



Защити созданное

Лечит сети,
когда «припекло»

Централизованное лечение
локальных сетей — в том числе
с установленным антивирусом
другого производителя

<http://products.drweb.com/curenet/>



В Вашей сети нет вирусов? Вы в этом уверены?

Проверьте качество работы вашего антивируса при помощи Dr.Web CureNet!

Для многих компаний, предъявляющих высокие требования к уровню информационной безопасности корпоративных сетей, уже давно стало нормой использование антивирусов разных производителей на станциях, серверах или корпоративном шлюзе.

Если в Вашей локальной сети используется антивирус другого производителя, но Вы сомневаетесь в его эффективности, с помощью сетевой утилиты **Dr.Web CureNet!** без деинсталляции используемых продуктов и без установки **Dr.Web CureNet!** в систему Вы можете просканировать все компьютеры и, в случае необходимости, вылечить их.

Dr.Web CureNet! лечит сети, когда «припекло»

Факты о Dr.Web CureNet!

Продукт	Dr.Web CureNet!
Для чего предназначен	<ol style="list-style-type: none"> 1. Удаленное централизованное лечение рабочих станций и серверов Windows с установленным антивирусом другого производителя в локальных сетях любого масштаба. 2. Проверка качества антивирусной защиты другого производителя.
Описание продукта	http://products.drweb.com/curenet/
Поддерживаемые ОС	MS Windows 2012 / 8, 8.1 (Professional/Enterprise) / 2008 SP2 / 7 (Professional/Enterprise/Ultimate) / 2008 / Vista SP1 (Business/Enterprise/Ultimate) / 2003 SP1 / XP Professional SP2 (32- и 64-битная архитектура)
Что такое «Мой Dr.Web CureNet!»?	Это личный кабинет, в котором в течение всего срока действия лицензии хранится индивидуальная ссылка для скачивания обновленного дистрибутива. Также через личный кабинет можно связаться со службой техподдержки, отправить подозрительный файл на анализ, воспользоваться другими сервисами.
Как лицензируется?	Срок лицензий на Dr.Web CureNet! составляет 1, 2 или 3 года, количество проверяемых станций — от 5.
Демоверсия	Будучи эффективным средством скорой антивирусной помощи, Dr.Web CureNet! также представляет собой совершенный инструмент для проведения диагностики сети. Запустив утилиту в демонстрационном режиме, администратор может в любой момент просканировать компьютеры в локальной сети и проверить, не «проглядел» ли установленный антивирус троянского коня или любую другую вредоносную программу. В демонстрационном режиме программой можно пользоваться бесплатно, но функция лечения в таком случае работать не будет. Запросите демонстрационную версию сейчас! http://download.drweb.com/demoreq/
Системные требования	<p>Мастер</p> <ul style="list-style-type: none"> ■ Любой ПК под управлением MS Windows 2012 / 8, 8.1 (Professional/Enterprise) / 2008 SP2 / 7 (Professional/Enterprise/Ultimate) / 2008 / Vista SP1 (Business/Enterprise/Ultimate) / 2003 SP1 / XP Professional SP2 (32- и 64-битная архитектура) ■ Свободная оперативная память: не менее 360 МБ ■ Свободное место на жестком диске: не менее 200 МБ ■ Подключение ко всем проверяемым станциям по протоколу TCP/IP ■ Доступ в Интернет: для обновления вирусных баз и компонентов Dr.Web CureNet! <p>Сканер</p> <ul style="list-style-type: none"> ■ Любой ПК под управлением MS Windows XP Professional и более поздних версий, кроме Windows® Server 2003 x64 Edition и Windows® XP Professional SP2 x64 Edition ■ Свободная оперативная память: не менее 360 МБ ■ Свободное место на жестком диске: не менее 200 МБ
Где купить?	У партнеров (http://partners.drweb.com) или через Интернет (http://estore.drweb.com)



Преимущества

Соблюдение установленных политик безопасности

Dr.Web CureNet! не требует наличия сервера или установки какого-либо дополнительного ПО, его работа не оказывает никакого влияния на бизнес-процессы компании и не нарушает принятую для ее серверов политику безопасности.

