Dr.WEB®
www.drweb.com

AXOFT

Защити созданное

Современные вирусные угрозы
Технологические новинки Dr.Web

14 мая 2010 г.

Валерий
Ледовской

Dr.WEB®
www.drweb.com

Защити созданное

План:

1. Актуальные вирусные угрозы
2. Линейка продуктов
3. Технологии Dr.Web

Dr.WEB®
www.drweb.com

Пишут ли сотрудники АВ-компаний вирусы?

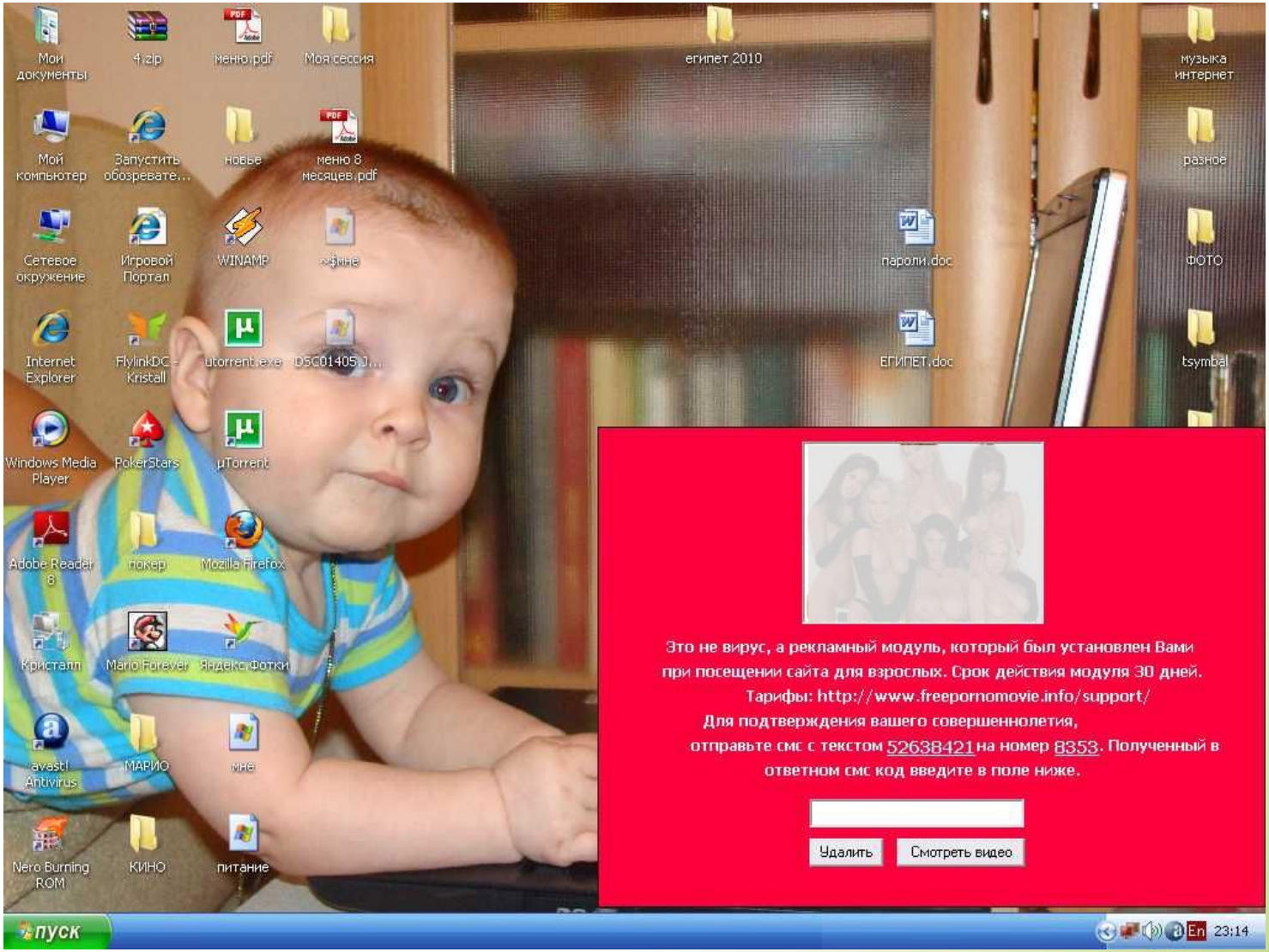
☺

1. **Вирусописатели получают доходы на порядок больше, чем АВ-вендоры.**
2. **В день в вирусную базу добавляется несколько тысяч вирусных записей.**
3. **Написание вирусов – уголовное преступление (ст. 273 УК РФ, до 7 лет лишения свободы)**
4. **Dr.Web предлагает бесплатные утилиты и интернет-ресурсы для пользователей-жертв**

