



Защити созданное

## Руководство администратора

**© 2009-2013 «Доктор Веб». Все права защищены.**

Материалы, приведенные в данном документе, являются собственностью «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

**ТОРГОВЫЕ ЗНАКИ**

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk и логотипы Dr.WEB являются зарегистрированными товарными знаками «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

**ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ**

Ни при каких обстоятельствах «Доктор Веб» и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

**Dr.Web® CureNet!™**

**Версия 8.0.0**

**Руководство администратора**

**29.5.2013**

«Доктор Веб», Центральный офис в России  
125124

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: [www.drweb.com](http://www.drweb.com)

Телефон: +7 (495) 789-45-87

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

# **«Доктор Веб»**

«Доктор Веб» - российский разработчик средств информационной безопасности.

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

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

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

**Мы благодарны пользователям за поддержку  
решений семейства Dr.Web!**



# Содержание

<b>Используемые обозначения</b>	<b>6</b>
<b>1. Dr.Web® CureNet!™</b>	<b>7</b>
<b>1.1. Системные требования</b>	<b>9</b>
1.1.1. Требования к удаленным компьютерам	<b>10</b>
1.1.2. Подготовка систем начиная с Windows® Vista®	<b>12</b>
1.1.3. Подготовка систем Windows XP® и более ранних	<b>23</b>
<b>1.2. Лицензирование</b>	<b>31</b>
<b>2. Начало работы</b>	<b>34</b>
<b>2.1. Консоль администрирования</b>	<b>34</b>
<b>2.2. Репозиторий Dr.Web CureNet!</b>	<b>36</b>
<b>2.3. Методы обнаружения вирусов</b>	<b>36</b>
<b>2.4. Режимы работы</b>	<b>38</b>
<b>3. Антивирусная проверка</b>	<b>39</b>
<b>3.1. Профили проверки</b>	<b>41</b>
<b>3.2. Выбор станций</b>	<b>43</b>
3.2.1. Настройка списка учетных записей	<b>46</b>
<b>3.3. Настройка действий</b>	<b>50</b>
3.3.1. Вкладка Общие	<b>52</b>
3.3.2. Вкладка Типы файлов	<b>53</b>
3.3.3. Вкладка Действия	<b>55</b>
3.3.4. Вкладка Сеть	<b>57</b>
3.3.5. Вкладка Прокси	<b>58</b>
<b>3.4. Отчет о работе Dr.Web CureNet!</b>	<b>58</b>



3.4.1. Статистика компьютера	61
<b>4. Обновление</b>	<b>65</b>
<b>Приложение А. Сетевые маски</b>	<b>69</b>
<b>Приложение Б. Техническая поддержка</b>	<b>71</b>



## Используемые обозначения

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

**Таблица 1. Условные обозначения.**

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



# 1. Dr.Web® CureNet!™

Благодарим вас за выбор программы **Dr.Web® CureNet!™** (далее **Dr.Web CureNet!**).

Данный продукт предназначен для проведения централизованной антивирусной проверки компьютеров по сети без установки антивируса на удаленные компьютеры. **Dr.Web CureNet!** позволяет проводить удаленное лечение рабочих станций и серверов Windows, в том числе с установленными антивирусами других производителей, в локальных сетях любого масштаба, при этом 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.

В программе **Dr.Web CureNet!** применены наиболее передовые разработки и технологии компании «Доктор Веб», которые позволяют обнаруживать и обезвреживать вредоносные объекты, представляющие угрозу функционированию компьютеров и сети.

**Dr.Web CureNet!** проверяет файлы, архивы, файловые контейнеры, почтовые сообщения, а также загрузочные записи на наличие всевозможных угроз информационной безопасности (в частности, вирусов, червей, руткитов, троянских программ, программ дозвона, рекламных программ, потенциально опасных программ, программ взлома и программ-шуток). При обнаружении угроз безопасности **Dr.Web CureNet!** по возможности обезвреживает обнаруженные вредоносные программы.

Для защиты от действия анти-антивирусных программ, направленных на выведение антивирусов из строя, используется **Dr.Web SelfPROtect**, защищающий файлы **Dr.Web CureNet!** на удаленной машине.



## Основные функции программы

**Dr.Web CureNet!** предоставляет вам следующие преимущества:

- централизованная проверка удаленных компьютеров без установки антивируса на каждый проверяемый компьютер;
- обнаружение вредоносного программного обеспечения;
- проверка файлов в архивах и файловых контейнерах;
- лечение зараженных объектов;
- предоставление информации о состоянии сканирования на компьютере администратора;
- сбор статистики антивирусной проверки и ее отображение на компьютере администратора;
- высокую скорость проверки;
- возможность регулярного обновления вирусных баз и модулей программы;
- сохранение отчета о проверке удаленных компьютеров в формате XML.

Настоящее руководство призвано помочь системным администраторам организовать и провести антивирусную проверку компьютеров сети с помощью технологий компании **«Доктор Веб»**.





## 1.1. Системные требования

Использование **Dr.Web® CureNet!™** возможно на компьютерах, удовлетворяющих следующим требованиям ([табл. 2](#)).

**Таблица 2. Системные требования.**

Компонент	Требование
Платформа	Полная поддержка системы команд процессора i80386.
Свободная оперативная память	Не менее 256 МБ
Место на жестком диске	Свободного дискового пространства не менее: <ul style="list-style-type: none"><li>• 230 МБ на компьютере, на котором запускается <b>Консоль администрирования</b>, из них до 110 МБ занимает установочный файл;</li><li>• 42 МБ на каждом проверяемом компьютере.</li></ul>
Операционная система	Версии для 32-битных и 64-битных процессоров следующих операционных систем: <ul style="list-style-type: none"><li>• Microsoft® Windows® 2000 с пакетом обновлений SP4 и Update Rollup 1;</li><li>• Windows® XP Professional с пакетом обновлений SP2 или более поздним;</li><li>• Microsoft® Windows Server® 2003 с пакетом обновлений SP1 или более поздним;</li><li>• Windows Vista® (только редакции Business, Enterprise или Ultimate) с пакетом обновлений SP1 или более поздним;</li><li>• Microsoft® Windows Server® 2008;</li><li>• Microsoft® Windows® 7 (только редакции Профессиональная/Professional, Корпоративная/Enterprise или Максимальная/Ultimate)</li><li>• Microsoft® Windows Server® 2008 с пакетом обновлений SP2;</li><li>• Microsoft® Windows® 8;</li><li>• Microsoft® Windows Server® 2012.</li></ul>



Прочее	<p>Подключение компьютера, на котором запускается <b>Консоль администрирования</b>, к сети Интернет для обновления вирусных баз и компонентов <b>Dr.Web CureNet!</b>.</p> <p>Подключение ко всем проверяемым компьютерам по протоколу TCP/IP.</p>
--------	---

Опущенные требования к конфигурации совпадают с таковыми для соответствующих операционных систем.

Запуск **Dr.Web CureNet!** и подключение к удаленным компьютерам должны осуществляться под соответствующими административными учетными записями.

### 1.1.1. Требования к удаленным компьютерам



На проверяемых компьютерах рекомендуется устанавливать все критические обновления операционных систем. Если поддержка операционной системы производителем прекращена, рекомендуется переходить на более современную версию операционной системы.

Во избежание прерывания работы **Dr.Web CureNet!** рекомендуется на время сканирования отключать автоматическое обновление операционной системы.

Для проведения проверки удаленных компьютеров требуется одновременное выполнение следующих условий:

- удаленный компьютер должен быть доступен по сети;
- используемая для подключения учетная запись должна существовать и обладать необходимыми правами;
- если для защиты удаленного компьютера используется брандмауэр, то он должен быть настроен;
- дополнительных условий для конкретных групп операционных систем: новых (начиная с Windows Vista) или старых (Windows XP и более ранние).



## Учетные записи

**Dr.Web CureNet!** позволяет использовать для подключения к удаленным компьютерам следующие административные учетные записи:

- учетная запись на компьютере администратора, под которой запущена **Консоль администрирования** (используется по умолчанию);
- учетные записи администраторов удаленных компьютеров, заданные в **Консоли администрирования**.

Перед началом работы убедитесь, что у вас имеется информация о действующих учетных записях с административными правами на всех удаленных компьютерах, подлежащих проверке.

## Настройка брандмауэров



Если для защиты удаленного компьютера используется брандмауэр стороннего производителя, то в настройках брандмауэра необходимо разрешить доступ по портам 139 и 445.

Для проверки компьютеров, защищенных стандартным Брандмауэром Windows, необходимо настроить данный сетевой фильтр на каждом удаленном компьютере.

### Настройка Брандмауэра Windows

1. Запустите Панель управления на удаленном компьютере. При настройке Windows Vista, Windows 7 или Microsoft Windows Server 2008 выберите режим просмотра по категории.
2. Выполните одно из следующих действий для доступа к настройкам Брандмауэра Windows:



- при настройке Windows XP или Microsoft Windows Server 2003 выберите пункт **Брандмауэр Windows** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**);
  - при настройке Windows Vista выберите пункт **Брандмауэр Windows** и перейдите по ссылке **Разрешить запуск программы через брандмауэр Windows**;
  - при настройке Windows 7 или Microsoft Windows Server 2008 откройте категорию **Система и безопасность**, выберите группу **Брандмауэр Windows** и на навигационной панели окна управления Брандмауэром Windows выберите пункт **Дополнительные параметры**.
3. Внесите следующие изменения в настройки сетевого фильтра:
- при настройке Windows XP, Microsoft Windows Server 2003 или Windows Vista перейдите на вкладку **Исключения** и включите настройку **Общий доступ к файлам и принтерам**;
  - при настройке Windows 7 или Microsoft Windows Server 2008 в дереве консоли выберите группу **Правила для входящих подключений** и включите все правила с названиями **Общий доступ к файлам и принтерам (входящий трафик SMB)** и **Общий доступ к файлам и принтерам (входящий трафик сессии NB)**.
4. Сохраните изменения и закройте окно настроек.

### 1.1.2. Подготовка систем начиная с Windows® Vista®

Для проведения проверки удаленных компьютеров, работающих под управлением операционных систем Windows Vista или Windows 7, требуется одновременное выполнение следующих дополнительных условий:

- ограничения системы контроля учетных записей (UAC) должны быть **отключены**;



- все необходимые для работы сети службы должны быть установлены и настроены;
- параметры общего доступа должны допускать расширенную настройку;
- для локальных учетных записей должна использоваться обычная модель совместного доступа и безопасности.



Все действия по подготовке операционной системы удаленного компьютера к использованию **Dr.Web CureNet!** необходимо проводить под учетной записью с правами администратора.

## Контроль учетных записей

По умолчанию в операционных системах начиная с Windows Vista доступ к удаленному компьютеру под локальной учетной записью запрещен. Подробную информацию об этом ограничении можно найти на официальном сайте Справки и поддержки компании Microsoft по адресу <http://support.microsoft.com/kb/951016> (на английском языке).