Не зависит от подключения к Интернету

Dr.Web CureNet! не является веб-сервисом, поэтому распространение лечащих сканеров на проверяемые станции не производится через Интернет, а значит - скорость распространения и проверки станций, равно как и скорость сбора статистики не зависят от состояния связи. Проверяйте сети, даже полностью изолированные от Интернета!

Полная конфиденциальность

В процессе проверки никакого обмена данными между Dr.Web CureNet! и сервером «Доктор Веб» не производится, статистические данные о проверке корпоративной сети не передаются на сайт разработчика антивируса. Формирование отчета производится внутри локальной сети на ПК администратора. Не беспокойтесь о конфиденциальности итогов проверки вирусного состояния сети!

Простота администрирования

С управлением Dr.Web CureNet! справится даже начинающий системный администратор. Интерфейс Мастера Dr.Web CureNet! организован в виде последовательных шагов, что делает процедуру проверки интуитивно понятной. Наблюдайте за процессом сканирования в режиме реального времени!

Утилита всегда актуальна

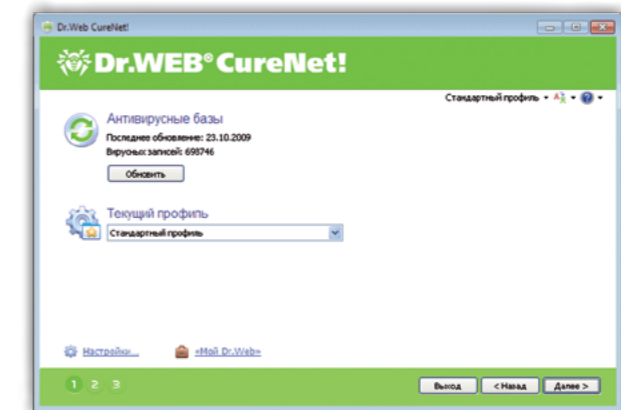
Ссылка на скачивание индивидуального дистрибутива хранится в личном кабинете «Мой Dr.Web CureNet!» в течение всего срока действия лицензии. В нужный момент просто скачайте обновленную версию Dr.Web CureNet! Или запустите утилиту обновления и получите самые свежие дополнения к вирусной базе и обновления программных модулей на уже запущенный Dr.Web CureNet!

Как это работает? Просто, как дважды два

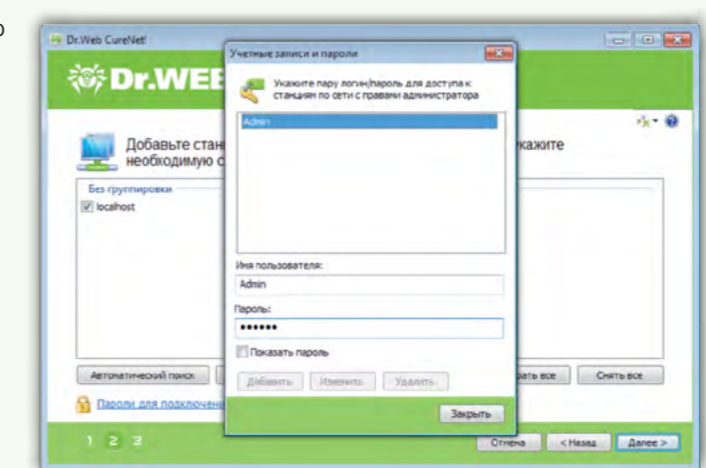
А. Скачайте дистрибутив Dr.Web CureNet! из вашего личного кабинета «Мой Dr.Web CureNet!».



В. В дистрибутив включены актуальные вирусные базы, однако, если Вы решите воспользоваться Dr.Web CureNet! позже, не забудьте обновить как саму утилиту Dr.Web CureNet!, так и вирусные базы.