Защити созданное

Dr.WEB®
www.drweb.com

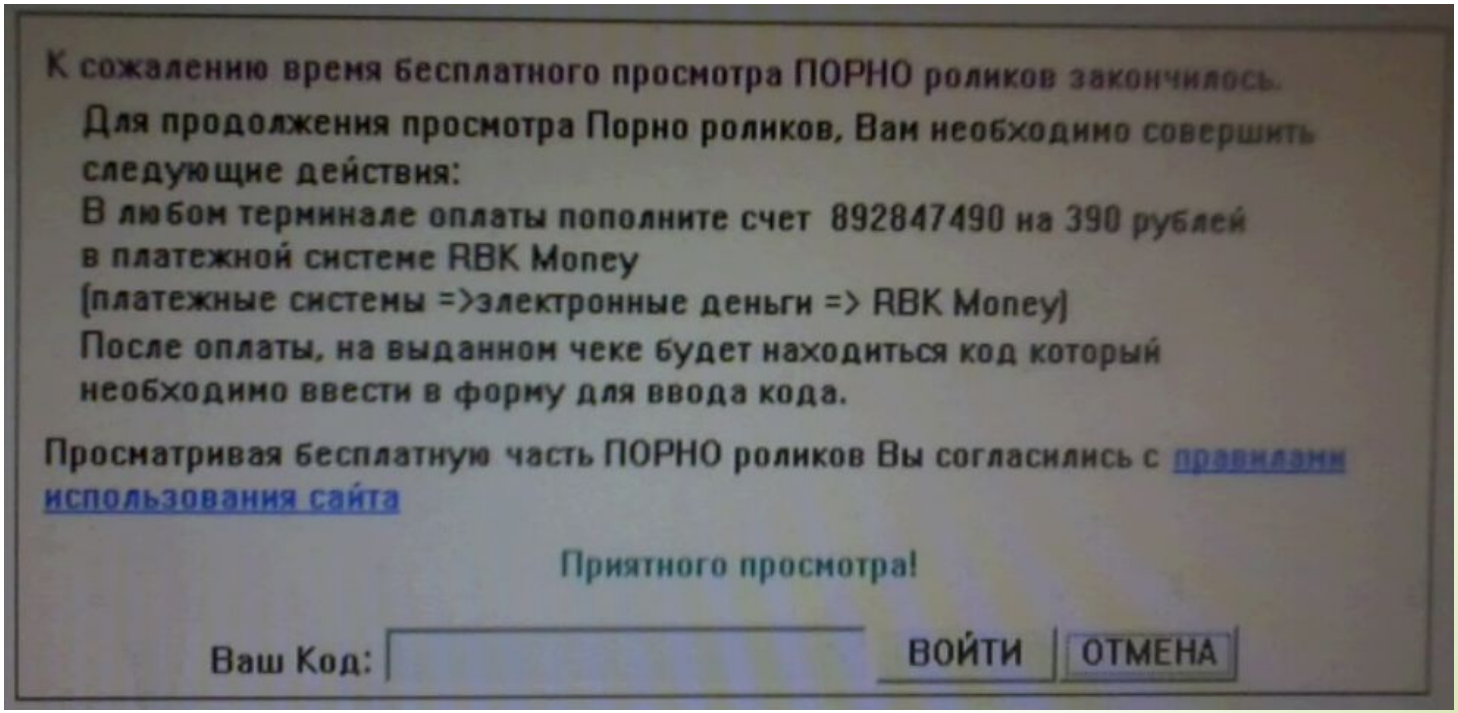
Trojan.Winlock



Защити созданное

Dr.WEB®
www.drweb.com

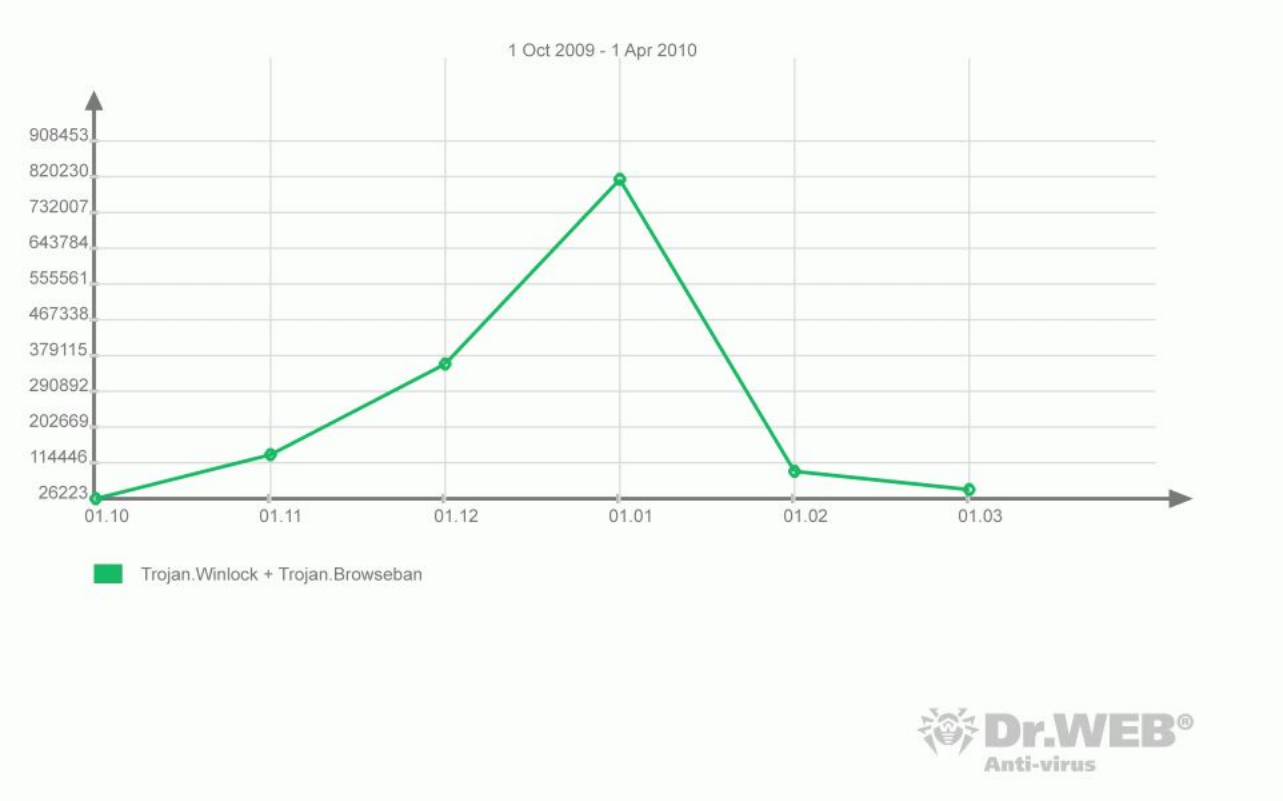
Trojan.Winlock



Защити созданное

Dr.WEB®
www.drweb.com

Масштабы Trojan.Winlock



Январь 2010 (оценка):

- количество пострадавших пользователей: несколько млн.

- доход злоумышленников: сотни миллионов рублей

Dr.WEB®
www.drweb.com

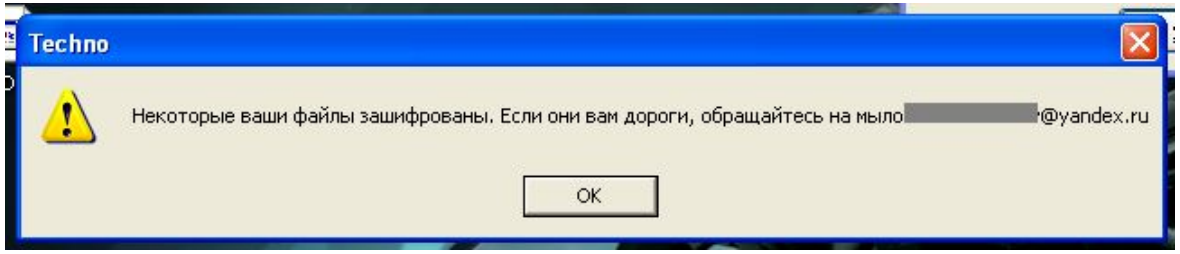
Лечение Trojan.Winlock

1. Не отсылать деньги злоумышленникам!
2. Раздел сайта для разблокировки Windows:
http://www.drweb.com/unlocker
3. Техподдержка:
https://support.drweb.com/new/tech
4. Форум (раздел «Помощь по лечению»):
http://forum.drweb.com
5. Специальные версии Dr.Web CureIt!:
http://freedrweb.com
6. Загрузочный диск Dr.Web LiveCD:
http://freedrweb.com

Защити созданное

Dr.WEB®
www.drweb.com

Trojan.Encoder



Выкуп: 2000 руб.; Dr.Web лечит бесплатно!

Дешифровка от Trojan.Encoder.68

Подробнее в новости Trojan.Encoder.68 архивирует файлы с длинным паролем.

ID: Получить пароль

Аптечка сисадмина

Утилиты от троянских программ

Форма дешифровки от Trojan.Encoder.68
Утилита дешифровки от Trojan.Encoder
Утилита дешифровки от Trojan.Encoder.19
Утилита дешифровки от Trojan.Encoder.33
Утилита дешифровки от Trojan.Encoder.34,37-39,41-46,49
Утилита дешифровки от Trojan.Encoder.47
Утилита дешифровки от Trojan.Encoder.55
Утилита разблокирования файлов после Trojan.Locker.8

Dr.WEB®
www.drweb.com

Ботсе
ти

-Скрытно устанавливается клиентское ПО на компьютеры жертвы
- Управляются хозяином с сервера
- Используются для:
•Рассылки спама
•Атаки ресурсов
•Подбора паролей
•Загрузки и запуска других вредоносных программ

Пример: ботсеть **Win32.HLLW.Shadow** (**Kido**, **Conficker**).

Защити созданное

Dr.WEB®
www.drweb.com

Ботсеть

Trojan.Oficla

Защити созданное

1. В настоящее время около **200 000 детектов** в неделю
2. Продаётся по цене $450 – 700
3. Использует установленный Microsoft Word для скрытия факта общения со своим сервером
4. Принимает команды от хозяина на загрузку и запуск других вредоносных программ

Dr.WEB®
www.drweb.com

Ботсеть

Trojan.Oficla

Защити созданное

Описание:

NON RESIDENT - Это не резидентная версия Lite. Отличие её от версии Lite в том,что лоадер сразу запускается в оперативной памяти выполняя все задачи. Только после успеха выполнения данных ему задач лоадер самоудаляется из оперативной памяти.Все действия проводимые в оперативной памяти лоадер делает в обход всех защит и полностью невидимо, даже специфическими таск-менеджерами. Однако данная версия лоадера срабатывает только на момент получения задания. То есть говоря простым языком - это разовый лоадер.

LITE - Версия лоадера,для тех кому нужно сохранять каждого бота и нужна упращенная версия админки. Данная версия срабатывает,так же,как версия NON RESIDENT, но в отличае от выше упомянутой версии LITE намертво встраивается в систему и тем самым сохряняет бота даже после перезагрузки системы. И попыток её восстановления, путем перемоток сервисными службами ОС.