Для проведения антивирусной проверки с использованием **Dr.Web CureNet!** на каждом удаленном компьютере, работающем под управлением операционной системы Windows Vista или более поздней, должно быть отключено данное ограничение системы контроля учетных записей (UAC).

## Разрешение удаленного подключения под локальной учетной записью



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.

1. Откройте редактор реестра операционной системы.
2. Найдите и выберите ветку



HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM.

3. 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**.
4. В контекстном меню ключа **LocalAccountTokenFilterPolicy** выберите **Изменить**.
5. В поле **Значение** введите **1**.
6. Нажмите кнопку **ОК** и выйдите из редактора реестра.
7. Перезагрузите компьютер.
8. Повторите операцию для всех удаленных компьютеров, подлежащих проверке.



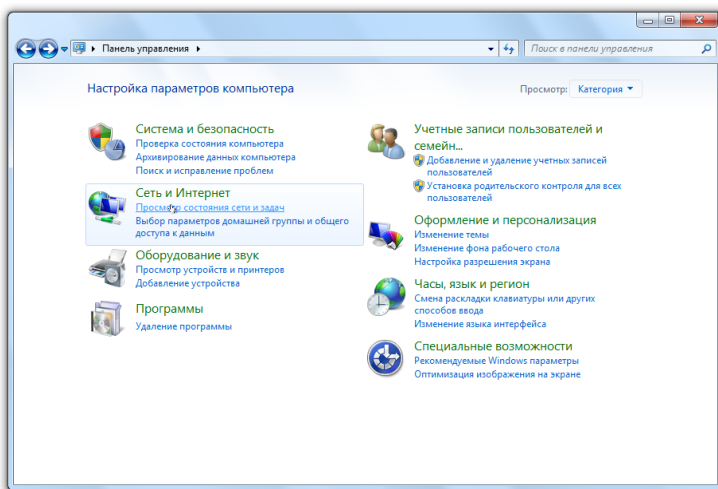
Доступ на удаленные компьютеры, работающие под управлением операционной системы Windows Vista и входящие в домены, возможен также под учетной записью администратора домена. В таком случае снимать запрет на подключение к компьютеру под локальными учетными записями не обязательно.

## Сетевые настройки

Все подлежащие проверке компьютеры должны быть настроены для работы в сети, из которой планируется инициировать проверку.

### Проверка сетевых настроек

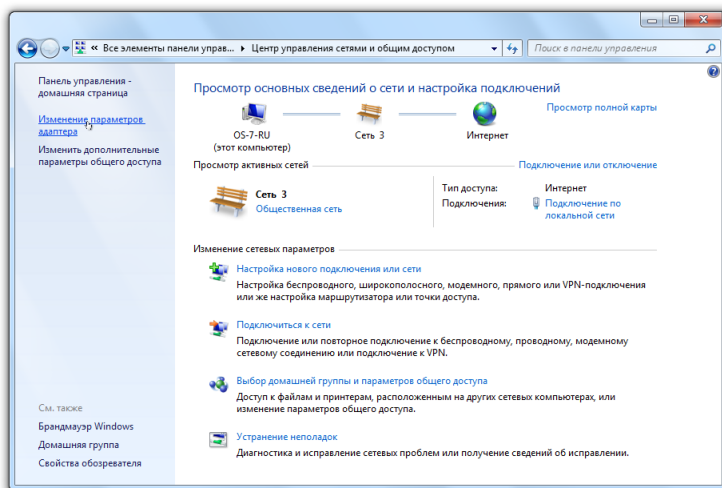
1. Запустите Панель управления на удаленном компьютере и выберите режим просмотра по категории.
2. В категории **Сеть и Интернет** выберите подраздел **Просмотр состояния сети и задач**.



**Рисунок 1. Панель управления: Сеть и Интернет**

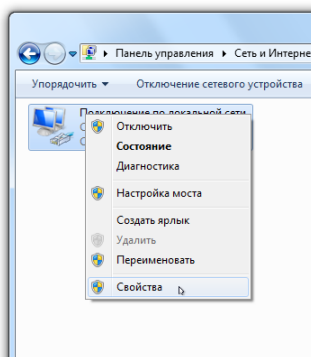
3. Выполните одно из следующих действий:

- при настройке Windows Vista в Центре управления сетями и общим доступом выберите пункт **Управление сетевыми подключениями**;
- при настройке Windows 7 или Microsoft Windows Server 2008 на навигационной панели Центра управления сетями и общим доступом выберите пункт **Изменение параметров адаптера**.



**Рисунок 2. Центр управления сетями и общим доступом**

4. В окне **Сетевые подключения** щелкните правой кнопкой мыши по необходимому подключению и выберите пункт **Свойства**.



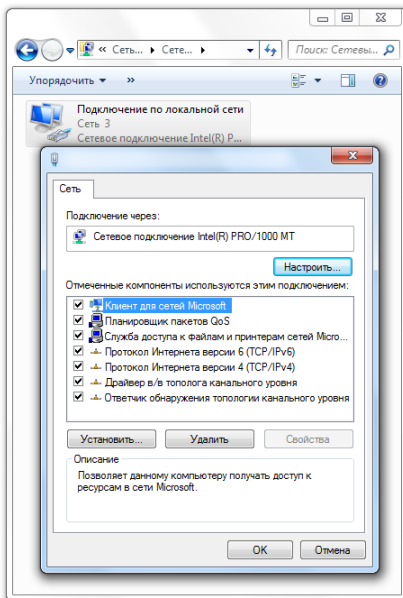
**Рисунок 3. Сетевые подключения**

5. 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).



**Рисунок 4. Свойства подключения**

6. Сохраните изменения и закройте окно настроек.



## Общий доступ

Для доступа **Dr.Web CureNet!** к удаленным компьютерам необходимо включить режим расширенной настройки общего доступа.

### Настройка общего доступа

1. Запустите Панель управления на удаленном компьютере и выберите режим просмотра по категории.
2. В категории **Сеть и Интернет** выберите подраздел **Просмотр состояния сети и задач**.

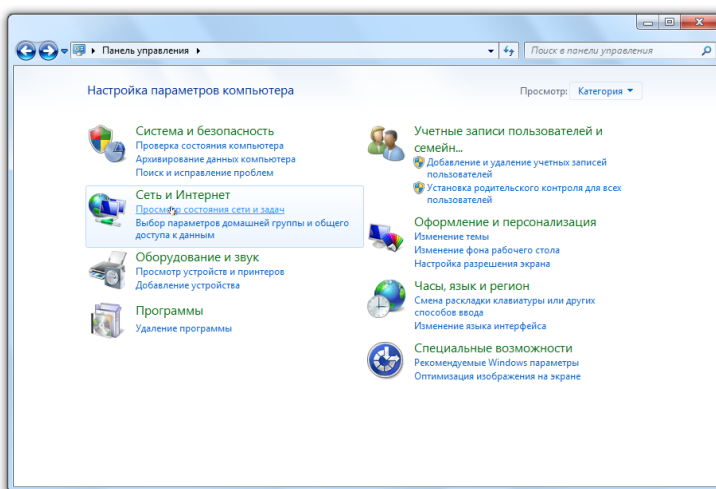


Рисунок 5. Панель управления: Сеть и Интернет

3. Выполните одно из следующих действий:
  - при настройке Windows Vista в Центре управления сетями и общим доступом выберите пункт **Общий доступ и сетевое обнаружение**;



- при настройке Windows 7 или Microsoft Windows Server 2008 на навигационной панели Центра управления сетями и общим доступом выберите пункт **Изменить дополнительные параметры общего доступа**.
4. В окне настроек общего доступа выполните одно из следующих действий:
- при настройке Windows Vista установите **Сетевое обнаружение** и **Общий доступ к файлам**;
  - при настройке Windows 7 в группе **Общий доступ к файлам и принтерам** выберите **Включить сетевое обнаружение** и **Включить общий доступ к файлам и принтерам**;
  - при настройке Microsoft Windows Server 2008 в группе **Общий доступ к файлам и принтерам** выберите **Включить общий доступ к файлам и принтерам**.
5. Сохраните изменения и закройте окно настроек.

## Политика безопасности

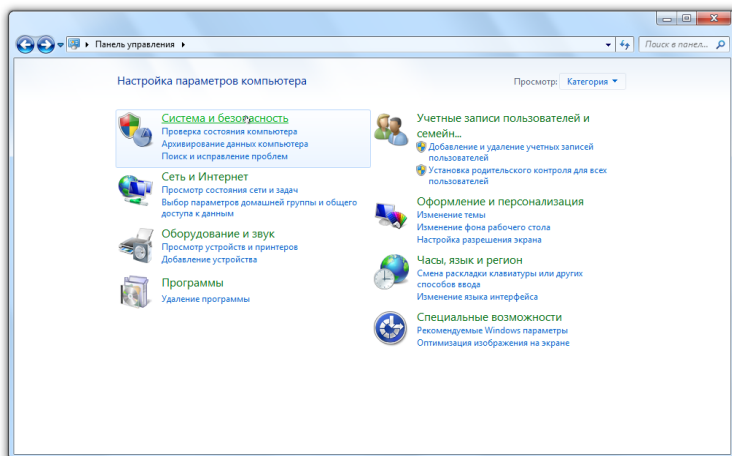
Настройки совместного доступа и безопасности настраиваются с помощью утилиты **Локальная политика безопасности**.

### Настройка модели совместного доступа и безопасности



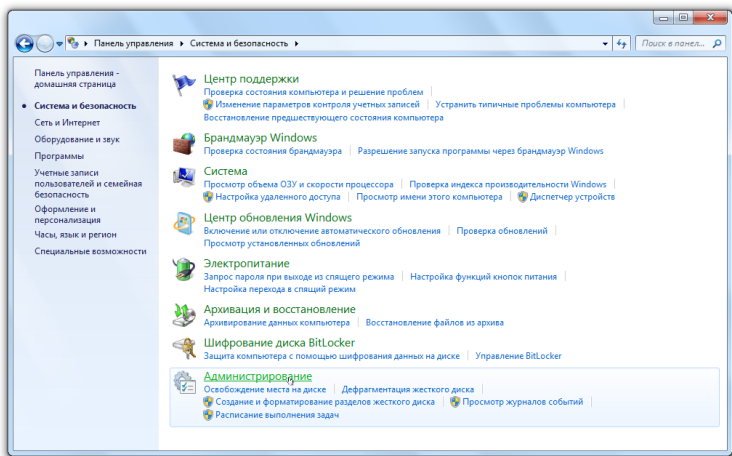
Для запуска утилиты по настройке локальных политик безопасности вы также можете набрать в поле поиска операционной системы Windows команду **secpol.msc** и нажать клавишу ENTER.

1. Запустите Панель управления на удаленном компьютере и выберите режим просмотра по категориям.
2. Откройте категорию **Система и безопасность**.



