенного лицензионного ключевого файла). При работе в демонстрационном режиме производится только информирование.

На этой вкладке вы можете изменить реакцию Сканера Dr.Web в зависимости от типа обнаруженной угрозы и вида зараженного объекта.

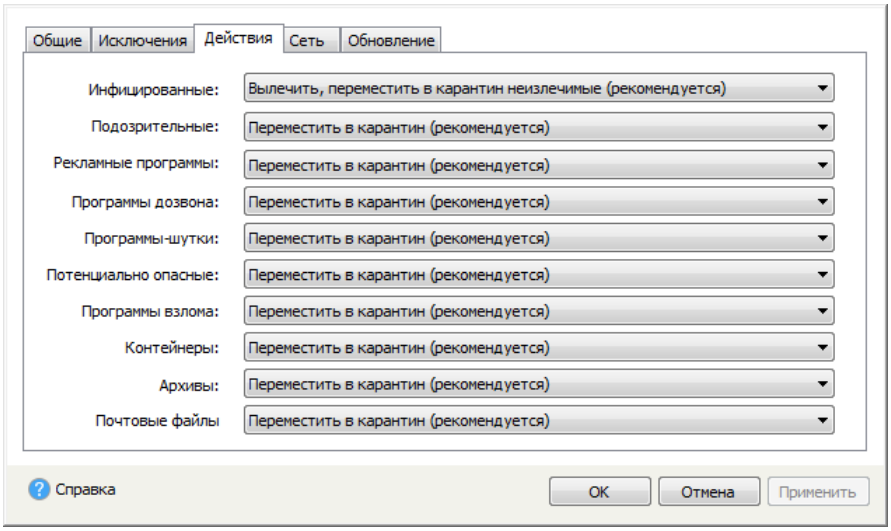

Рисунок 11. Настройка Dr.Web. Вкладка Действия.

По умолчанию в случае обнаружения известного вируса или при подозрении на зараженность объекта вирусом Сканер Dr.Web, запущенный Dr.Web на станции, предпринимает автоматические действия по предотвращению угрозы.

Реакция задается отдельно для каждой категории объектов:

- **Инфицированные** – зараженные известным и (предположительно) излечимым вирусом;
- **Подозрительные** – предположительно представляющие угрозу информационной безопасности.

Также отдельно задается реакция для конкретных видов вредоносных программ и типов пакетов (архивов, почтовых файлов, контейнеров).

При обнаружении инфицированного объекта в архиве применяется реакция, заданная для архивов. Предписанное действие выполняется для всего архива целиком, а не только для вредоносного объекта.

При необходимости вы можете изменить действие по умолчанию на одну из следующих реакций:

- **Вылечить, переместить в карантин неизлечимые (рекомендуется)** (доступна только для инфицированных объектов) – предписывает Сканеру Dr.Web пытаться излечить объект, зараженный известным вирусом. Если вирус неизлечим или попытка лечения была не успешной, файл будет помещен в карантин;
- **Переместить в карантин (рекомендуется)** – (невозможна для загрузочных секторов) предписывает Сканеру Dr.Web переместить вредоносный или подозрительный объект в карантин;
- **Игнорировать** – (доступна только для вредоносных программ) – не выводить информацию об обнаружении вредоносной программы в отчете о работе Dr.Web;

- **Информировать** – вывести информацию о вредоносном или подозрительном объекте в отчете о работе Dr.Web.

5.4.4. Вкладка Сеть

На этой вкладке вы можете указать дополнительные настройки сетевого взаимодействия станции во время проверки Сканером Dr.Web.