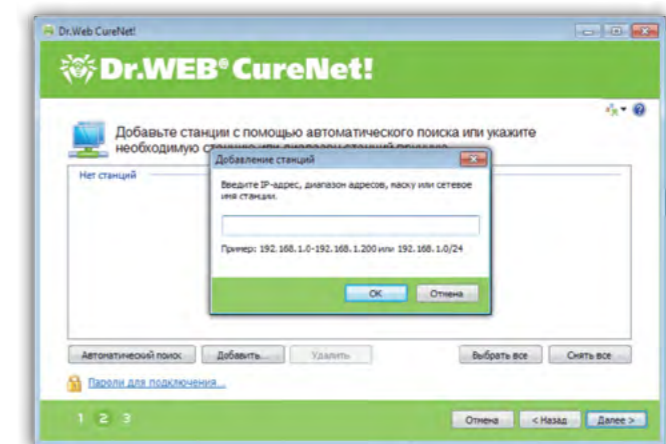


С. Поиск станций и запуск сканеров Dr.Web CureNet! для Windows на сканируемых компьютерах производится удаленно при помощи Мастера Dr.Web CureNet! Будучи обычным приложением для Windows, Мастер устанавливается на любой компьютер в сети, в которой проводится сканирование.



Для установления соединения со станцией используется текущая учетная запись администратора или список паролей для доступа к машинам в сети.

Д. Мастер ищет компьютеры, подключенные к сети, а затем размещает сканеры на обнаруженных станциях.

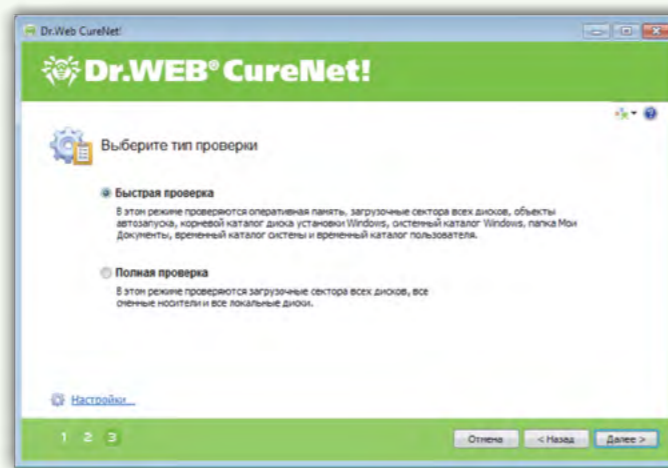


Вы можете провести сканирование на всех доступных компьютерах или выбрать рабочие станции и серверы, которые необходимо проверить на вирусы. Станции выбираются по IP-адресу из указанного диапазона адресов, по маске или по имени компьютера.

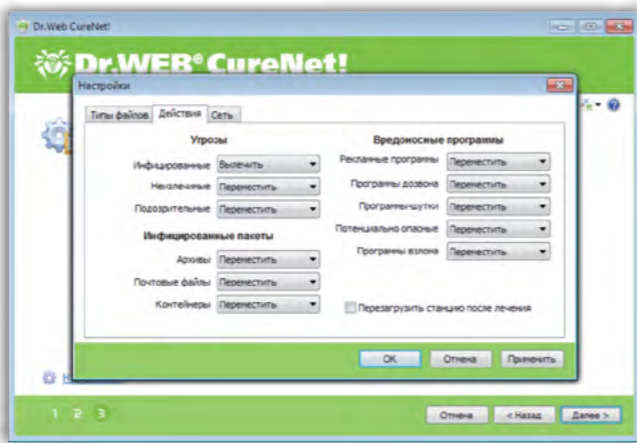
Dr.Web CureNet! готов просканировать и вылечить вашу сеть!

Широкие возможности сканирования и лечения

Выберите оптимальную глубину проверки, используя режимы Быстрого и Полного сканирования. В большинстве случаев установки по умолчанию обеспечивают оптимальный режим работы.



Настраивайте действия сканера в различных ситуациях при помощи индивидуальных настроек сканирования.