FULL - Эта версия лоадера нужна тем,кто серьёзно занимается загрузками. Таким людям требуется самый качественный пробив и максимальная живучесть ботнета, потому что каждая загрузка и технология самой загрузки влияет на монетезацию их работы. Поэтому в эту версию лоадера встроен лучший движок по пробиву фаерволлов, а так же старый добрый руткитный модуль, который встраивается в системные модули и драйвера самой системы. А также перехватывает собственный API ядра. Это наиболее надежный и действенный способ перехвата системы. Поэтому бот работающий под таким лоадером будет жить максимально долго. Так же в этой версии лоадера в админке присутствует Builder, для возможности клиентом получения лоадера прямо из его админки с возможностью записи парраметра adv. Данный парраметр отвечает за уникальность специального номера билда. Таким образом клиент может сделать несколько билдов с разными парраметрами adv и раздать билды разным адвертам. При прогрузки каждого билда в статистике такие билды можно не только различать, но и давать каждому номеру свои задания, или даже разделять трафик полученный от разных адвертов. Так же в последних версиях версии FULL присутствует адвертская часть. Вы сможете создать в админке специальную статистику, по билдам и выдать каждому адверту эту статистику на конкретно его номер билда.Таким образом каждый адверт будет знать, сколько конкретно вы получили загрузок от него. Такая система на сегодняшний день не заменима, для людей серьёзно занимающихся загрузками.

NON RESIDENT myLoader - 450$

LITE myLoader - 550$

FULL myLoader - 700$

Чистки - 30$

Смена урла - 90$

* Бесплатно поможем поставить и настроить. Проконсультируем по всем вашим вопросам.

Dr.WEB®
www.drweb.com

Интернет-банкинг

Защити созданное

Dr.WEB®
www.drweb.com

Trojan.Ibank

Защити созданное

1. До **160 000** детектов в день в марте 2010г.
2. Использует уязвимости **Adobe Reader**
3. Осуществляет мониторинг работы пользователя с онлайновыми банковскими системами
4. Большие суммы денег на счетах некоторых пользователей
5. Малое количество потенциальных жертв –> большое распространение
(3% вредоносного трафика за март 2010г.)

Dr.WEB®
www.drweb.com

Dr.Web Desktop Security Suite

Защити созданное

Корпоративные сети:

- Dr.Web Enterprise Suite
- Dr.Web CureNet!

Защита рабочих станций:

- Dr.Web Security Space Pro
- Антивирус Dr.Web Pro
- Dr.Web для Mac OS X
- Dr.Web для Linux
- Консольные сканеры

Dr.WEB®
www.drweb.com

Dr.Web Mail Security Suite

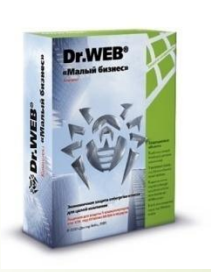
Защити созданное

Защита почты:

- Dr.Web для почтовых серверов Unix
- Dr.Web для MS Exchange
- Dr.Web для IBM Lotus Domino
- Dr.Web для MIMEsweeper
- Dr.Web для Kerio Mail Server

Защита SMTP-шлюзов:

- Dr.Web Mail Gateway



Dr.WEB®
www.drweb.com

Dr.Web Server Security Suite

Защита файловых серверов:

- Dr.Web для файловых серверов Windows
- Dr.Web для файловых серверов Unix
- Dr.Web для файловых серверов Novel Netware

Dr.Web Gateway Security Suite

Защита интернет-шлюзов

- Dr.Web для интернет-шлюзов Unix
- Dr.Web для Kerio WinRoute Firewall

Dr.Web Mobile Security Suite

Защита мобильных устройств

- Dr.Web для Windows Mobile
- Dr.Web для Symbian OS

Защити созданное

Dr.WEB®
www.drweb.com

Dr.Web Security Suite для Appliance

Защити созданное

Dr.Web Office Shield

Решаемые задачи

Уменьшение зависимости предприятий от уровня квалификации IT-персонала.

Снижение потерь рабочего времени, простоев оборудования и персонала за счет уменьшения количества вирусных инцидентов в корпоративной сети.

Повышение производительности труда путем снижения количества отвлекающих факторов.

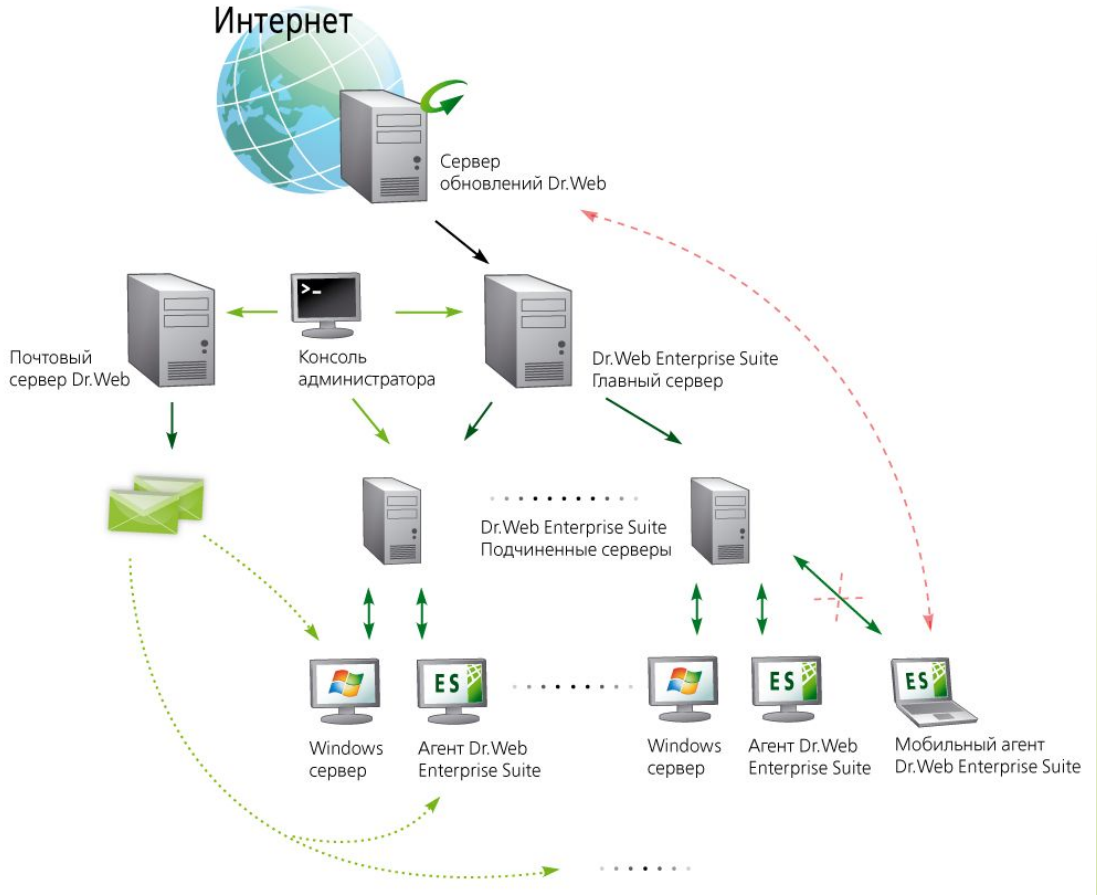
Оптимизация расходов на интернет-трафик и контроль за деятельностью сотрудников в сети Интернет.