**Рисунок 6. Панель управления: Система и безопасность**

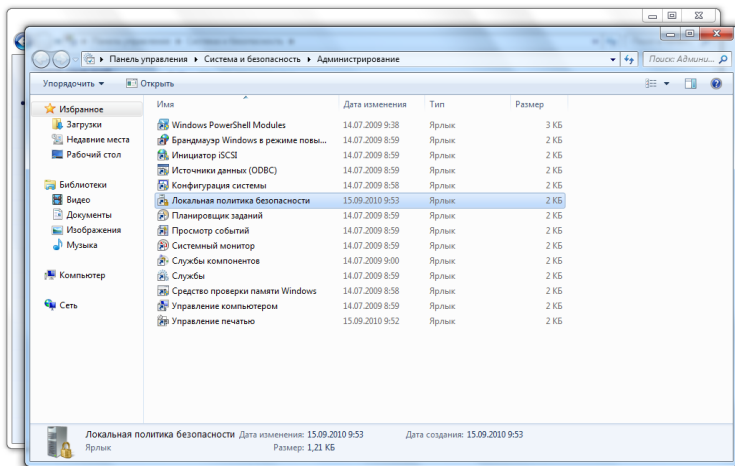
### 3. Выберите группу **Администрирование**.



**Рисунок 7. Администрирование**

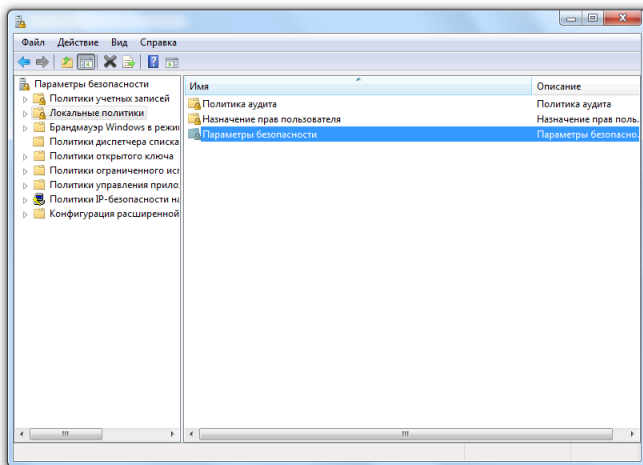


4. Запустите утилиту **Локальная политика безопасности**.



**Рисунок 8. Локальная политика безопасности**

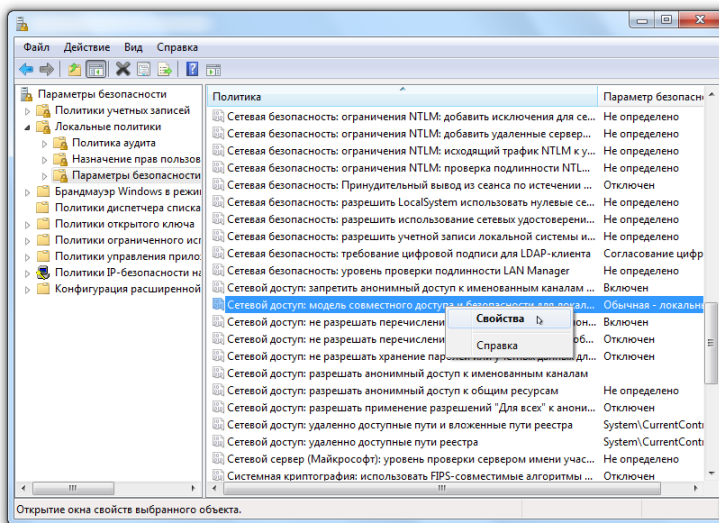
5. В дереве консоли выберите группу **Локальные политики**, а затем – группу **Параметры безопасности**.



**Рисунок 9. Локальные политики**



6. 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**.



**Рисунок 10. Модель совместного доступа и безопасности**

По умолчанию, подключение к удаленной станции может быть установлено, только если используемая учетная запись содержит непустой пароль. Данное ограничение, накладываемое соответствующей политикой безопасности, можно отключить. Для этого в открывшемся окне щелкните правой кнопкой мыши по параметру **Учетные записи: разрешить использование пустых паролей только при консольном входе**, выберите пункт **Свойства** и задайте значение **Отключен**.

7. Закройте консоль.



### 1.1.3. Подготовка систем Windows XP® и более ранних

Для проведения проверки удаленных компьютеров, работающих под управлением операционных систем Windows XP или более ранних, требуется одновременное выполнение следующих дополнительных условий:

- все необходимые для работы сети службы должны быть установлены и настроены;
- параметры общего доступа должны допускать расширенную настройку (не требуется для удаленных компьютеров, работающих под управлением Microsoft Windows Server 2003);
- для локальных учетных записей должна использоваться обычная модель совместного доступа и безопасности (не требуется для удаленных компьютеров, работающих под управлением Microsoft Windows 2000).



Все действия по подготовке операционной системы удаленного компьютера к использованию **Dr.Web CureNet!** необходимо проводить под учетной записью с правами администратора.

## Сетевые настройки

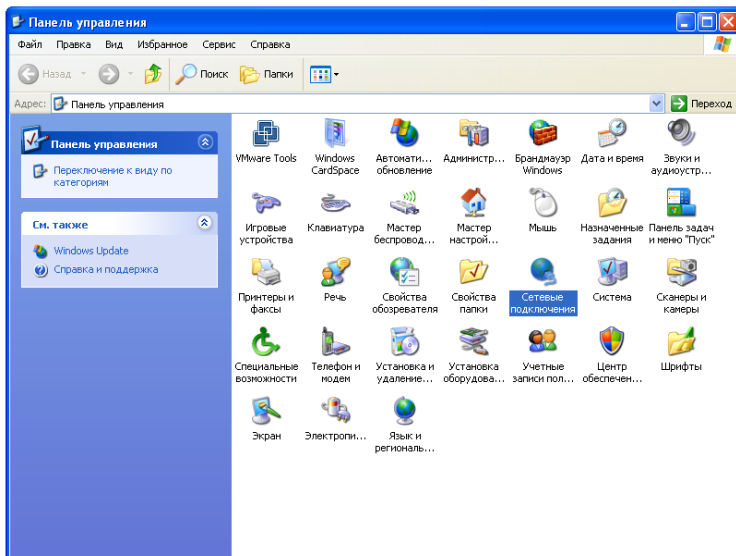
Все подлежащие проверке компьютеры должны быть настроены для работы в сети, из которой планируется инициировать проверку.

### Проверка сетевых настроек

1. Для получения доступа к сетевым настройкам выполните на удаленном компьютере одно из следующих действий:
  - при настройке Microsoft Windows 2000 в меню Пуск выберите пункт **Настройки**, затем пункт **Сеть и удаленный доступ к сети**;



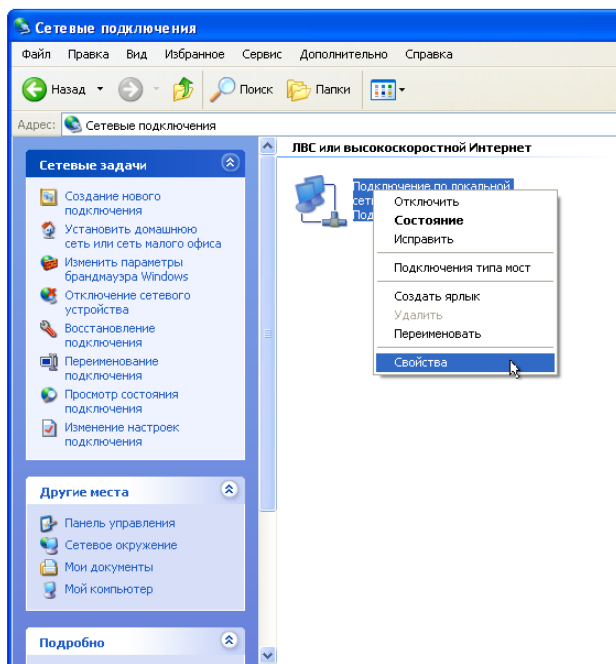
- при настройке Windows XP или Microsoft Windows Server 2003 запустите Панель управления и выберите раздел **Сетевые подключения** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**).



**Рисунок 11. Панель управления Windows XP**

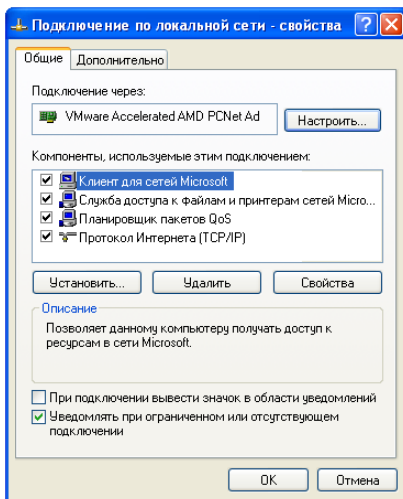
2. Щелкните правой кнопкой мыши по необходимому подключению и выберите пункт **Свойства**.





**Рисунок 12. Сетевые подключения**

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 (TCP/IP).



**Рисунок 13. Свойства подключения**

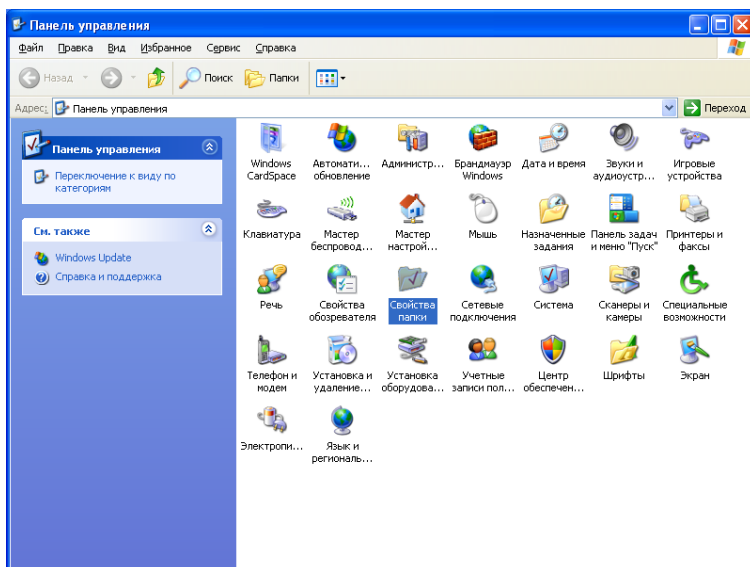
4. Сохраните изменения и закройте окно настроек.

## Общий доступ

Для доступа **Dr.Web CureNet!** к удаленным компьютерам необходимо включить режим расширенной настройки общего доступа.

### Настройка общего доступа

1. Запустите Панель управления на удаленном компьютере.
2. Выберите пункт **Свойства папки** (если раздел отсутствует, нажмите кнопку Переключиться к стандартному виду).



**Рисунок 14. Панель управления**

3. В окне **Свойства папки** перейдите на вкладку **Вид**.
4. Отключите опцию **Использовать простой общий доступ к файлам**.
5. Нажмите кнопку **ОК**.