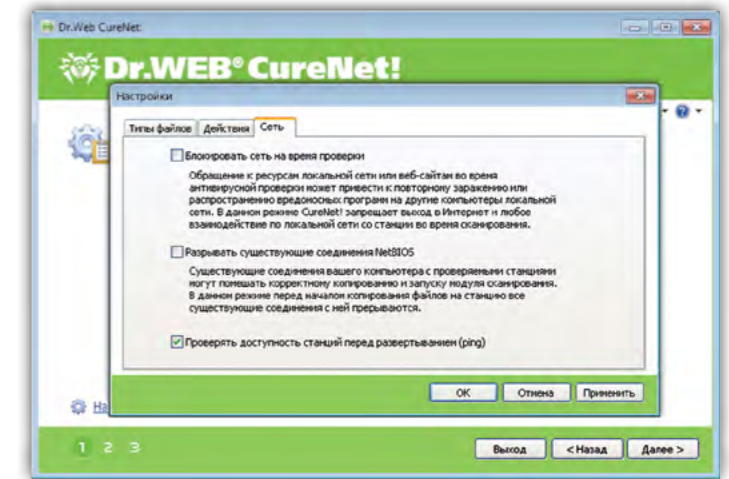


Для ускорения процесса сканирования Вы можете отключить проверку архивов и файлов электронной почты.

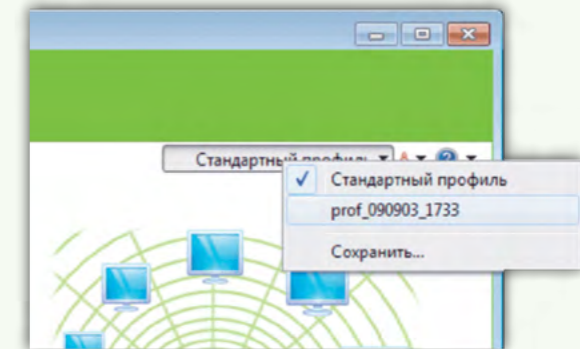
Подозрительные объекты перемещаются в карантин, расположенный на компьютере, на котором установлен Мастер Dr.Web CureNet!



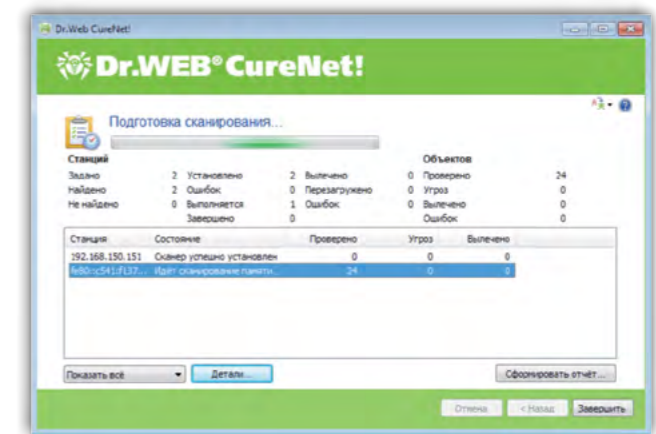
Во избежание повторных заражений сетевыми червями Вы можете отключить доступ рабочих станций к сети. Эта функция не распространяется на компьютер с установленным Мастером.



Настройки сканирования Вы можете сохранять в профилях XML. При работе утилиты воспользуйтесь профилем по умолчанию или создавайте собственные.



Следите за ходом проверки компьютеров в режиме реального времени.



По окончании сканирования ознакомьтесь с отчетом о работе антивирусных сканеров.