Dr.WEB®
www.drweb.com

Логическая схема работы Dr.Web Enterprise Suite

Защити созданное

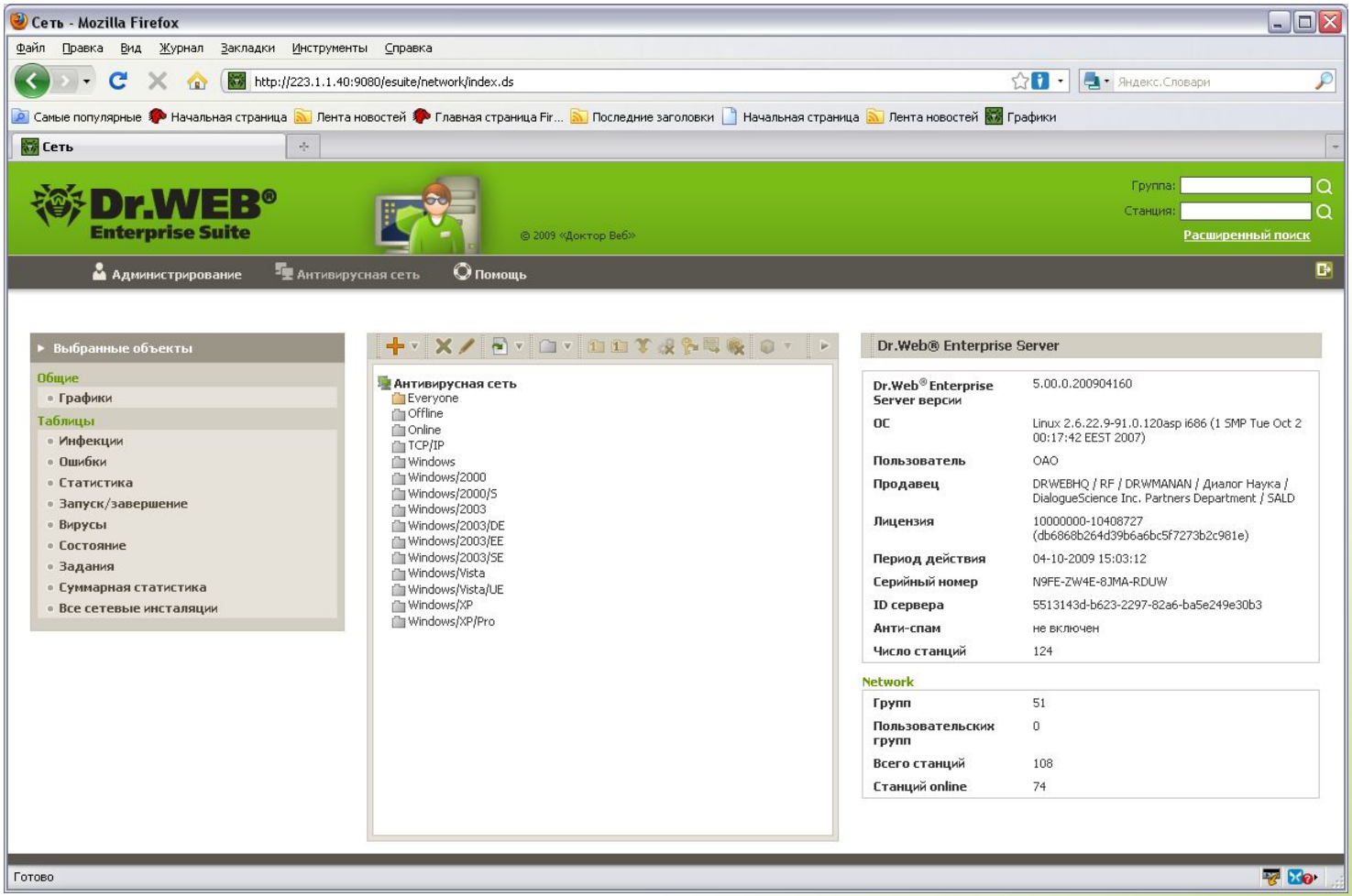
Dr.Web® Enterprise Suite



Dr.WEB®
www.drweb.com

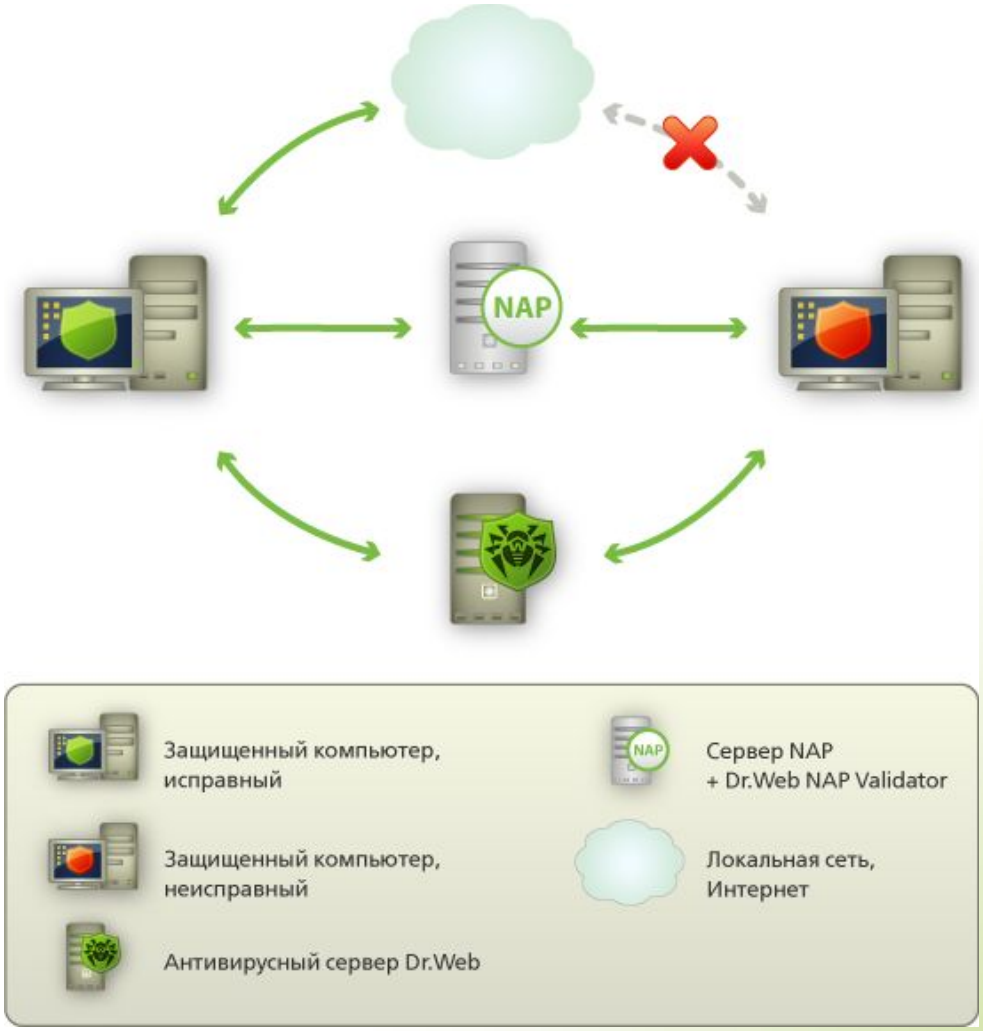
Веб-консоль Dr.Web Enterprise Suite

Защити созданное



Dr.WEB®
www.drweb.com

Поддержка технологии
Microsoft Network Access Protection (NAP)