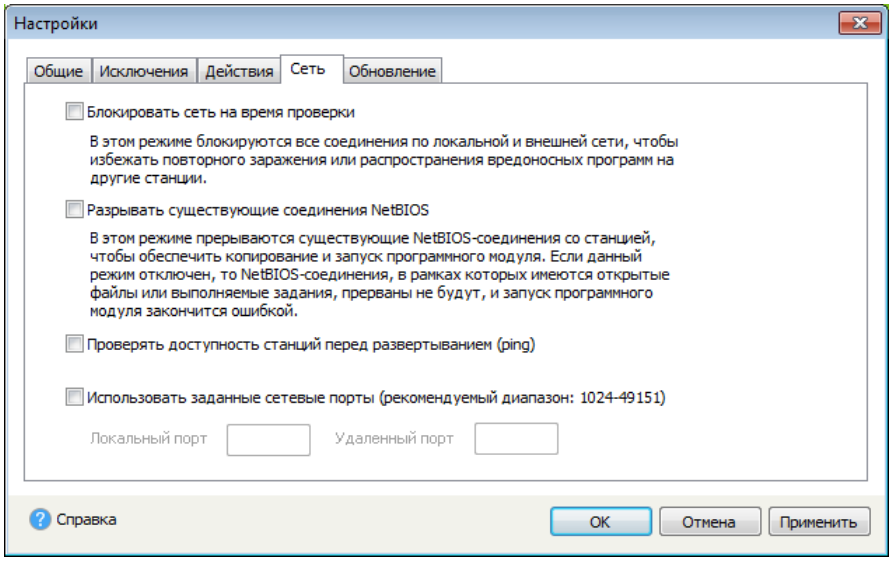

Рисунок 12. Настройка Dr.Web. Вкладка Сеть.

При необходимости вы можете выбрать следующие режимы:

- **Блокировать сеть на время проверки** – выберите этот режим, чтобы на время проверки запретить взаимодействие по сети на станции и, таким образом, предотвратить распространение эпидемии в сети и избежать повторного заражения самой станции;
- **Разрывать существующие соединения NetBIOS** – выберите этот режим, чтобы перед началом проверки прерывать все существующие NetBIOS-соединения, включая те, в рамках которых имеются открытые файлы или выполняемые задания (необходимо для копирования файлов и запуска Сканера Dr.Web);
- **Проверять доступность станций перед развертыванием (ping)** – выберите этот режим, чтобы перед началом копирования файлов проверять доступность станции по сети с использованием утилиты ping;
- **Использовать заданные сетевые порты (рекомендуемый диапазон: 1024-49151)** – выберите этот режим, чтобы во время проверки сетевое взаимодействие Сканера Dr.Web и станции происходило по заданным портам.

5.4.5. Вкладка Обновление

На этой вкладке вы можете указать параметры сетевого подключения, которое используется для обновления репозитория Dr.Web.

При необходимости вы можете выбрать следующие режимы:

- **Использовать HTTPS-соединение** – поставьте этот флажок, если вы хотите загружать обновления по безопасному протоколу;
- **Использовать прокси-сервер** – поставьте этот флажок, если вы хотите использовать прокси-сервер. Укажите **Адрес** и **порт** необходимого прокси-сервера. Если на указанном прокси-сервере требуется авторизация, введите соответствующие данные в поля **Имя пользователя** прокси-сервера и **Пароль.**

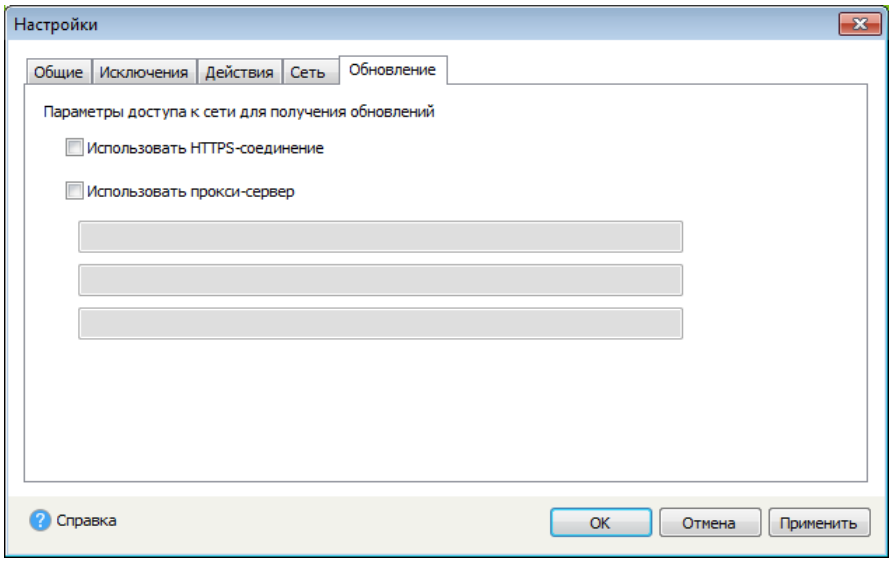

Рисунок 13. Настройка Dr.Web. Вкладка Обновление.