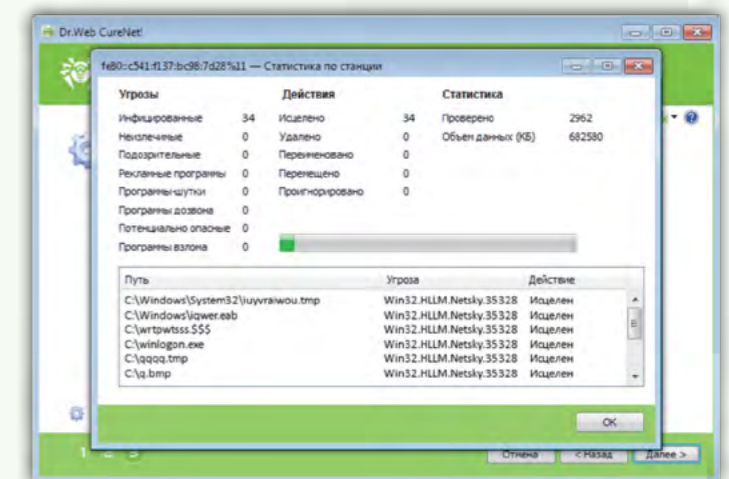


Таблица функциональности

Лечит компьютеры и серверы	Под управлением MS Windows XP Professional и более поздних версий, кроме Windows® Server 2003 x64 Edition и Windows® XP Professional SP2 x64 Edition.
Лечение в сетях, изолированных от Интернета	Включая IPv6
Размер сети	Без ограничений
Установка Мастера Dr.Web CureNet!	На ПК под управлением MS Windows 2012 / 8, 8.1 (Professional/Enterprise) / 2008 SP2 / 7 (Professional/Enterprise/Ultimate) / 2008 / Vista SP1 (Business/Enterprise/Ultimate) / 2003 SP1 / XP Professional SP2 (32- и 64-битная архитектура)
Запуск Dr.Web CureNet! с USB-носителя	■
Установка сканеров Dr.Web для Windows	Установка не требуется
Удаленный централизованный запуск лечащих сканеров в зараженной системе без предварительного лечения системы	Лучший в отрасли!
Удаленный централизованный запуск лечащих сканеров на всех станциях/на выбранных станциях	■
Возможность отключения на удаленной машине на время сканирования доступа к сети с целью предупреждения повторного заражения	■
Возможность выборочного сканирования на удаленных станциях	■
Возможность прерывания или остановки сканирования на выбранных станциях	■
Централизованное задание действий для обнаруженных вредоносных объектов	■
Централизованный сбор статистики	■
Самоудаление лечащих сканеров после проверки	■
Экспорт отчета о сканировании	■
Поиск станций	
Автоматический поиск станций	■
■ по IP-адресу	
■ по диапазону IP-адресов	
■ по маске	
■ по сетевому имени	
Возможности сканирования	
Собственные профили проверки	■
Выбор действий для каждого типа вредоносных объектов (шпионского ПО, рекламного ПО, потенциально опасного ПО, программ платного дозвона, программ-шутки)	■
Выбор действий для зараженных, подозрительных объектов и объектов другого типа, включая лечение, переименование, перемещение и удаление	■
Возможность задавать варианты действий над обнаруженным вредоносным объектом, если первоначальное или последующее действие невозможно	■
Выбор действий для инфицированных пакетов (архивов, контейнеров, почтовых файлов)	■

Сканирование архивов любой степени вложенности	Лучшее в отрасли!
Быстрая проверка (проверяются оперативная память, загрузочные секторы всех дисков, объекты автозапуска, корневой каталог загрузочного диска, корневой каталог диска установки Windows, системный каталог Windows, папка «Мои документы», временный каталог системы, временный каталог пользователя)	■
Полная проверка (все объекты Быстрой проверки, а также все локальные диски ПК)	■
Эвристический анализатор	■
Дополнительные технологии обнаружения вредоносных объектов, помимо сигнатурного метода и эвристического анализа	Origins Tracing™
Исключение архивов из проверки	■
Исключение почтовых файлов из проверки	■
Самозащита от анти-антивирусных программ	
Защита модулей и файлов Dr.Web CureNet! на удаленной машине перед запуском сканирования	Dr.Web SelfPROtect
Возможности лечения	
Обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками	FLY-CODE
Проверка скриптов, включая VB-Script, Java Script	■
Проверка логических дисков	■
Проверка почтовых файлов	■
Возможность обнаружения и удаления активных (запущенных и выполняющихся в момент проверки) и пассивных вредоносных программ следующих типов:	Лидер в лечении активных заражений!
■ почтовые и сетевые черви	
■ руткиты	
■ файловые вирусы	
■ троянские программы	
■ бестелесные и стелс-вирусы	
■ полиморфные вирусы	
■ макро-вирусы и вирусы, поражающие документы MS Office	
■ скрипт-вирусы	
■ шпионское ПО	
■ рекламное ПО	
■ хакерские утилиты	
■ программы платного дозвона	
■ программы-шутки	
Обновление	
Обновление компонентов Dr.Web CureNet! и вирусных баз по требованию через сеть Интернет	■
Размер вирусной базы	Оптимизированное число записей!!!
Размер обновлений	Самый маленький в отрасли!!!