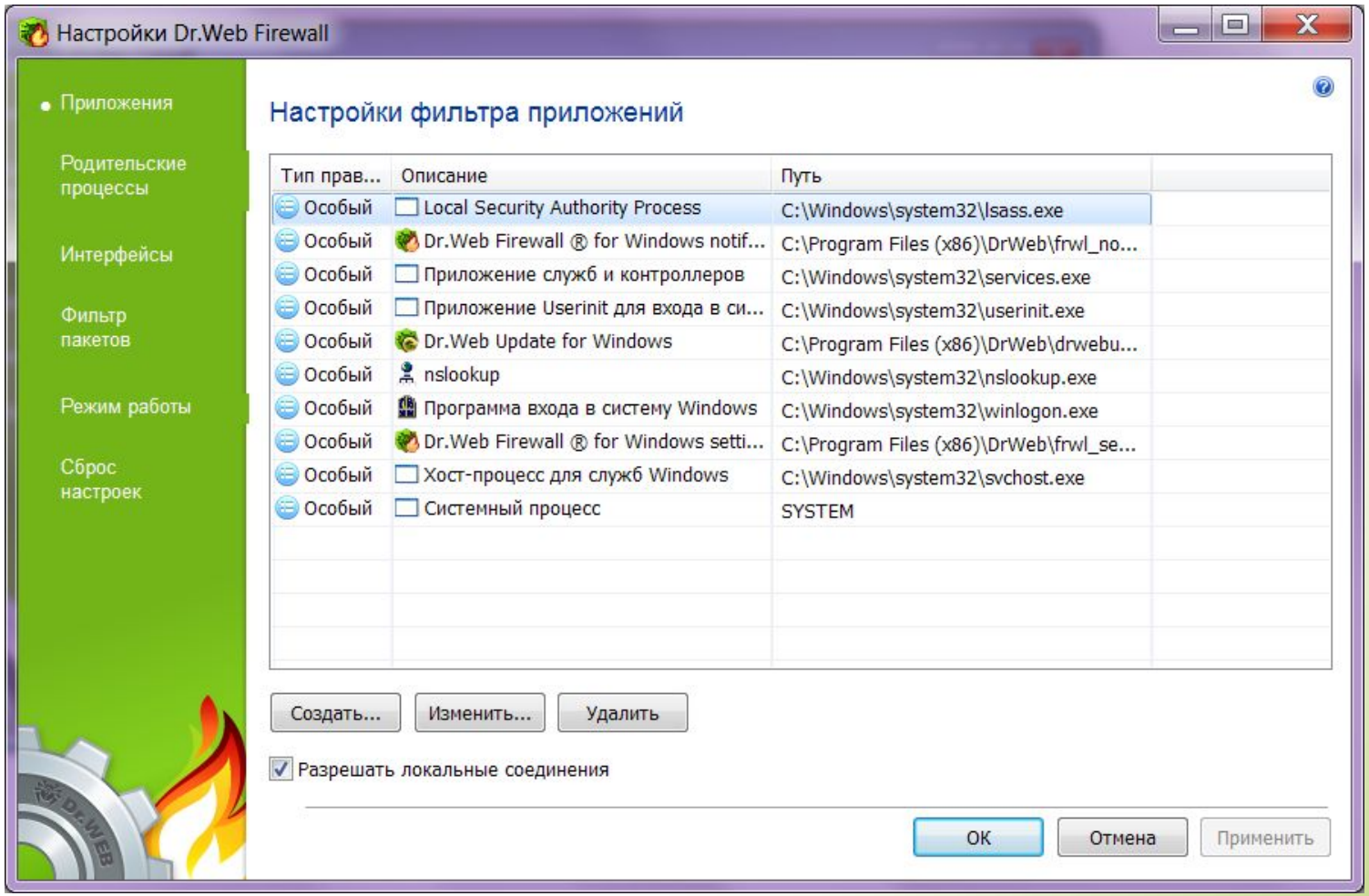


Защити созданное

Dr.WEB®
www.drweb.com

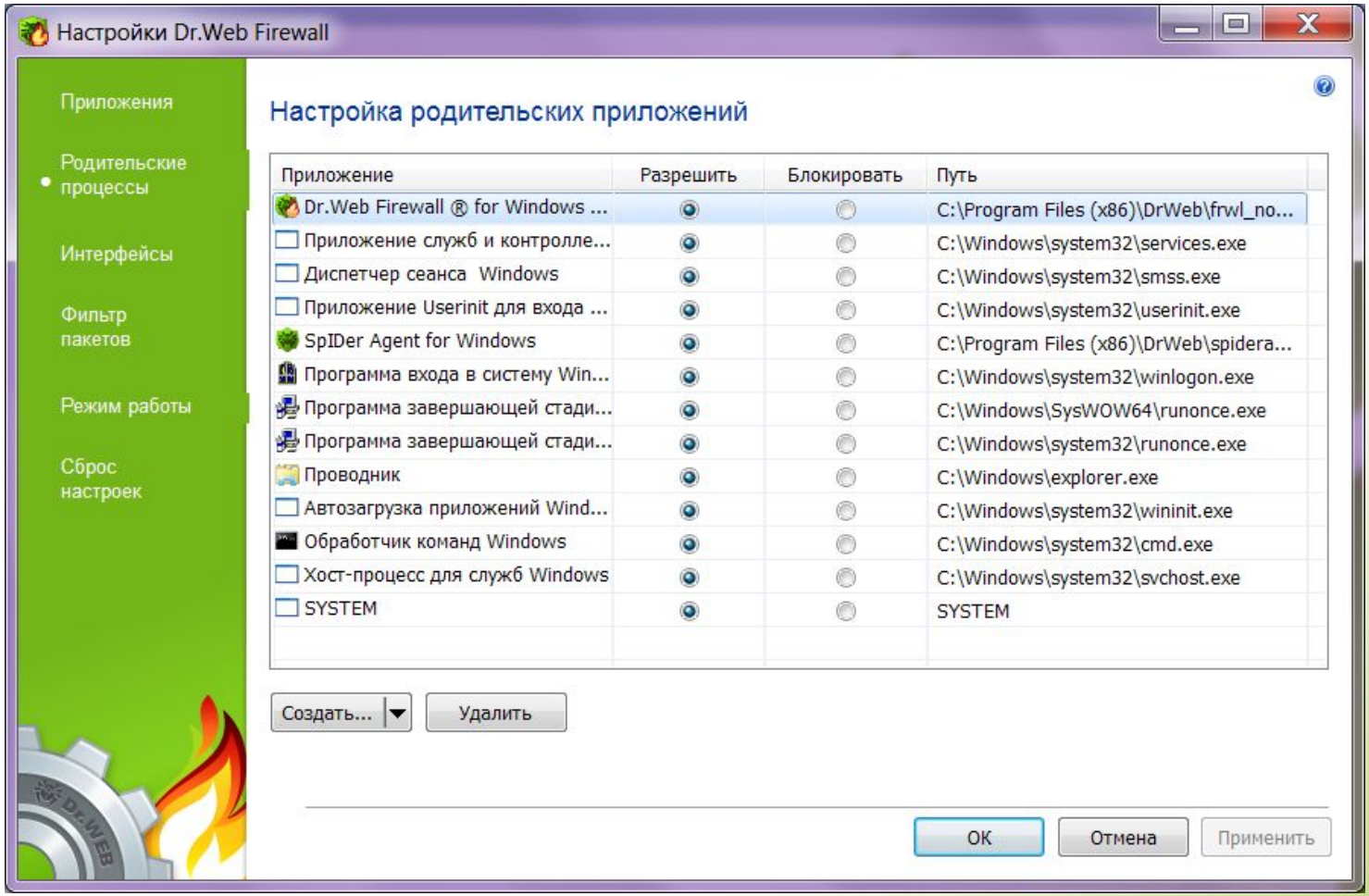
Настройки фильтра приложений

Защити созданное



Dr.WEB®
www.drweb.com

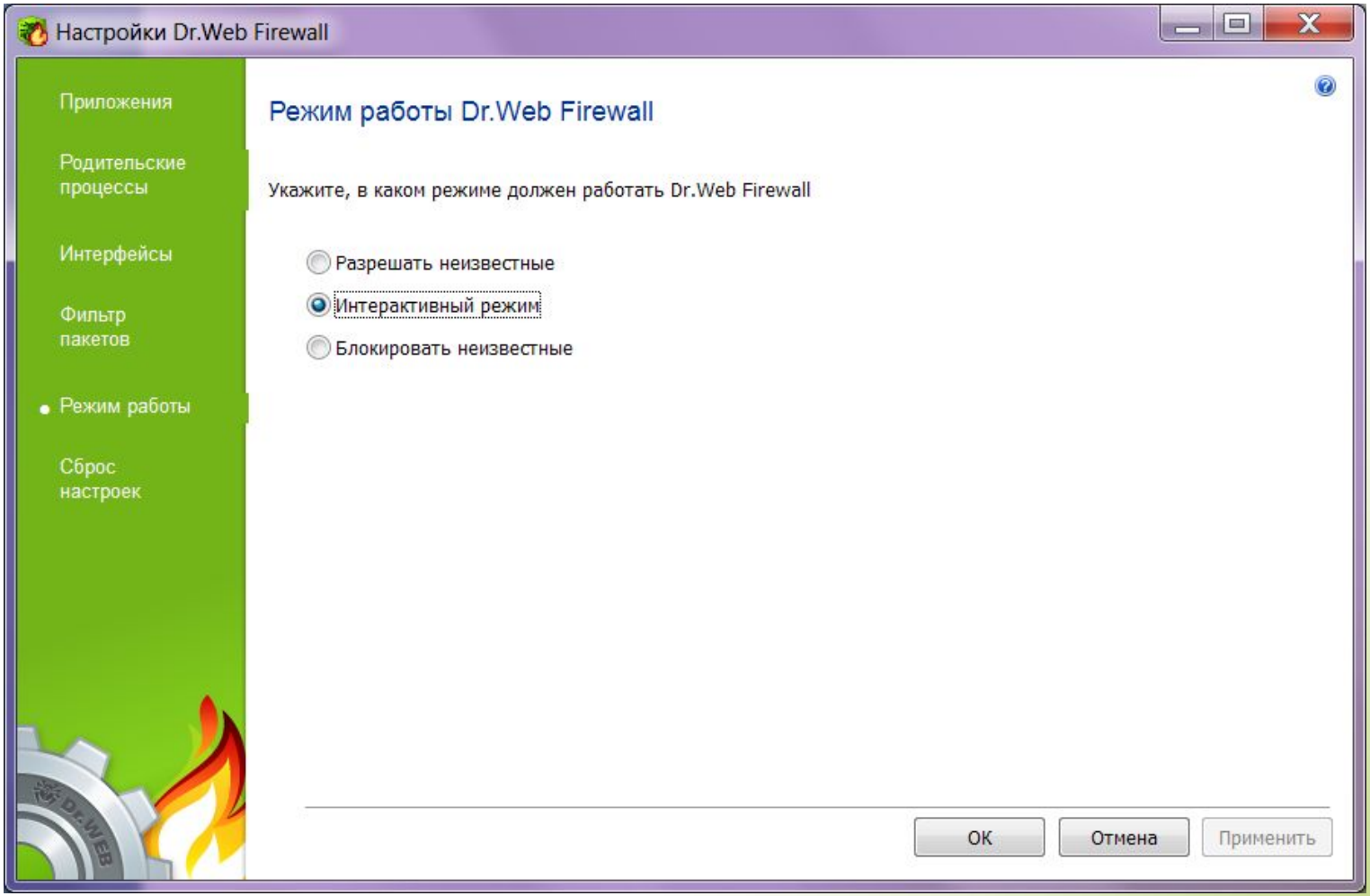