5.5. Отчет о работе Dr.Web

На шаге **Статистика работы** отображаются текущие сведения о работе Сканера Dr.Web на всех проверяемых станциях. Сбор статистики не зависит от качества связи между компьютером, на котором запущена Консоль администрирования, и проверяемыми станциями. При кратковременной утере связи со станцией после начала проверки Dr.Web предпринимает попытки восстановить соединение и обновляет статистику проверки после восстановления связи.

В верхней части окна отображается информация о статусе проверки и общая статистка сканирования всех станциях.

Секция **Станции** включает следующую информацию:

Поле	**Описание**
Задано	Общее количество заданных к проверке станций.
Найдено	Количество доступных по сети станций.
Не найдено	Количество недоступных по сети станций.

Поле	Описание
Доставлено	Количество станций, к которым удалось успешно подключиться и скопировать файлы Dr.Web.
Ошибок доставки	Количество станций, к которым не удалось подключиться и/или скопировать файлы Dr.Web.
Проверяется	Количество все еще проверяемых станций.
Завершено	Количество уже проверенных станций.
Вылечено	Общее количество полностью вылеченных станций, на которых все вредоносные объекты были обезврежены.
Перезагружено	Общее количество станций, перезагруженных для корректного завершения лечения.

Секция **События** включает следующую информацию:

Поле	Описание
Проверено	Общее количество проверенных объектов на всех станциях.
Угроз	Общее количество вирусных угроз, обнаруженных на всех станциях.
Обезврежено	Общее количество объектов, вылеченных на всех станциях.
Ошибок проверки	Общее количество ошибок проверки.

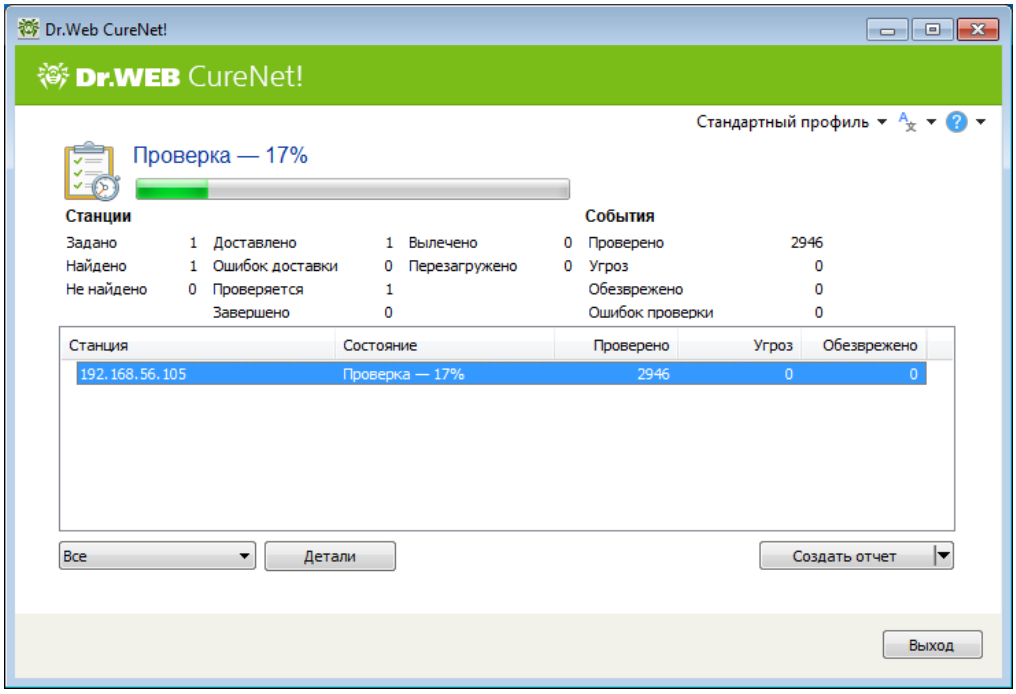

Рисунок 14. Отчет о работе Dr.Web.