Локализация

- Локализованная версия программы на русском языке ■
- Руководство по эксплуатации на русском языке ■

Поддержка

- Бесплатная техническая поддержка на русском языке в России ■
- Анализ вирусов, неизвестных вирусной базе Dr.Web ■

Dr.Web – лидер отрасли в лечении активных заражений

Важным показателем качества работы антивирусной программы является не только ее способность находить вирусы, но и лечить их; не просто удалять инфицированные файлы вместе с важной для пользователя информацией, но и возвращать их в первоначальное «здоровое» состояние.

Антивирус Dr. Web может работать на инфицированных компьютерах, исключительная вирусоустойчивость выделяет его среди аналогичных программ.

- Лидер отрасли! У Dr.Web самые высокие показатели успешного лечения активных заражений.
- Лидер отрасли! Благодаря уникальным технологиям сканирования памяти и лечения инфицированных файлов антивирус Dr.Web можно запускать в инфицированной системе, не проводя предварительного лечения.

Антивирусное ядро

- Только Dr.Web может сканировать заархивированные файлы на любом уровне вложенности. Даже если вредоносный объект был несколько раз заархивирован различными программами для сжатия данных, Dr.Web обязательно обнаружит и нейтрализует угрозу.
- Алгоритмы и технологии Dr.Web обеспечивают обнаружение упакованных объектов и позволяют проводить их детальный анализ для выявления скрытых угроз. Даже если вредоносная программа была сжата при помощи неизвестного упаковщика, она все равно не останется незамеченной.
- Dr.Web – недостижимый лидер в нейтрализации таких сложных вирусов как MaosBoot, Rustock.C, Sector.
- Блокирование вируса в оперативной памяти до того, как он скопирует себя на жесткий диск, снижает вероятность того, что вредоносная программа воспользуется уязвимостью в одном из установленных приложений или в операционной системе.
- В Dr.Web реализована способность обнаруживать и нейтрализовывать вирусы, существующие в оперативной памяти и никогда не встречающиеся в виде отдельных файлов, такие как Slammer и CodeRed. Эта отличительная антивирус Dr.Web от многих других антивирусов способность появилась в программе благодаря реализации полной проверки системной памяти компьютера. В июле 2001 года, когда разразилась эпидемия CodeRed, оказалось, что только один антивирус в мире – Dr.Web – был способен обнаружить этот вирус. **Даже сейчас лишь немногие средства информационной безопасности умеют лечить подобные вирусы.**

Антируткит

- Dr.Web Shield™ обеспечивает обнаружение вирусов, использующих руткит-технологии для сокрытия своего присутствия в системе.
- Dr.Web® Shield™ предоставляет антивирусному сканеру привилегированный доступ к файлам, реестру и некоторым базовым компонентам системы. Таким образом антивирус может обнаруживать руткиты и блокировать механизм самозащиты руткитов и невидимых вирусов.

Обнаружение неизвестных вирусов

Новейшие технологии Dr.Web позволяют антивирусу обнаруживать даже неизвестные угрозы, обеспечивая тем самым сохранность вашей информации.