Родительские процессы



Защити созданное

Dr.WEB®
www.drweb.com

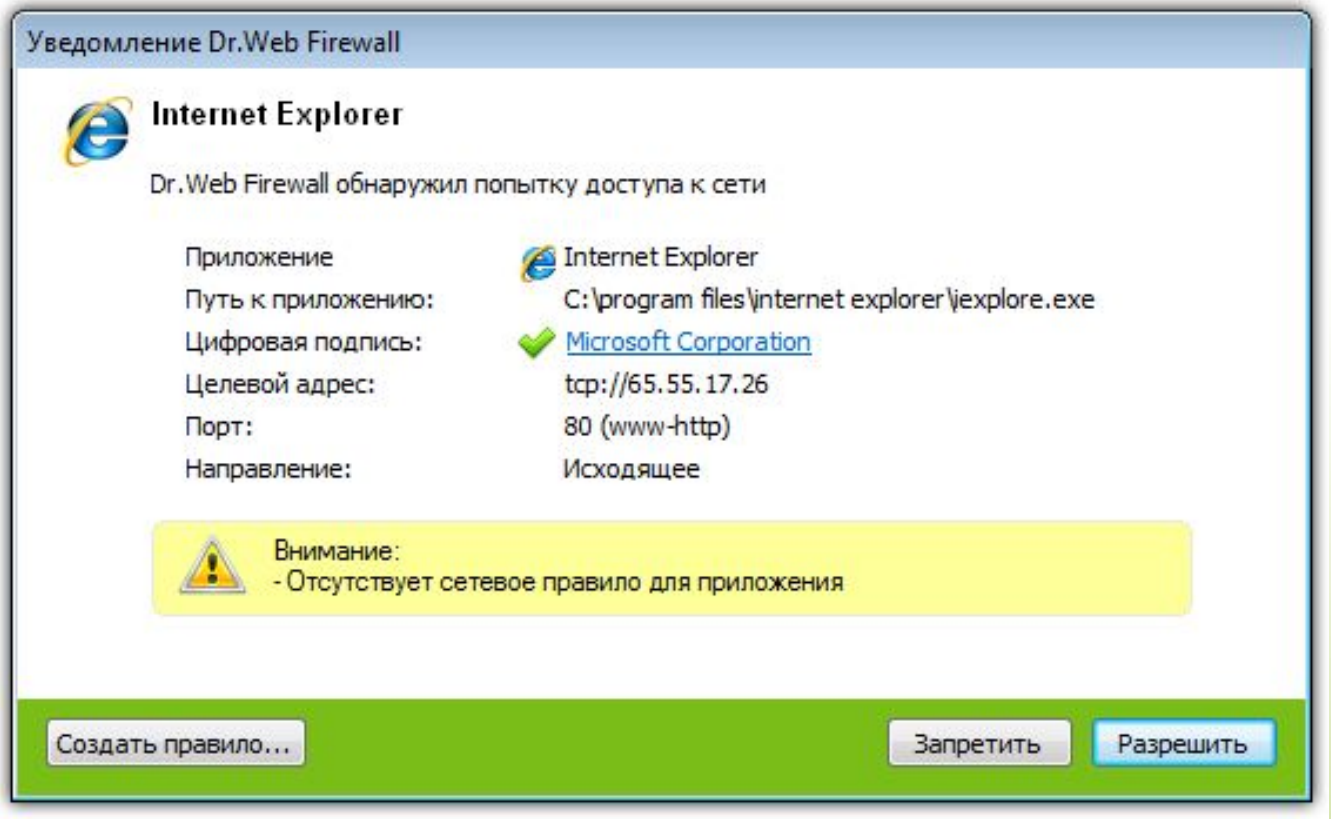
Режимы работы



Защити созданное

Dr.WEB®
www.drweb.com

Обучение Dr.Web Firewall

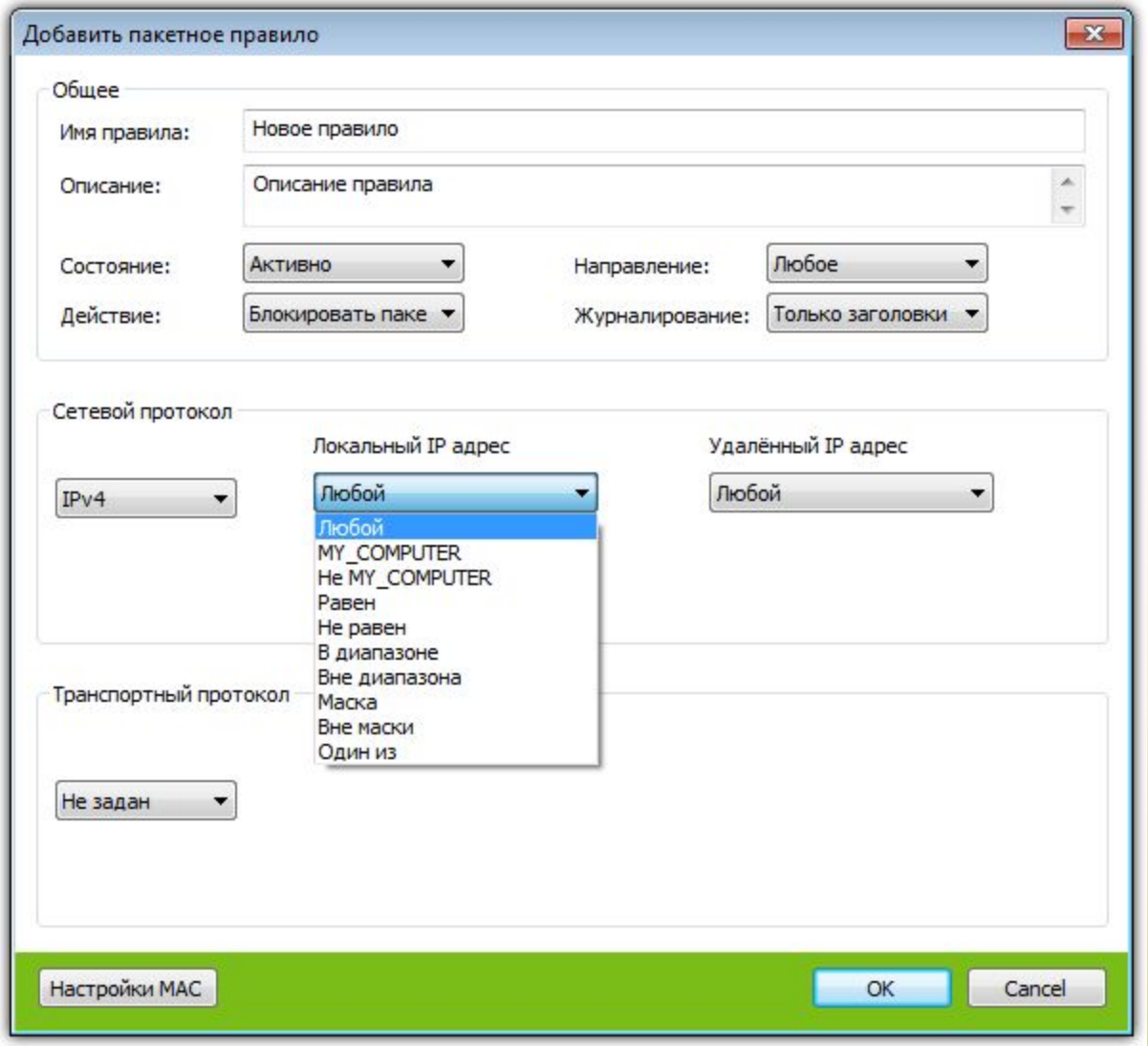