## Политика безопасности

Настройки совместного доступа и безопасности настраиваются с помощью утилиты **Локальная политика безопасности**.



## Настройка модели совместного доступа и безопасности



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

1. Запустите Панель управления на удаленном компьютере.
2. Выберите пункт **Администрирование** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**).

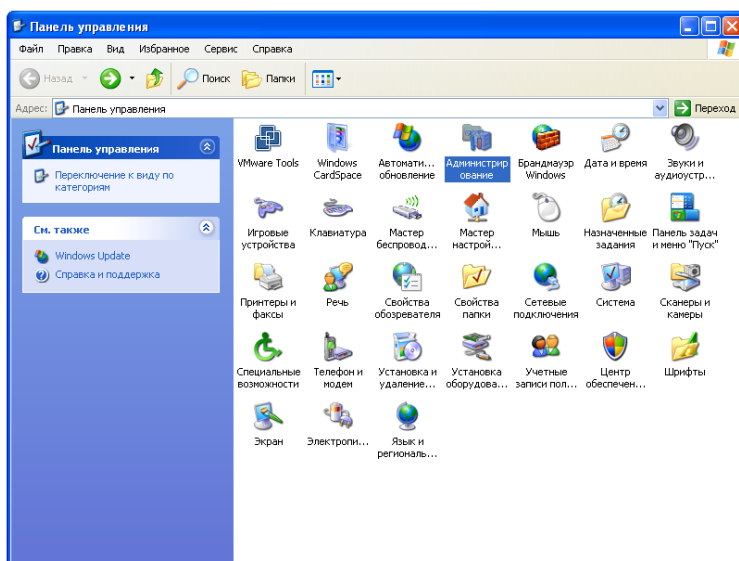
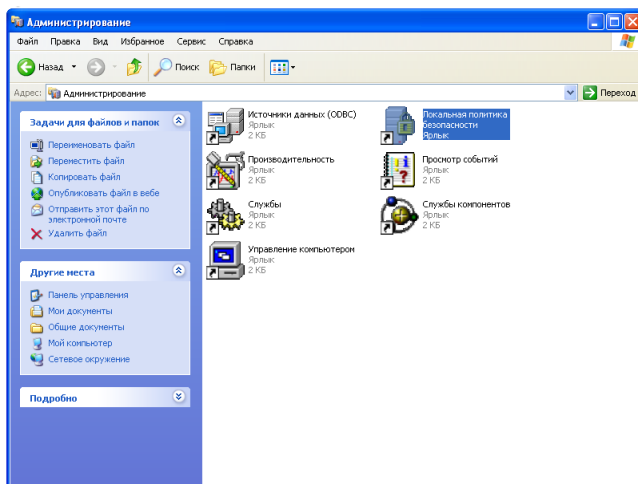


Рисунок 15. Панель управления

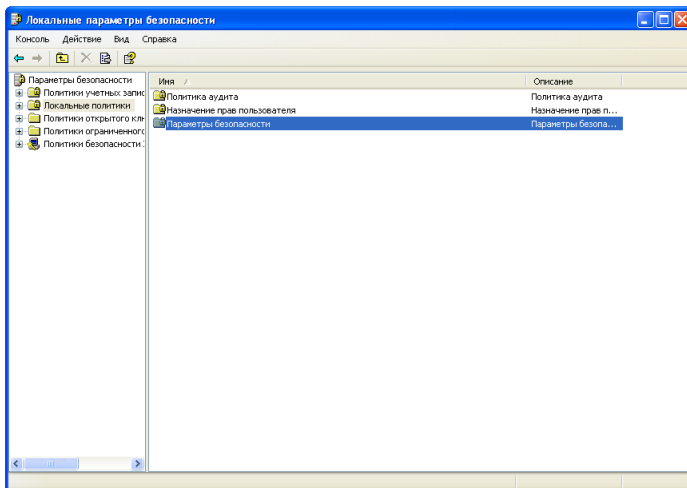


3. Запустите утилиту **Локальная политика безопасности**.



**Рисунок 16. Локальная политика безопасности**

4. В дереве консоли выберите группу **Локальные политики**, а затем – группу **Параметры безопасности**.



**Рисунок 17. Локальные политики**



- Локальные параметры безопасности

Консоль Действие Вид Справка

Параметры безопасности

  - Политики учетных записей
  - Локальные политики
  - Политика аудита
  - Назначение прав по умолчанию
  - Параметры безопасности
  - Политики открытого ключа
  - Политики ограничений
  - Политики безопасности

Политика /

Политика	Параметр безопасности	Значение
Сервер сети Microsoft: использовать цифровую подпись (всегда)	Отключен	
Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)	Отключен	
Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов доступа	Включен	
Сетевая безопасность: минимальная сетевая безопасность для клиентов на базе ...	Минимум нет	
Сетевая безопасность: минимальная сетевая безопасность для серверов на базе ...	Минимум нет	
Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене...	Отключен	
Сетевая безопасность: Принудительный вывод из связи по истечении допустимых ...	Отключен	
Сетевая безопасность: требование подписывания для LDAP клиента	Согласование под...	
Сетевая безопасность: уровень проверки подлинности LAN Manager	Отправлять LM и ...	
Сетевой доступ: модель совместного доступа и политики для локальных учетн...	Гостевая - локаль...	
Сетевой доступ: <b>Свойства</b> ...	исключение учетных записей SAM анонимных пол...	Включен
Сетевой доступ: ...	исключение учетных записей SAM в общи: ресурсо...	Отключен
Сетевой доступ: ...	исключение учетных записей данных или цифровых паспорто...	Отключен
Сетевой доступ: путь в реестре доступных через удаленное подключение	System\CurrentCon...	
Сетевой доступ: разрешать анонимный доступ к именам канала	COM+Object...	
Сетевой доступ: разрешать анонимный доступ к общему ресурсу	COM+FSF...	
Сетевой доступ: разрешать применение разрешений для всех к анонимным пользо...	Отключен	
Системная криптография: использовать FIPS-совместимые алгоритмы для шифрова...	Отключен	
Системные объекты: владение по умолчанию для объектов, созданных членами гру...	Создатель объекта	
Системные объекты: упрощать разрешения по умолчанию для внутренних системных ...	Включен	
Системные объекты: утилизировать регистр для подостен, отличных от Windows	Включен	
Устройства: запретить пользователям установку драйверов принтера	Отключен	
Устройства: поведение при установке компакт-дисков только локальных по...	Успешная установ...	
Устройства: разрешить отставку без входа в систему	Включен	
Устройства: разрешено форматировать и извлекать съемные носители	Администраторы	
Устройства: разрешить доступ к дисководам гибких дисков только локальным по...	Отключен	
Устройства: разрешить доступ к дисководам компакт-дисков только локальным по...	Отключен	
Учетные записи: ограничить использование пустых паролей только для консольно...	Включен	

Открытие окна выбора анонимного объекта.

По умолчанию, подключение к удаленной станции может быть установлено, только если используемая учетная запись содержит непустой пароль. Данное ограничение, накладываемое соответствующей политикой безопасности, можно отключить. Для этого в открывшемся окне щелкните правой кнопкой мыши по параметру **Учетные записи: ограничить использование пустых паролей только для консольного входа**, выберите пункт **Свойства** и задайте значение **Отключен**.

6. Закройте консоль.



## 1.2. Лицензирование

Права пользователя на использование **Dr.Web CureNet!** регулируются при помощи специального файла, называемого *ключевым файлом*.

### Ключевой файл

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 удаленных компьютеров, которые разрешается проверять одновременно, и разрешение на проведение лечения).

Ключевой файл является *действительным* при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится *недействительным*, при этом выдается соответствующее предупреждение, и использование **Dr.Web CureNet!** становится невозможным.

В некоторых случаях для ознакомления с программой можно получить *демонстрационный ключевой файл*. Такие ключевые файлы обеспечивают полную функциональность проверки удаленных компьютеров, но не предполагают проведение действий над обнаруженными зараженными или подозрительными файлами, а также оказание поддержки пользователю.



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


## Получение ключевого файла

Ключевой файл входит в состав дистрибутива продукта при его комплектации. При работе программы ключевой файл должен находиться в той папке **Dr.Web CureNet!**, в которую вы распаковали файлы программы.

## Продление лицензии

В некоторых случаях, например, при окончании срока действия лицензии или при увеличении защищаемой сети, вы можете принять решение о приобретении новой или расширенной лицензии на **Dr.Web CureNet!**.

## Замена ключевого файла

1. Чтобы обновить лицензию, запустите **Консоль администрирования**.
2. На шаге [обновления и профилей](#) 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 «**Доктор Веб**», где вы сможете продлить срок действия лицензии и после этого загрузить обновленную версию дистрибутива **Dr.Web CureNet!**, в котором будет содержаться ваш новый ключевой файл.

3. Закройте **Консоль администрирования** старой версии **Dr.Web CureNet!**, после чего запустите дистрибутив **Dr.Web CureNet!**, чтобы распаковать файлы программы и запустить обновленную **Консоль администрирования**.





## Определение параметров лицензирования

Использование **Dr.Web CureNet!** регулируется ключевым файлом. Параметры лицензии отображаются в окне **О программе Консоли администрирования**. Чтобы отобразить окно, нажмите кнопку **Справка**  и выберите пункт **О программе**.



## 2. Начало работы

**Dr.Web CureNet!** не требует установки и настройки компьютеров. Для начала работы с программой и запуска первой проверки необходимо выполнить следующие действия:

- скопировать на компьютер администратора дистрибутив **Dr. Web CureNet!** и запустить его, после чего файлы программы распаковываются в папку **Dr.Web CureNet!**, автоматически создается репозиторий **Dr.Web CureNet!** и запускается Консоль администрирования;
- убедиться в возможности доступа на удаленные компьютеры, подлежащие проверке.

В дальнейшем в **Консоли администрирования** вы можете запустить обновление **Репозитория Dr.Web CureNet!**.

### 2.1. Консоль администрирования

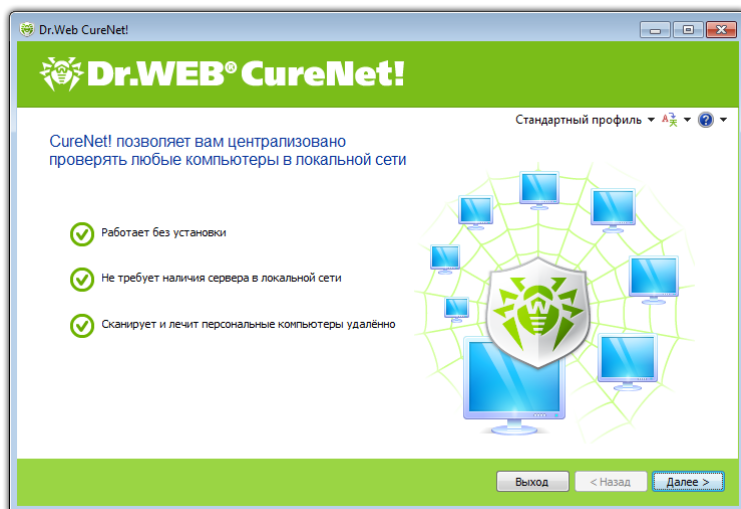
Административным компонентом **Dr.Web® CureNet!™** является **Консоль администрирования** (CureNet.exe), которая представляет собой обычное пользовательское приложение с графическим интерфейсом и позволяет настраивать и запускать антивирусную проверку удаленных компьютеров, а также обновлять имеющиеся на компьютере администратора **вирусные базы Dr.Web** и компоненты программы.