В поле отчета в табличной форме представлены сведения о ходе проверки станций:

Поле	Описание
Станция	Наименование или адрес станции.
Состояние	Статус проверки станции (установка, процент выполнения проверки, сообщение об ошибке сканирования или недоступности станции и пр.).
Проверено	Общее количество проверенных объектов на станции.
Угроз	Общее количество обнаруженных угроз информационной безопасности.
Обезврежено	Общее количество обезвреженных вредоносных объектов (лечение доступно только для объектов, зараженных известным и предположительно излечимым вирусом).

При необходимости используйте фильтр для отображения информации в зависимости от статуса проверки и состояния станции. Также вы можете отсортировать список, нажав на заголовок той колонки, по которой хотите упорядочить станции.

Корректность главной загрузочной записи (MBR, master boot record) является критической характеристикой операционной системы, поэтому для удаления MBR-вирусов и восстановления загрузочных записей Сканер Dr.Web применяет обязательную перезагрузку операционной системы непосредственно после обнаружения вируса и восстановления записи (так называемая «жесткая» перезагрузка). Проверка станции при этом завершается досрочно.

В отчете о работе Dr.Web о подобной перезагрузке свидетельствует досрочное завершение сканирования зараженной станции по сравнению со всеми остальными станциями, а также информация о вирусе в главной загрузочной записи операционной системы, доступная в окне статистики станции.

Для окончания проверки станций, зараженных MBR-вирусами, необходимо повторно запустить сканирование.

Добавление новой станции для сканирования

Чтобы добавить новую станцию для сканирования во время уже запущенного сканирования, кликните правой кнопкой мыши в поле отчета нажмите **Добавить станцию** и введите IP-адрес или сетевое имя необходимой станции.

Просмотр статистики станции

Чтобы получить более подробные сведения о проверке конкретной станции в отдельности, выполните одно из следующих действий:

- дважды щелкните по имени или адресу станции в списке;
- выберите станцию в списке и нажмите **Детали**.

Откроется окно статистики станции. При возникновении ошибок в процессе копирования файлов Dr.Web на станцию или потере связи при проверки в данном окне выводятся соответствующие предупреждения.

Если указанные объекты обнаружены в файловых архивах, почтовых файлах или файловых контейнерах, в отчете приводятся как инфицированные объекты, так и содержащие их архивы.

Подробнее о настройке действий над вредоносными объектами см. раздел Дополнительная настройка.

Сохранение отчета

Для сохранения отчета нажмите на **Создать отчет**, выберите формат отчета и станции, которые необходимо включить в отчет. Отчет будет автоматически сохранен в папку продукта.

5.6. Менеджер карантина

Dr.Web позволяет просматривать и редактировать содержимое карантина, созданного на станциях, а также копировать на свой компьютер изолированные файлы для дальнейшей работы с ними. Карантин служит для изоляции файлов, подозрительных на наличие вредоносных объектов. Также в него помещаются резервные копии файлов, обработанных Dr.Web.

Переход в режим карантина

1. Укажите станции, на которых вы хотите открыть содержимое карантина.
2. В окне выбора режимов работы укажите режим **Менеджер карантина**.
3. Нажмите **Начать**.

В верхней части окна вы увидите информацию о работе Менеджера карантина на указанных станциях:

Поле	Описание
Задано	Общее количество указанных станций.
Найдено	Количество доступных по сети станций.
Не найдено	Количество недоступных по сети станций.
Доставлено	Количество станций, к которым удалось успешно подключиться и скопировать файлы Dr.Web.
Ошибок доставки	Количество станций, к которым не удалось подключиться и/или скопировать файлы Dr.Web.
Запущено	Количество станций, на которых в данный момент запущен **Менеджер карантина**.
Завершено	Количество станций, на которых **Менеджер карантина** завершил работу (например, из-за того, что станция была выключена пользователем).