Защити созданное

Dr.WEB®
www.drweb.com

Создание своего правила

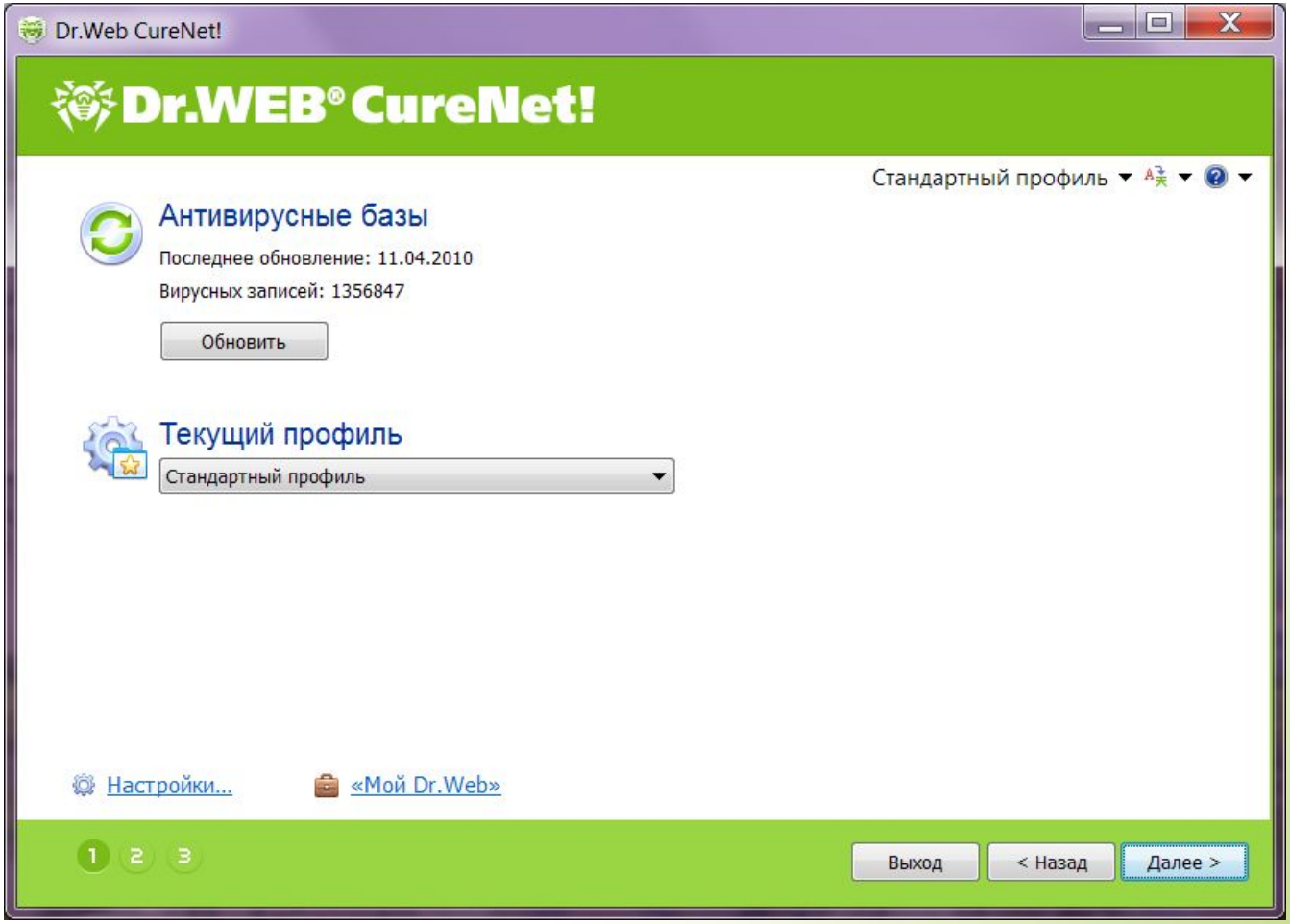
Защити созданное



Dr.WEB®
www.drweb.com

Защити созданное

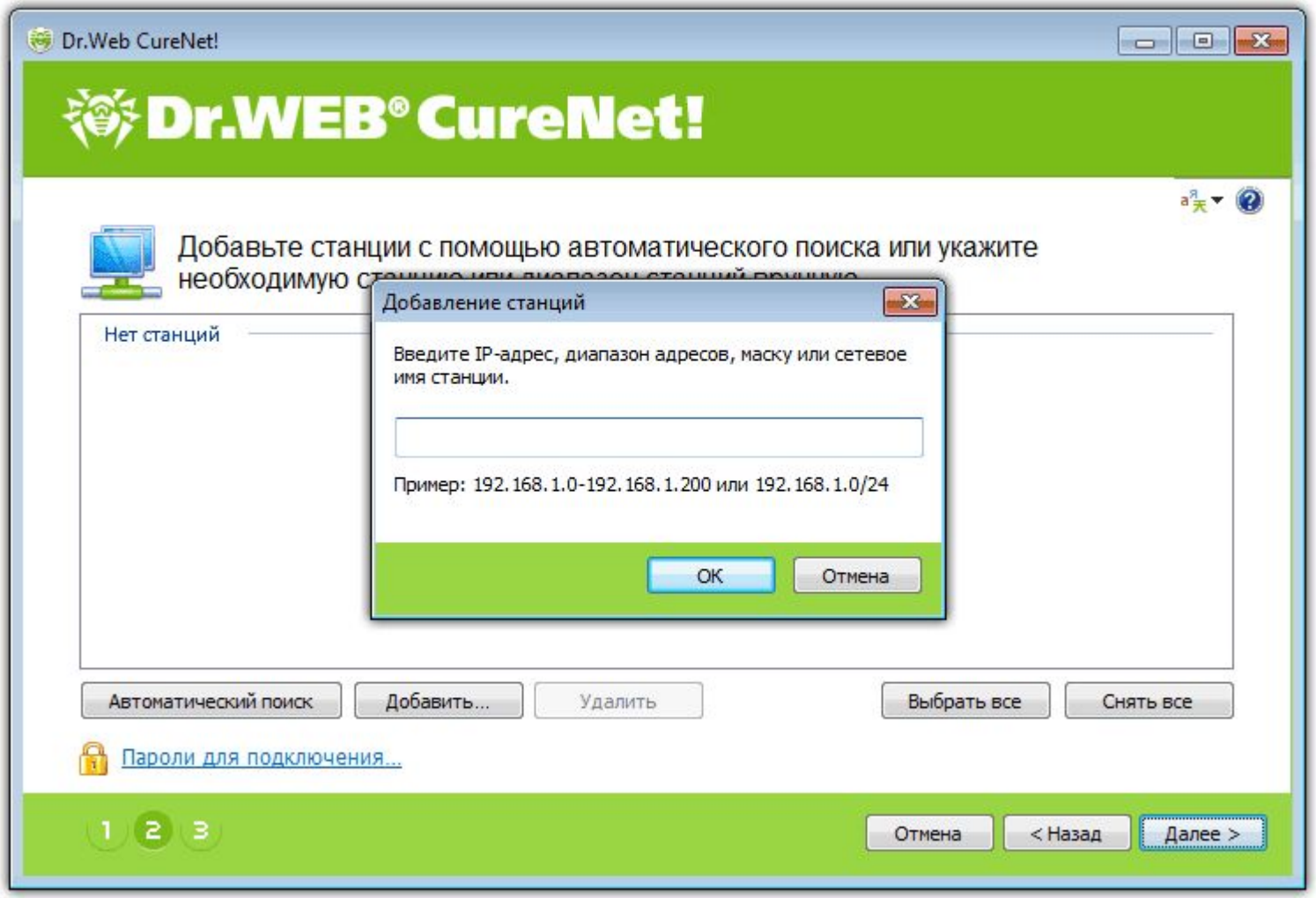
Обновление и первоначальные настройки