**Консоль администрирования** включает следующие компоненты:

- модуль обновления, позволяющий поддерживать актуальность **вирусных баз Dr.Web** на компьютере администратора, а также загружать с **официального сайта компании «Доктор Веб»** последние обновления исполняемых файлов и библиотек программы;
- сканер сети, позволяющий как автоматически обнаруживать все подключенные к сети компьютеры, так и вручную добавлять IP-адреса компьютеров, подлежащих проверке;



- модуль управления списком учетных записей, под которыми выполняется антивирусная проверка удаленных компьютеров.



**Рисунок 19. Консоль администрирования Dr.Web CureNet!**

Для запуска проверки на удаленных компьютерах **Dr.Web CureNet!** использует специальный **Сервис сканирования**, который является приложением без графического интерфейса и выполняется в фоновом режиме с высоким приоритетом на удаленных компьютерах. **Сервис сканирования** реализует следующие функции:

- запуск антивирусной проверки на удаленном компьютере;
- контроль процесса проверки;
- сбор и отправку статистики проверки на компьютер администратора.

**Консоль администрирования** запускается автоматически после распаковки дистрибутива **Dr.Web CureNet!**.



## 2.2. Репозиторий Dr.Web CureNet!

**Репозиторий Dr.Web CureNet!** хранится в подкаталоге Repository каталога **Dr.Web CureNet!** и содержит все файлы, необходимые для проведения антивирусной проверки:

- **Сканер Dr.Web** (drweb32w.exe);
- основные **вирусные базы Dr.Web** (drwebbase.vdb, drwnasty.vdb, drwrisky.vdb);
- дополнения вирусных баз (файлы \*.vdb), включая последние дополнения (drwtoday.vdb, dwntoday.vdb, dwrtoday.vdb);
- **ядро Dr.Web** (drweb32.dll).

При запуске проверки из **Консоли администрирования** файлы из **Репозитория** копируются на удаленные компьютеры.

**Репозиторий** создается автоматически при распаковке дистрибуционного архива **Dr.Web CureNet!** и обновляется только через **Консоль администрирования**. Создание или обновление **Репозитория** вручную не допускается.

## 2.3. Методы обнаружения вирусов

Все антивирусы **Dr.Web** одновременно используют несколько методов обнаружения вредоносных объектов, что позволяет максимально тщательно проверить подозрительные файлы:

1. В первую очередь применяется *сигнатурный* анализ. Он выполняется путем анализа кода подозрительных файлов на предмет соответствия сигнатурам известных вирусов (*сигнатурой* называется непрерывная конечная последовательность байт, необходимая и достаточная для опознания вируса). При этом сравнение проводится по контрольным суммам сигнатур, что позволяет значительно снизить размер записей в вирусных базах данных, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения и лечения зараженных файлов. **Вирусные базы Dr.Web** составлены таким образом, что



благодаря одной записи можно обнаруживать целые классы угроз.

2. После завершения сигнатурного анализа применяется уникальная технология **Origins Tracing**, которая позволяет определить новые или модифицированные вирусы, использующие известные механизмы заражения файлов. Так, например, эта технология защищает пользователей антивирусных решений **Dr.Web** от таких вирусов, как вирус-шантажист Trojan.Encoder.18 (также известный под названием grcode). Кроме того, именно введение **Origins Tracing™** позволяет значительно снизить количество ложных срабатываний эвристического анализатора.
3. Работа эвристического анализатора основывается на неких знаниях (*эвристиках*) о характерных признаках вирусного и, наоборот, безопасного кода. Каждый признак имеет определенный вес (число, показывающее серьезность и достоверность данного признака). На основании суммарного веса, характеризующего каждый конкретный файл, эвристический анализатор вычисляет вероятность заражения файла неизвестным вирусом. Как и любая система проверки гипотез в условиях неопределенности, эвристический анализатор может допускать ошибки как первого (пропуск неизвестных вирусов), так и второго рода (ложная тревога).



## 2.4. Режимы работы

Программа позволяет проводить проверку в демонстрационном или основном режиме. Режим работы программы зависит от типа [ключевого файла](#), входящего в состав дистрибуционного пакета.

### Демонстрационный режим

В этом режиме доступна вся функциональность проверки удаленных компьютеров на вирусы. Вы можете [выбирать станции](#), задавать [тип проверки](#), а также ознакомиться с возможной [реакцией Dr.Web CureNet!](#) на обнаружение зараженных или подозрительных файлов. Информация о результатах проверки предоставляется в [отчете](#) о работе **Dr.Web CureNet!**.

В данном режиме лечение зараженных файлов и проведение любых других действий над обнаруженными угрозами недоступно.

### Основной режим

В этом режиме доступна вся функциональность программы, включая проведение действий над обнаруженными зараженными и подозрительными объектами на удаленных компьютерах.



## 3. Антивирусная проверка

Проверка удаленных компьютеров настраивается и инициируется с компьютера администратора при помощи **Консоли администрирования**.



Во избежание прерывания работы **Dr.Web CureNet!** рекомендуется на время сканирования отключать автоматическое обновление операционной системы.

### Запуск проверки

1. Запустите **Консоль администрирования**.
2. На первом шаге нажмите кнопку **Далее**.
3. На шаге обновления и профилей выберите предварительно сохраненный **профиль проверки** (по умолчанию, **Стандартный профиль**).
4. При необходимости выполните **обновление**:
  - чтобы загрузить с официального сайта компании **«Доктор Веб»** последние обновления вирусных баз и модулей сканирования, нажмите кнопку **Обновить**;
  - чтобы заново **загрузить** дистрибутив **Dr.Web CureNet!**, нажмите на **Мой Dr.Web**.



При значительном устаревании **вирусных баз Dr.Web** на этом шаге отображается соответствующее предупреждение.

4. Если вы выбрали обновление вирусных баз, дождитесь завершения загрузки обновлений. Если вы загрузили новую версию дистрибутива **Dr.Web CureNet!**, закройте **Консоль администрирования** старой версии и запустите новый дистрибутив. Для продолжения работы нажмите кнопку **Далее**.
5. На шаге формирования списка станций выполните следующие действия:



- укажите удаленные компьютеры, которые подлежат проверке;
- сформируйте список учетных записей, под которыми **Dr.Web CureNet!** будет подключаться к указанным компьютерам.

После завершения выбора и настройки нажмите кнопку **Далее**.

6. На шаге выбора типа проверки укажите режим сканирования и при необходимости измените следующие настройки **Сканера Dr.Web**:
  - общие настройки работы удаленных компьютеров при проверке (оповещение пользователей и перезагрузка проверенных компьютеров и т.п.);
  - проверка архивов и контейнеров;
  - реакция на обнаружение определенных типов вирусных угроз на удаленных компьютерах;
  - режим работы сети во время сканирования и проверка доступности удаленных компьютеров перед началом копирования файлов **Dr.Web CureNet!**;
  - параметры сетевого подключения, которое используется для обновления **Репозитория Dr.Web CureNet!**.

После завершения настройки нажмите кнопку **Начать**.

**Dr.Web CureNet!** инициирует копирование файлов из **Репозитория Dr.Web CureNet!** на выбранные компьютеры (при условии их доступности). По окончании копирования на каждом удаленном компьютере запускается антивирусная проверка и, если установлена соответствующая настройка, выводится оповещение в области уведомлений Windows.

7. Процесс и результаты проверки отображаются в отчете о работе **Dr.Web CureNet!**. При необходимости вы можете сохранить отчет в файле формата XML.





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

## 3.1. Профили проверки

**Dr.Web CureNet!** позволяет сохранять все настройки сканирования в файлах профилей.

### Создание нового профиля проверки

- На любом шаге проверки нажмите название профиля в верхней части окна (по умолчанию, **Стандартный профиль**) и выберите пункт **Сохранить**.

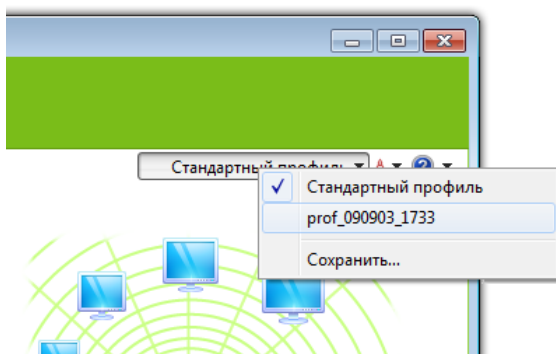
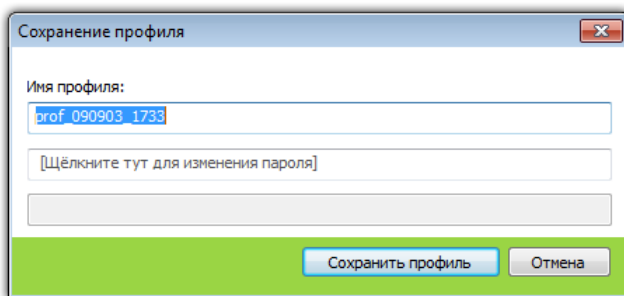


Рисунок 20. Профили проверки.

- В окне **Сохранение профиля** введите имя нового профиля проверки и при необходимости пароль доступа к данному профилю.



Пароль доступа к профилю требуется при сохранении **паролей для подключения** к удаленным компьютерам.



**Рисунок 21. Сохранение профиля.**

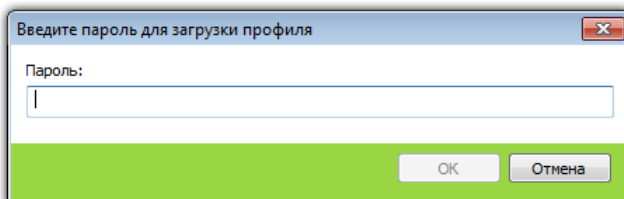
3. Нажмите кнопку **Сохранить профиль**.
4. Перейдите к следующим шагам проверки или нажмите кнопку **Выход**.



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

## Задание профиля проверки

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



**Рисунок 22. 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 проверки

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

## 3.2. Выбор станций

На этом шаге вы можете выбрать удаленные компьютеры, подлежащие проверке, и указать параметры подключения к ним.