- FLY-CODE – не имеющая аналогов технология универсальной распаковки, реализованная в поисковом модуле Dr.Web версии 5.0, которая позволяет распаковывать неизвестные Dr.Web упаковщики. Основываясь на специальных записях в вирусной базе Dr.Web, поисковый модуль может строить эвристические предположения о возможно содержащемся в упакованном архиве вредоносном объекте, добавляя к названию детектируемого объекта запись вида «Возможно Trojan.Packed».
- Origins Tracing™ – уникальный алгоритм несигнатурного обнаружения вредоносных объектов, который дополняет традиционные сигнатурный поиск и эвристический анализатор Dr.Web, дает возможность существенно повысить уровень детектирования ранее неизвестных вредоносных программ.
- Эвристический анализатор обнаруживает большинство известных угроз. Даже если вредоносная программа не внесена в вирусные базы, эвристический анализатор обнаружит ее по характерным признакам.

Самозащита

- Dr.Web SelfPROtect обеспечивает иммунитет антивируса к любым попыткам вредоносных программ нарушить его работу.
- Dr.Web SelfPROtect реализован в виде драйвера, работающего на самом низком системном уровне. Остановить работу драйвера без перезапуска системы невозможно.
- Для обеспечения работоспособности антивируса Dr.Web SelfPROtect может ограничивать доступ к файлам, папкам и съемным носителям информации, а также к определенным веткам реестра Windows.
- Некоторые антивирусы модифицируют ядро Windows (перехватывают прерывания, изменяют векторные таблицы и используют другие недокументированные функции). Это может нарушить стабильность системы и в итоге негативно сказаться на безопасности в целом. Dr.Web SelfPROtect обеспечивает безопасность антивируса и в то же время не вмешивается в работу ядра Windows.

О компании «Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности. Компания предлагает эффективные антивирусные и антиспам-решения как для крупных компаний и государственных организаций, так и для частных пользователей. Антивирусные продукты 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 Dr.Web свидетельствуют о высокой степени доверия к продуктам компании. Антивирусная продукция компании «Доктор Веб» создана на основе собственной технологии. «Доктор Веб» – один из немногих антивирусных вендоров в мире, владеющих собственной уникальной технологией детектирования и лечения вредоносных программ; имеет собственную службу вирусного мониторинга и аналитическую лабораторию. Это обуславливает высокую скорость реакции специалистов компании на новые вирусные угрозы, способность оказать помощь клиентам в решении проблем любой сложности в считанные часы.

- Россия** **ООО «Доктор Веб»**
Россия, 125124, Москва,
3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 (495) 789-45-87 (многоканальный)
Факс: +7 (495) 789-45-97
www.drweb.com | www.av-desk.com | www.freedrweb.com
- Германия** **Dr.Web Deutschland GmbH**
Германия, 63457 Hanau, Rodenbacher Chaussee 6
Тел.: +49 (6181) 9060-1210
Факс: +49 (6181) 9060-1212
www.drweb-av.de
- Казахстан** **ТОО «Доктор Веб – Центральная Азия»**
Республика Казахстан, 050009, Алматы,
ул. Шевченко /уг. ул. Радостовца, 165б/72г, офис 910
Тел.: +7 (727) 323-62-30, 323-62-31, 323-62-32
www.drweb.kz
- Украина** **ООО «Центр технической поддержки «Доктор Веб»**
Украина, 01001, Киев, пер. Михайловский, 17
Телефон/факс: +38 (044) 238-24-35, 279-77-70
www.drweb.ua
- Франция** **Doctor Web France**
333 b Avenue de Colmar, 67100 STRASBOURG
Тел.: +33 (0) 3-90-40-40-20
Факс: +33 (0) 3-90-40-40-21
www.drweb.fr
- Япония** **Doctor Web Pacific, Inc.**
NKF Kawasaki building 2F, 1-2,
Higashida-cho, Kawasaki-ku,
Kawasaki-shi, Kanagawa-ken 210-0005
Тел.: +81(0) 44-201-7711
www.drweb.co.jp



© ООО «Доктор Веб», 2003