В этом окне вы можете:

- изменить учетные данные для подключения к станции. Для этого выберите станцию в списке, нажмите на нее правой кнопкой мыши и выберите **Изменить учетные данные**.
- добавить новые станции для работы. Для этого нажмите правой кнопкой мыши внутри таблицы и выберите **Добавить станцию**. Откроется окно, в котором следует ввести IP-адрес или сетевое имя станции.
- отфильтровать станции по одному из параметров: с ошибками, найдено, не найдено, с непустым карантином, с пустым карантином. Для этого нажмите на выпадающий список под таблицей и выберите нужный фильтр.

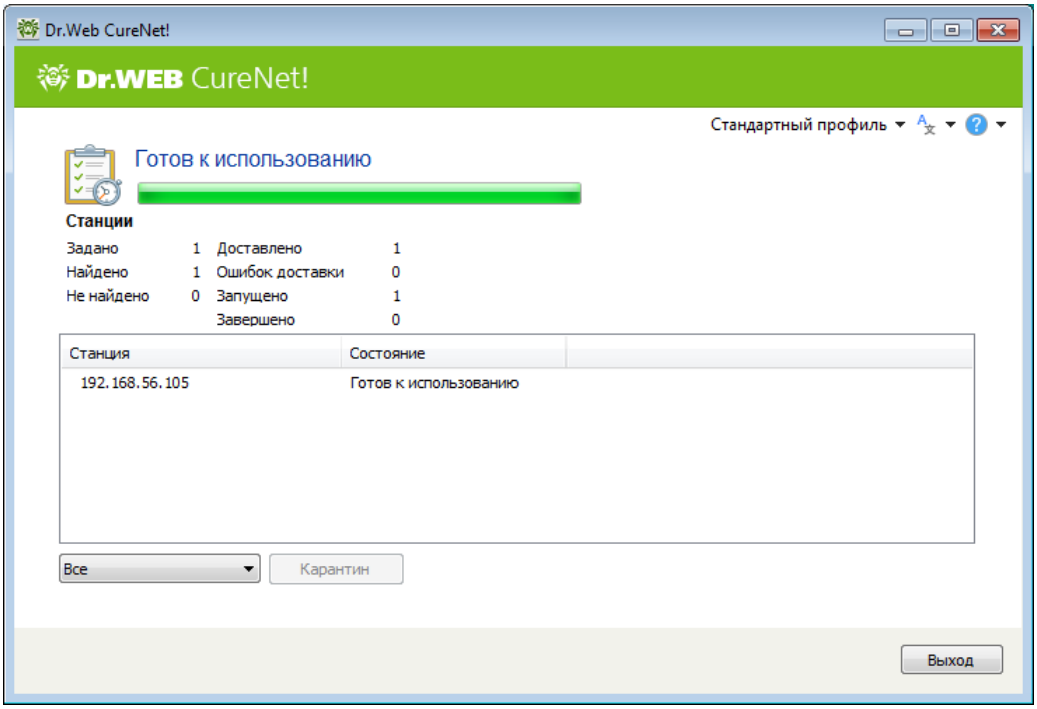

Рисунок 15. Менеджер карантина Dr.Web.

Для того, чтобы просмотреть и отредактировать содержимое карантина на конкретной станции, выберите ее в списке и либо в контекстном меню станции нажмите **Карантин**, либо нажмите кнопку **Карантин** внизу окна.