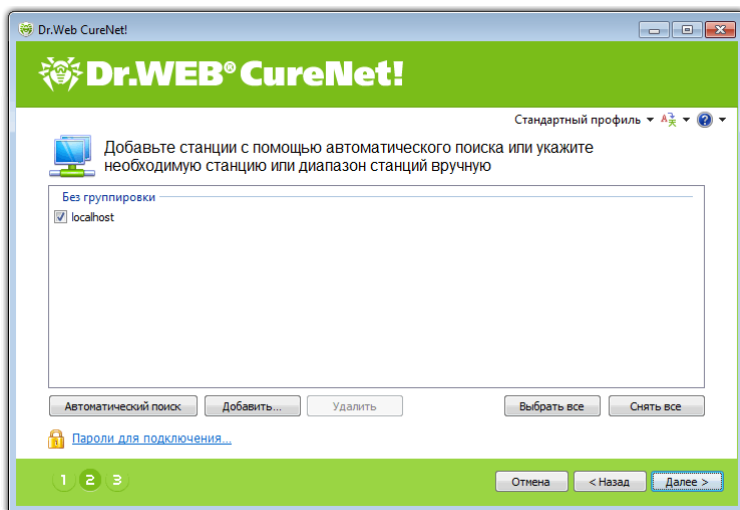


Рисунок 23. Выбор компьютеров для проверки.

**Dr.Web CureNet!** позволяет добавлять компьютеры к проверке как вручную, так и при помощи автоматического поиска во всех сетях, доступных с компьютера, на котором запущена **Консоль администрирования**.



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

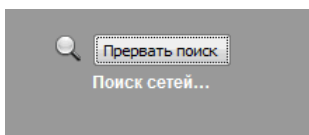
## Автоматический поиск компьютеров

1. Чтобы найти все доступные по сети компьютеры, нажмите кнопку **Автоматический поиск**.

Поиск всех станций может занять длительное время. Чтобы завершить поиск, нажмите кнопку **Прервать поиск**. Все компьютеры, обнаруженные на момент завершения поиска, будут добавлены в список станций.

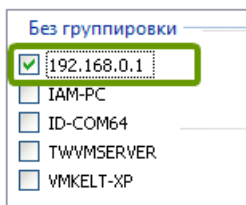


Если в процессе поиска компьютер не был найден, добавьте его [вручную](#).



**Рисунок 24. Автоматический поиск компьютеров.**

2. Выберите компьютеры, подлежащие проверке:
  - чтобы добавить к проверке определенный компьютер, установите флажок рядом с его именем или IP-адресом в списке станций;



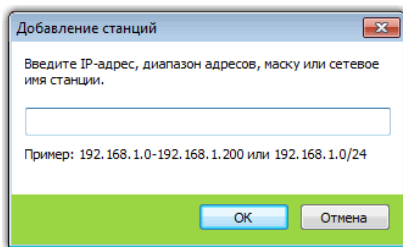
**Рисунок 25. Выбор компьютера для проверки.**



- чтобы добавить к проверке все компьютеры из списка, нажмите кнопку **Выбрать все**;
  - чтобы снять выделение со всех компьютеров и начать выбор заново, нажмите кнопку **Снять все**.
3. После завершения выбора сформируйте список учетных записей, под которыми **Dr.Web CureNet!** будет подключаться к указанным компьютерам. По умолчанию подключение происходит под учетной записью, под которой запущена **Консоль администрирования**. Если подключение под этой учетной записью невозможно, то используются записи из списка.

### Добавление компьютеров вручную

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



**Рисунок 26. Добавление компьютеров вручную.**



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

Нажмите кнопку **ОК**.



3. Компьютеры, добавленные к списку станций вручную, автоматически выбираются для проверки. При необходимости снимите флажки у компьютеров, которые вы хотите исключить из проверки.
4. После завершения выбора **сформируйте** список учетных записей, под которыми **Dr.Web CureNet!** будет подключаться к указанным компьютерам. 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 станции из списка

1. Чтобы удалить компьютер из списка станций, щелкните по его имени или IP-адресу в списке станций.

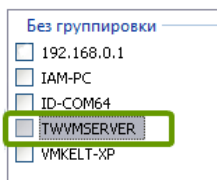


Рисунок 27. Выбор компьютера для удаления.

2. Нажмите кнопку **Удалить**.

### 3.2.1. Настройка списка учетных записей

Список учетных записей позволяет задать имена пользователей и пароли для доступа к удаленным компьютерам. Эти учетные записи используются для копирования необходимых файлов и запуска **Сканера Dr.Web** на проверяемых компьютерах.

По умолчанию подключение происходит с правами учетной записи, под которой запущена **Консоль администрирования**. Если подключение под этой учетной записью невозможно, **Dr.Web CureNet!** пытается подключиться к удаленным компьютерам, последовательно используя указанные в списке учетные записи.



## Настройка списка учетных записей

1. Чтобы отобразить список учетных записей, на шаге формирования списка станций нажмите на **Пароли для подключения**. Откроется окно **Учетные записи и пароли**.
2. Выполните одно из следующих действий:
  - чтобы добавить учетную запись в список, введите имя пользователя и пароль и нажмите кнопку **Добавить**;

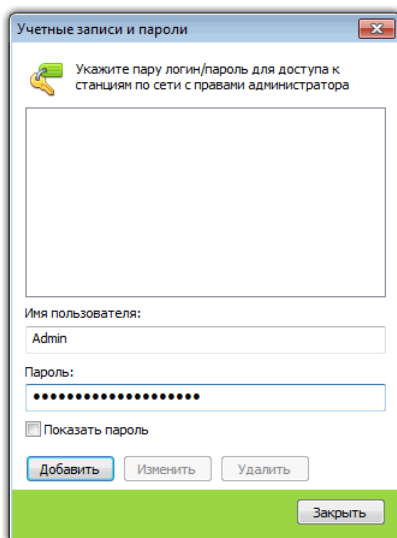


Имя пользователя необходимо указывать в одном из следующих форматов:

- **<домен>\<имя пользователя>**, где **<домен>** - имя домена, имеющего указанную учетную запись;
- **<компьютер>\<имя пользователя>**, где **<компьютер>** - сетевое имя компьютера, имеющего указанную учетную запись.

Если все удаленные компьютеры, которые вы хотите проверить, находятся вне доменов и имеют одинаковую административную учетную запись, то для ускорения подключения рекомендуется добавить к списку только эту общую учетную запись, опустив при этом имя компьютера. **Dr.Web CureNet!** автоматически попытается подключиться ко всем компьютерам под этой учетной записью.

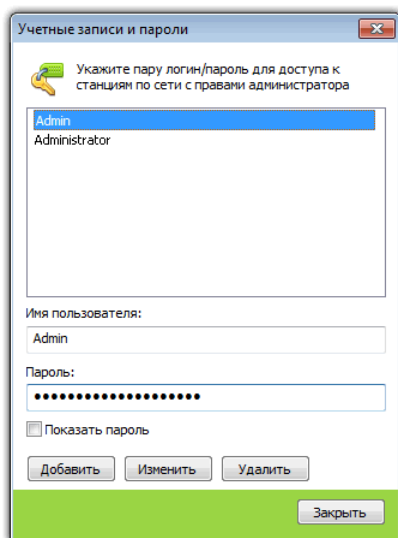
Данный способ подходит только для сетей с корректной конфигурацией.



**Рисунок 28. Добавление учетной записи.**

- чтобы удалить учетную запись из списка, выберите соответствующую строку в списке и нажмите кнопку **Удалить**;
- чтобы отредактировать учетную запись, выберите соответствующую строку в списке, измените имя пользователя и/или пароль и нажмите кнопку **Изменить**;
- чтобы повторно создать учетную запись с другим паролем, выберите имя пользователя в списке, введите новый пароль и нажмите кнопку **Добавить**.





**Рисунок 29. Управление учетной записью.**



Для контроля вводимого пароля установите флажок **Показать пароль**.

3. После завершения редактирования списка нажмите кнопку **Заккрыть**.



### 3.3. Настройка действий

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

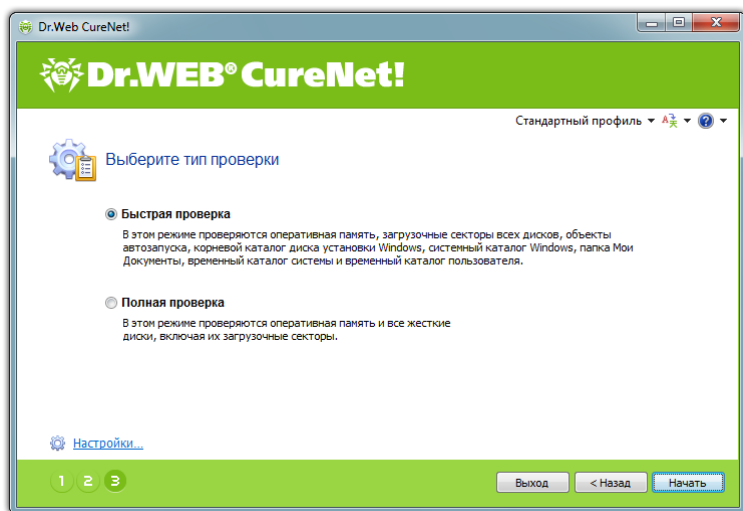


Рисунок 30. Выбор типа проверки.

#### Тип проверки

По умолчанию после копирования файлов **Dr.Web CureNet!** запускает на удаленном компьютере **Сканер Dr.Web**, который выполняет быструю проверку (тип **Быстрая**). В данном режиме производится сканирование 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.

Архивированные файлы в данном режиме не сканируются.

Вы можете выбрать режим полной проверки (тип **Полная**), при котором производится сканирование оперативной памяти и всех жестких дисков, включая их загрузочные секторы.



Полная проверка удаленных компьютеров может занять длительное время, при этом процесс сканирования не зависит от **Консоли администрирования**, поэтому после запуска проверки у вас не будет возможности ее остановить.

## 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 **Настройки сканера Dr.Web**, нажмите на **Настройки**.
2. Задайте нужные параметры на следующих вкладках:
  - [Общие](#)
  - [Типы файлов](#)
  - [Действия](#)
  - [Сеть](#)



- [Прокси](#)

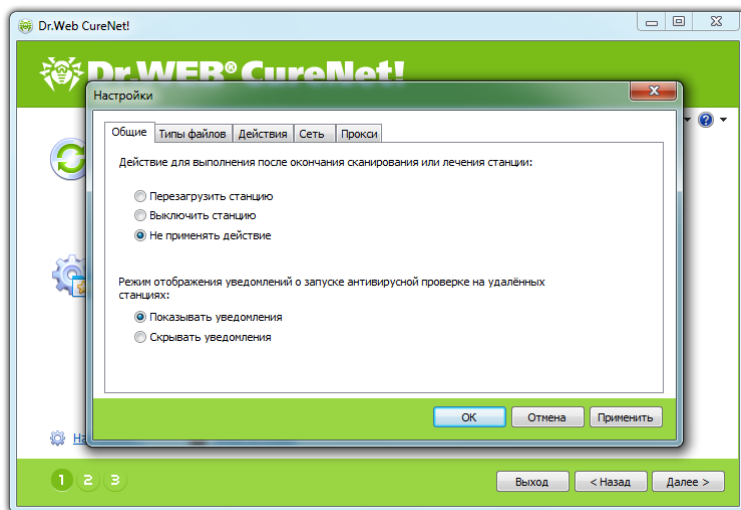
При необходимости нажимайте кнопку **Применить**.

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

Изменение настроек имеет силу только в данном сеансе работы **Dr.Web CureNet!**. При повторном запуске утилиты все настройки автоматически возвращаются к первоначальным значениям. Используйте [профили проверки](#) для сохранения настроек сканирования.

### 3.3.1. Вкладка Общие

На этой вкладке вы можете указать общие настройки работы удаленных компьютеров при проверке с помощью **Dr.Web CureNet!**.



**Рисунок 31. Настройка Dr.Web CureNet!. 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 удаленном компьютере автоматически, при этом пользователю удаленного компьютера выводится соответствующее предупреждение и выделяется время на завершение работы и сохранение информации. Перезагрузка выполняется один раз после завершения сканирования.

Режим **Не применять действия** позволяет пользователям продолжать работу без перезагрузки, но не гарантирует успешного завершения лечения некоторых инфекций.

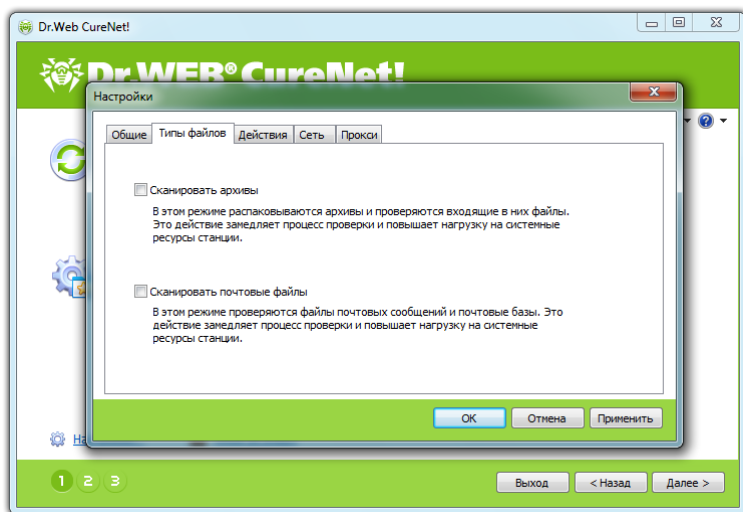


При обнаружении вирусов в главной загрузочной записи операционной системы (MBR) **Сканер Dr.Web** применяет обязательную перезагрузку удаленного компьютера непосредственно после обнаружения вируса и восстановления записи (так называемая «жесткая» перезагрузка). Такая перезагрузка выполняется вне зависимости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

**Dr.Web CureNet!** по умолчанию оповещает пользователей удаленных компьютеров о начале проверки при помощи подсказок-уведомлений, появляющихся в виде всплывающего окна в области уведомлений Windows. Чтобы не оповещать пользователей, выберите режим **Скрывать уведомления**.

### 3.3.2. Вкладка Типы файлов

На этой вкладке вы можете указать дополнительные типы файлов для проверки **Сканером Dr.Web** на удаленном компьютере.



**Рисунок 32. Настройка Dr.Web CureNet!. Вкладка Типы файлов.**

При необходимости вы можете выбрать следующие режимы:

- **Сканировать архивы** - выберите этот режим, чтобы проверять файлы в архивах;
- **Сканировать почтовые файлы** - выберите этот режим, чтобы проверять файлы почтовых клиентов.



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

Включение режимов сканирования архивов или почтовых файлов может значительно замедлить процесс проверки.

Во время **Быстрой** проверки файлы в архивах не проверяются.



### 3.3.3. 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 о наличии угроз.

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

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

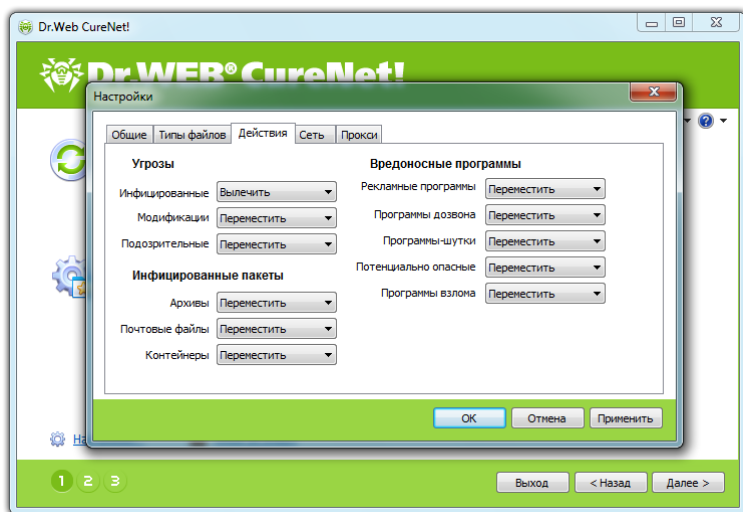
Реакция задается отдельно для каждой категории объектов:

- **Инфицированные** объекты, зараженные известным и (предположительно) излечимым вирусом;
- **Неизлечимые** объекты, зараженные неизлечимым вирусом;
- **Подозрительные** объекты, 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.



**Рисунок 33. Настройка Dr.Web CureNet!. Вкладка Действия.**

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

- **Вылечить** (доступна только для инфицированных объектов) – предписывает **Сканеру Dr.Web** пытаться излечить объект, зараженный известным вирусом. Если вирус неизлечим или попытка лечения не была успешной, будет отработана реакция, заданная для неизлечимых объектов;
- **Переместить** – (невозможна для загрузочных секторов) предписывает переместить вредоносный или подозрительный объект в каталог карантина Quarantine, расположенный на удаленном компьютере в каталоге %ALLUSERSPROFILE%\DoctorWeb\CureNet\;
- **Игнорировать** – (доступна только для вредоносных программ) – не выводить информацию об обнаружении вредоносной программы в отчете о работе **Dr.Web CureNet!**;





- **Информировать** – вывести информацию о вредоносном или подозрительном объекте в [отчете](#) о работе **Dr.Web CureNet!**.

### 3.3.4. Вкладка Сеть

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

При необходимости вы можете выбрать следующие режимы:

- **Блокировать сеть во время сканирования** - выберите этот режим, чтобы на время проверки запретить взаимодействие по сети на удаленном компьютере и избежать его повторного заражения;
- **Разрывать существующие соединения NetBIOS** - выберите этот режим, чтобы перед началом проверки прерывать подключения вашего компьютера к тем удаленным компьютерам, которые вы выбрали для проверки (необходимо для корректного копирования файлов и запуска **Сканера Dr.Web**);
- **Проверять доступность станций перед установкой (ping)** - выберите этот режим, чтобы перед началом копирования файлов проверять доступность удаленного компьютера по сети с использованием утилиты ping.

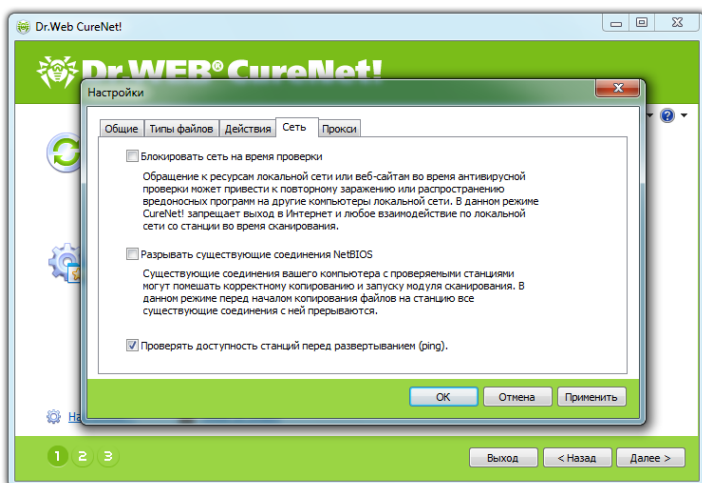


Рисунок 34. Настройка Dr.Web CureNet!. Вкладка Сеть.

### 3.3.5. Вкладка Прокси

На этой вкладке вы можете указать параметры сетевого подключения, которое используется для обновления **Репозитория Dr.Web CureNet!**.

## 3.4. Отчет о работе Dr.Web CureNet!

На шаге **Статистика работы** отображаются текущие сведения о работе **Сканера Dr.Web** на всех проверяемых удаленных компьютерах. Сбор статистики не зависит от качества связи между компьютером, на котором запущена **Консоль администрирования**, и проверяемыми компьютерами. При кратковременной утере связи с удаленным компьютером после начала процесса сканирования **Dr.Web CureNet!** 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 удаленных компьютеров.

Секция **Станций** включает следующую информацию:

- **Задано** – общее количество заданных к проверке компьютеров;
- **Найдено** – количество доступных по сети компьютеров;
- **Не найдено** – количество недоступных по сети компьютеров;
- **Доставлено** – количество удаленных компьютеров, к которым удалось успешно подключиться и скопировать файлы **Dr.Web CureNet!**;
- **Ошибок доставки** – количество удаленных компьютеров, к которым не удалось подключиться и/или скопировать файлы **Dr.Web CureNet!**;
- **Выполняется** – количество все еще проверяемых удаленных компьютеров;
- **Завершено** – количество уже проверенных удаленных компьютеров;
- **Вылечено** – общее количество полностью вылеченных компьютеров, на которых все вредоносные объекты были обезврежены;
- **Перезагружено** – общее количество компьютеров, перезагруженных для корректного завершения лечения.

Секция **Объектов** включает следующую информацию:

- **Проверено** – общее количество проверенных объектов на всех удаленных компьютерах;
- **Угроз** – общее количество вирусных угроз, обнаруженных на всех удаленных компьютерах;
- **Обезврежено** – общее количество объектов, вылеченных на всех удаленных компьютерах;
- **Ошибок проверки** – общее количество ошибок проверки.

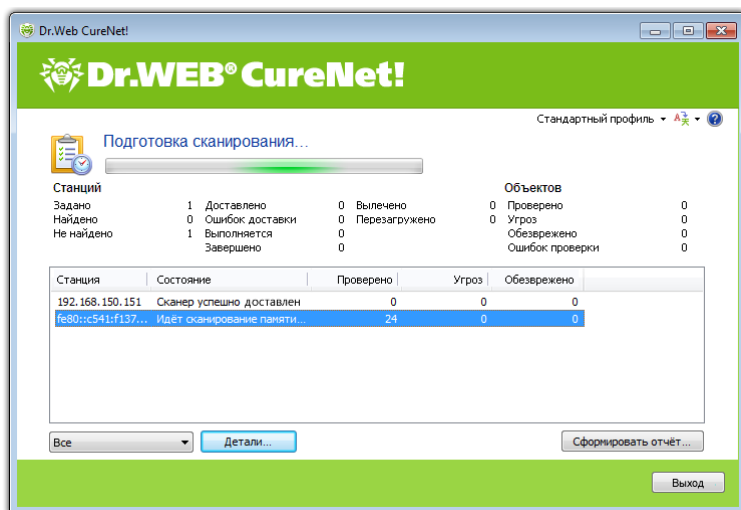


Рисунок 35. Отчет о работе Dr.Web CureNet!.