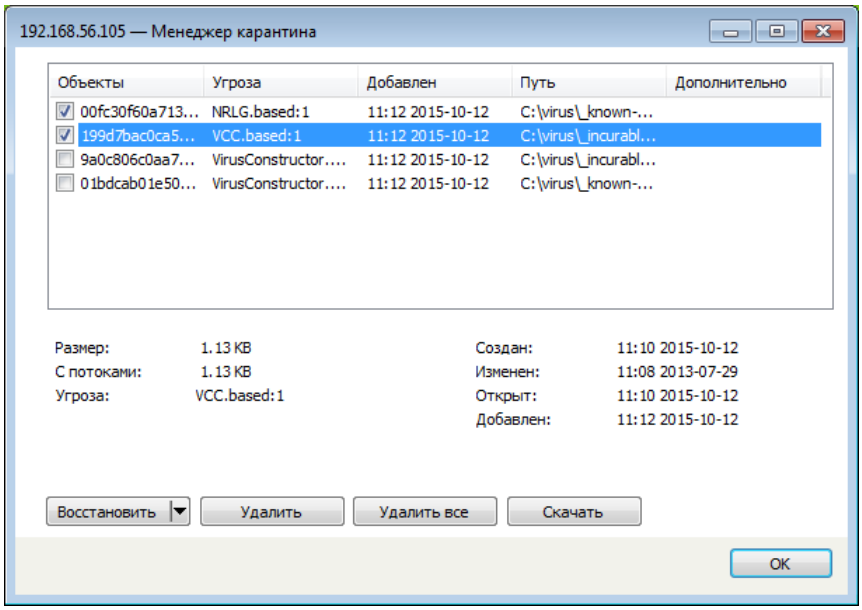

Рисунок 16. Просмотр содержимого карантина.

В открывшемся окне вы видите список имен объектов, изолированных на данной станции в карантин, а также краткую информацию по каждому из них: классификация вредоносной программы, определяемая Dr.Web, дата добавления объекта в карантин, путь, по которому объект находился до перемещения в карантин и т.д.

В данном окне вы можете:

- восстановить объекты в исходную папку. Для этого выберите их в списке и нажмите кнопку **Восстановить** внизу окна.
- восстановить объекты в заданную папку. Для этого нажмите кнопку **Восстановить** внизу окна и выберите **Восстановить как**.
- удалить конкретные объекты. Для этого выберите их в списке и нажмите кнопку **Удалить** внизу окна.
- удалить все объекты одновременно. Для этого нажмите кнопку **Удалить все** внизу окна.
- скачать на свой компьютер объекты из карантина. Для этого выберите в списке нужные объекты и нажмите кнопку **Скачать** внизу окна. В открывшемся окне укажите папку, куда следует сохранить объекты.

6. Приложение А. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела https://support.drweb.com/;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу https://company.drweb.com/contacts/offices/.

7. Приложение Б. Методы обнаружения вирусов

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. 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.

8. Приложение В. Сетевые маски

Маска задает общую часть двоичной записи IP-адресов компьютеров, добавляемых к проверке. Для задания группы IP-адресов при помощи маски необходимо указать IP-адрес одного из компьютеров в группе и собственно маску, которая при помощи операции побитового И (побитовой конъюнкции) определяет остальные компьютеры.

Например, чтобы добавить к проверке 254 удаленных компьютера с адресами от 10.30.0.1 до 10.30.0.254, можно указать маску 10.30.0.0/24:

Адрес 10.30.0.1	00001010.00011110.00000000.00000001
Маска 255.255.255.0 (24)	11111111.11111111.11111111.00000000
Хост (минимальный) 10.30.0.1	00001010.00011110.00000000.00000001
Хост (максимальный) 10.30.0.254	00001010.00011110.00000000.11111110
Широковещательный адрес 10.30.0.255	00001010.00011110.00000000.11111111

Хостов в сети: 254

При указании компьютеров для проверки допускается использование следующих форм записи битовых масок:

- в десятичном виде (четырёхкомпонентная система с точками). Например, 192.168.0.1/255.255.255.0, где 192.168.0.1 - IP-адрес одного из задаваемых компьютеров, 255.255.255.0 - маска;
- в двоичном виде (так называемая слэш-нотация или CIDR-нотация, при которой указывается количество единичных бит в двоичной записи маски). Например, 192.168.0.1/24, где 192.168.0.1 - IP-адрес одного из задаваемых компьютеров, 24 - десятичная запись двоичной маски, в которой первые 24 бита - единичные, остальные - нулевые.

В сетях IPv4 возможно использование обеих систем записи. В сетях IPv6 используется только запись в CIDR-нотации.