В поле отчета в табличной форме представлены сведения о ходе сканирования удаленных компьютеров:

- колонка таблицы **Станция** содержит наименование или адрес удаленного компьютера;
- колонка таблицы **Состояние** содержит статус проверки удаленного компьютера (установка, процент выполнения проверки, сообщение об ошибке сканирования или недоступности компьютера и пр.);
- колонка таблицы **Проверено** содержит общее количество проверенных объектов на удаленном компьютере;
- колонка таблицы **Угрозы** содержит общее количество обнаруженных угроз информационной безопасности;
- колонка таблицы **Обезврежено** содержит 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 сканирования и состояния удаленного компьютера.



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). Сканирование удаленного компьютера при этом завершается досрочно.

В отчете о работе **Dr.Web CureNet!** о подобной перезагрузке свидетельствует досрочное завершение сканирования зараженного компьютера по сравнению со всеми остальными компьютерами, а также информация о вирусе в главной загрузочной записи операционной системы, доступная в окне [статистики компьютера](#).

Для окончания проверки компьютеров, зараженных MBR-вирусами, необходимо повторно запустить сканирование с использованием **Консоли администрирования**.

## Просмотр статистики станции

Чтобы получить более подробные сведения о проверке конкретного удаленного компьютера в отдельности, выполните одно из следующих действий:

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

Откроется окно [статистики компьютера](#).

## Сохранение отчета

Для сохранения отчета в файле формата XML нажмите на **Сформировать отчет**.

### 3.4.1. Статистика компьютера

В окне статистики станции собраны итоговые сведения о работе **Сканера Dr.Web** на выбранном удаленном компьютере.



При возникновении ошибок в процессе копирования файлов **Dr. Web CureNet!** на удаленный компьютер или потере связи при проверки в данном окне выводятся соответствующие предупреждения.

Раздел **Угрозы** включает следующую информацию о проверенных объектах на удаленном компьютере:

- количество обнаруженных объектов, инфицированных известными вирусами;
- количество обнаруженных неизлечимых объектов;
- количество обнаруженных подозрительных объектов;
- количество обнаруженных рекламных программ;
- количество обнаруженных программ дозвона, перенаправляющих звонок модема на заранее запрограммированный платный номер или платный ресурс;
- количество обнаруженных программ-шутков;
- количество обнаруженных потенциально опасных программ;
- количество обнаруженных программ взлома.

Раздел **Действия** отражает итоговые сведения о действиях программы над зараженными и подозрительными объектами:

- количестве вылеченных объектов;
- количестве удаленных объектов;
- количестве переименованных объектов;
- количестве перемещенных объектов;
- количестве проигнорированных объектов.

Раздел **Статистика** отражает информацию о количестве проверенных объектов и объеме обработанных данных на удаленном компьютере.

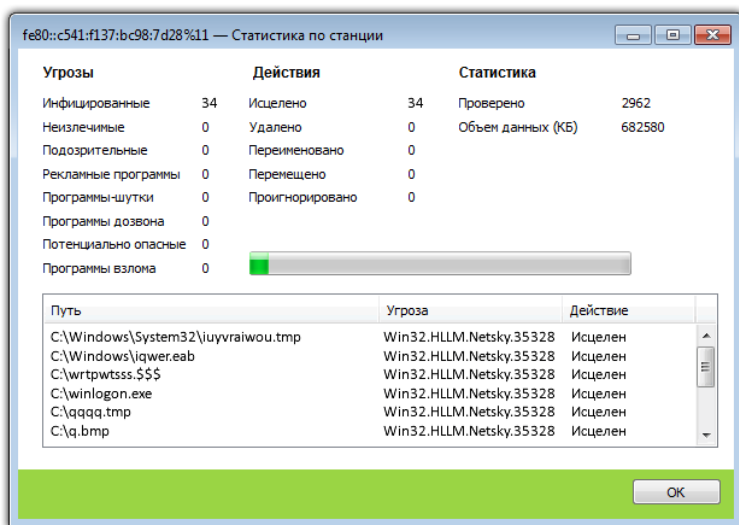


Рисунок 36. Отчет о работе. Статистика компьютера.

В нижней части окна отчета в табличной форме представлены конкретные сведения об обнаруженных вредоносных объектах, а также о произведенном **Сканером Dr.Web** действии над ними:

- колонка таблицы **Путь** содержит путь к инфицированному объекту и его наименование;
- колонка таблицы **Угроза** содержит условное наименование вируса (для файлов и загрузочных секторов) или сообщение об инфицированности архива;
- колонка таблицы **Действие** содержит сообщение о выполненных действиях (излечении, удалении, переименовании или перемещении объекта).

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



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 компьютера и выводит соответствующее оповещение в отчете. Для корректной обработки подобных объектов вы можете разрешить **Сканеру Dr.Web** перезагружать операционные системы проверенных компьютеров при необходимости или выключать их автоматически после окончания сканирования. При этом пользователю удаленного компьютера будет выводиться соответствующее предупреждение и выделяться время на завершение текущей работы и сохранение информации.

Подробнее о настройке действий над вредоносными объектами см. [Дополнительная настройка](#) действий.

При обнаружении вирусов в главной загрузочной записи операционной системы (MBR) **Сканер Dr.Web** применяет обязательную перезагрузку удаленного компьютера непосредственно после обнаружения вируса и восстановления записи (так называемая «жесткая» перезагрузка). Перезагрузка выполняется вне зависимости от того, установлен флажок **Перезагрузить ПК после лечения** или нет. Сканирование удаленного компьютера при этом завершается досрочно. Для продолжения проверки необходимо повторно запустить сканирование удаленного компьютера с использованием **Консоли администрирования**.





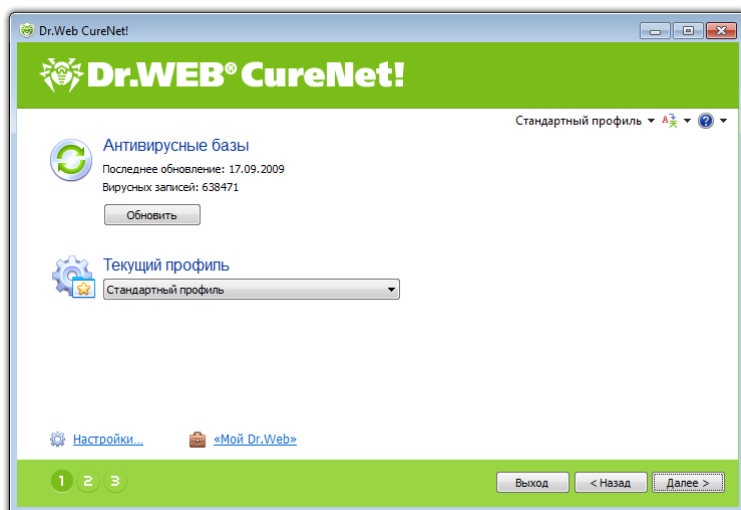
## 4. Обновление

Для обнаружения вредоносных объектов антивирусы компании **«Доктор Веб»** использует специальные **вирусные базы Dr.Web**, в которых содержится информация обо всех известных вредоносных программах. Так как каждый день появляются новые вирусные угрозы, то эти базы требуют периодического обновления. Такое обновление позволяет 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.

Для поддержания актуальности вирусных баз и программных алгоритмов компанией **«Доктор Веб»** реализована система распространения обновлений через сеть Интернет. **Модуль обновления** позволяет вам в течение срока действия лицензии загружать и устанавливать дополнения к вирусным базам и обновленные программные модули.

Программа **Dr.Web CureNet!** разработана специально для проведения централизованной проверки, поэтому для обеспечения максимальной защиты с ее помощью не требуется поводить обновление на каждом отдельном компьютере. **Вирусные базы Dr.Web** распространяются на проверяемые компьютеры из [репозитория Dr.Web CureNet!](#), 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.



**Рисунок 37. Обновление Dr.Web CureNet!.**



Для проведения обновления необходимо иметь доступ в сеть Интернет.

Поддерживается только автоматическое обновление. Файлы, добавленные в **Репозиторий Dr.Web CureNet!** вручную, программой не используются.

При помощи **Модуля обновления** возможна актуализация только **Репозитория Dr.Web CureNet!**.

Чтобы обновить **Консоль администрирования** и иные специализированные модули **Dr.Web CureNet!**, необходимо заново загрузить дистрибутив программы через **Мой Dr.Web**.



## Обновление Репозитория Dr.Web CureNet!

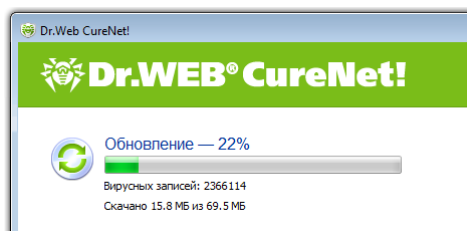
1. Запустите **Консоль администрирования**.
2. На шаге обновления и профилей ознакомьтесь с информацией о текущем состоянии **вирусных баз Dr.Web** и текущем профиле проверки.
3. При необходимости нажмите кнопку **Обновить**. Для проведения обновления требуется наличие действительного ключевого файла.



**Модуль обновления** проверяет не является ли ключевой файл заблокированным на сайте компании «**Доктор Веб**». В случае блокировки пользователю выдается соответствующее сообщение, обновление не производится, а компоненты программы могут быть заблокированы.

В случае блокировки вашего ключевого файла свяжитесь с [Технической поддержкой](#) компании «**Доктор Веб**».

4. После успешной проверки ключевого файла происходит обновление. **Модуль обновления** загружает все обновленные файлы, соответствующие вашей версии **Dr.Web CureNet!**. Дождитесь завершения процесса обновления.



**Рисунок 38. Процесс обновления Dr.Web CureNet!.**



## Обновление дистрибутива Dr.Web CureNet! через Мой Dr.Web

---



Количество обновлений дистрибутива программы во время срока действия лицензии неограничено. Для обеспечения максимальной эффективности работы программы рекомендуется проводить обновление дистрибутива **Dr.Web CureNet!** еженедельно.

---

1. Запустите **Консоль администрирования**.
2. На шаге обновления и профилей 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 CureNet!** при наличии действительной лицензии или продлить срок действия лицензии.

3. Сохраните обновленный дистрибутив **Dr.Web CureNet!**.
4. Запустите дистрибутив **Dr.Web CureNet!**, чтобы распаковать файлы программы и запустить обновленную **Консоль администрирования**.



## Приложение А. 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.



## Приложение Б. Техническая поддержка

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

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

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

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

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