Dr.WEB®
www.drweb.com

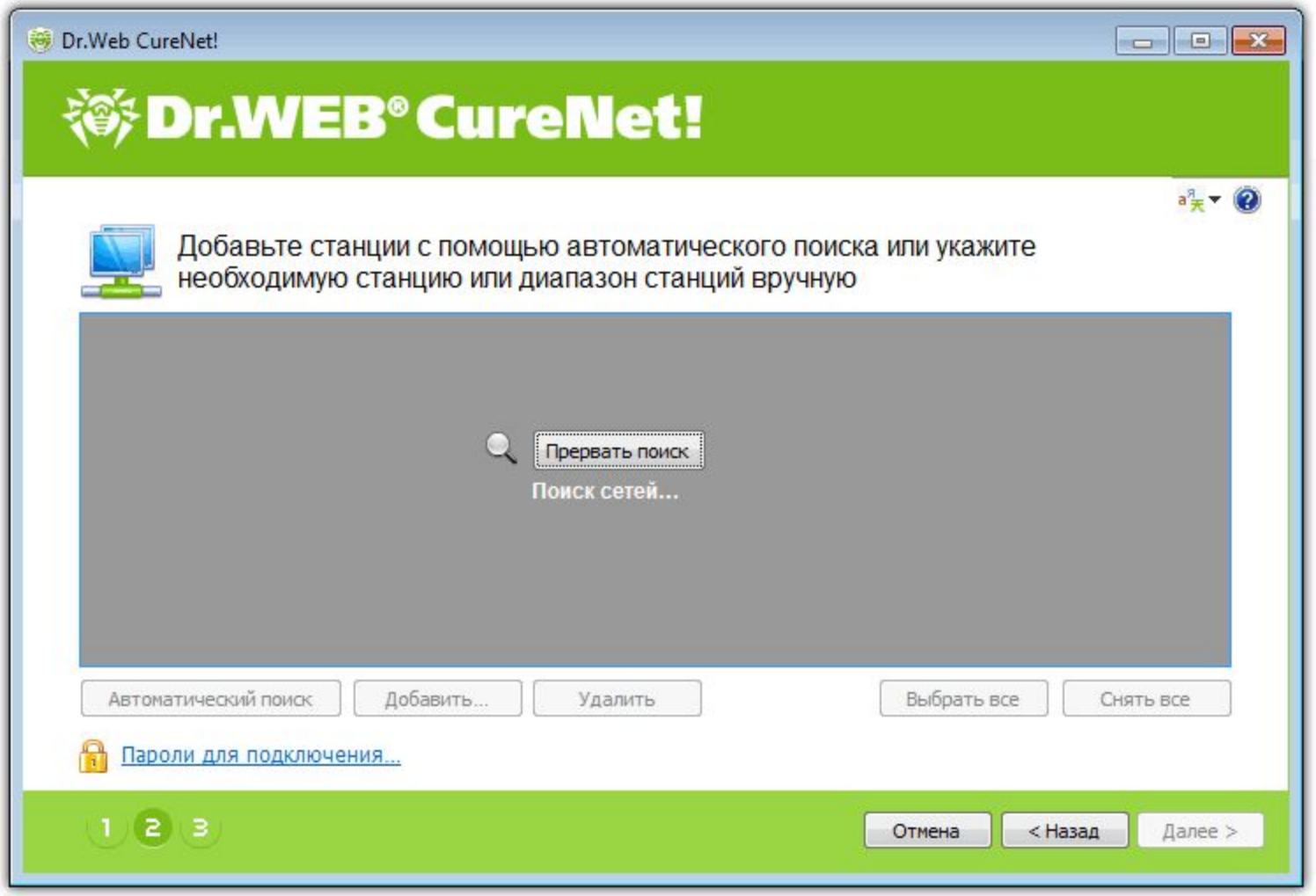
Добавление станций

Защити созданное



Dr.WEB®
www.drweb.com

Поиск сетей и компьютеров

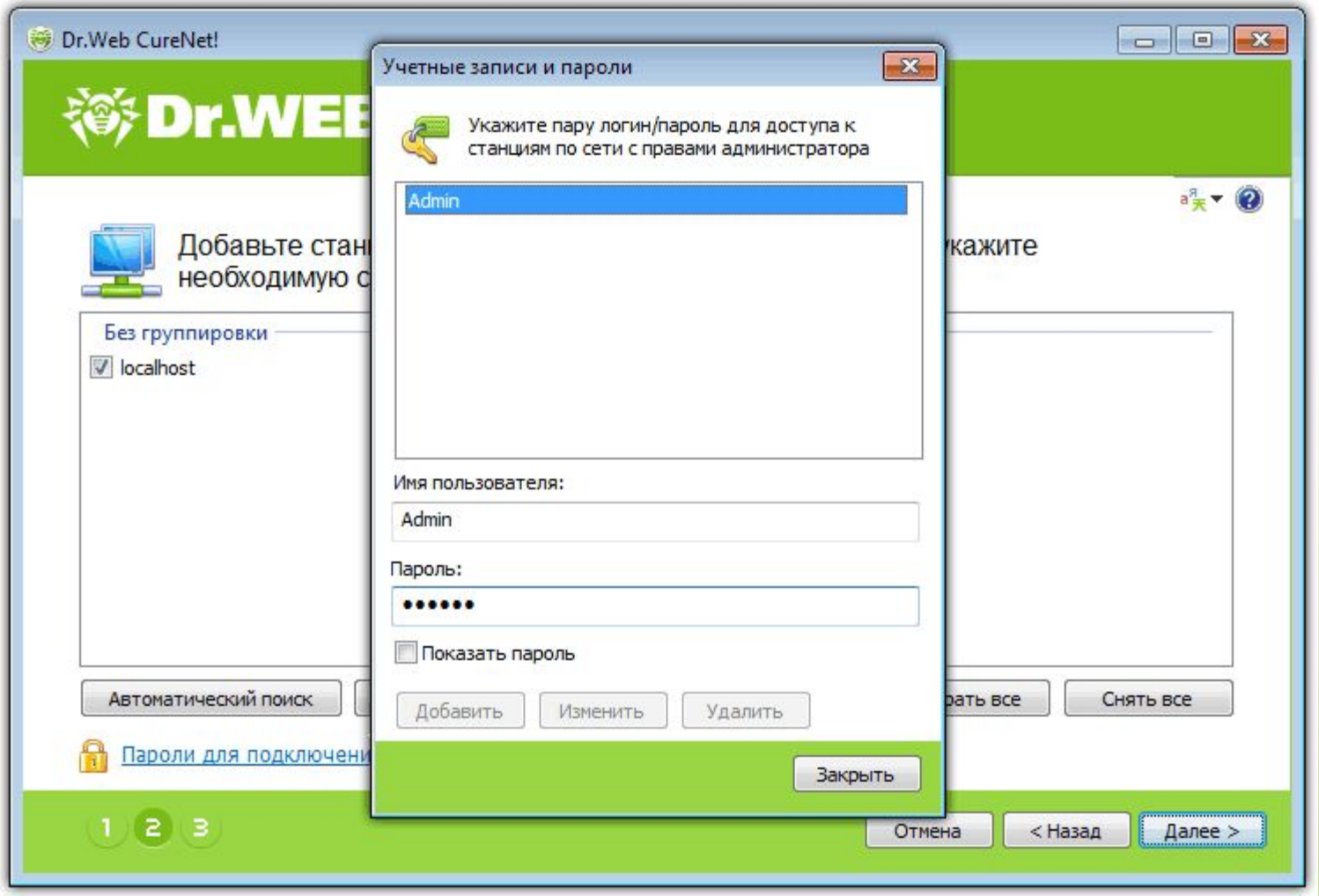


Защити созданное

Dr.WEB®
www.drweb.com

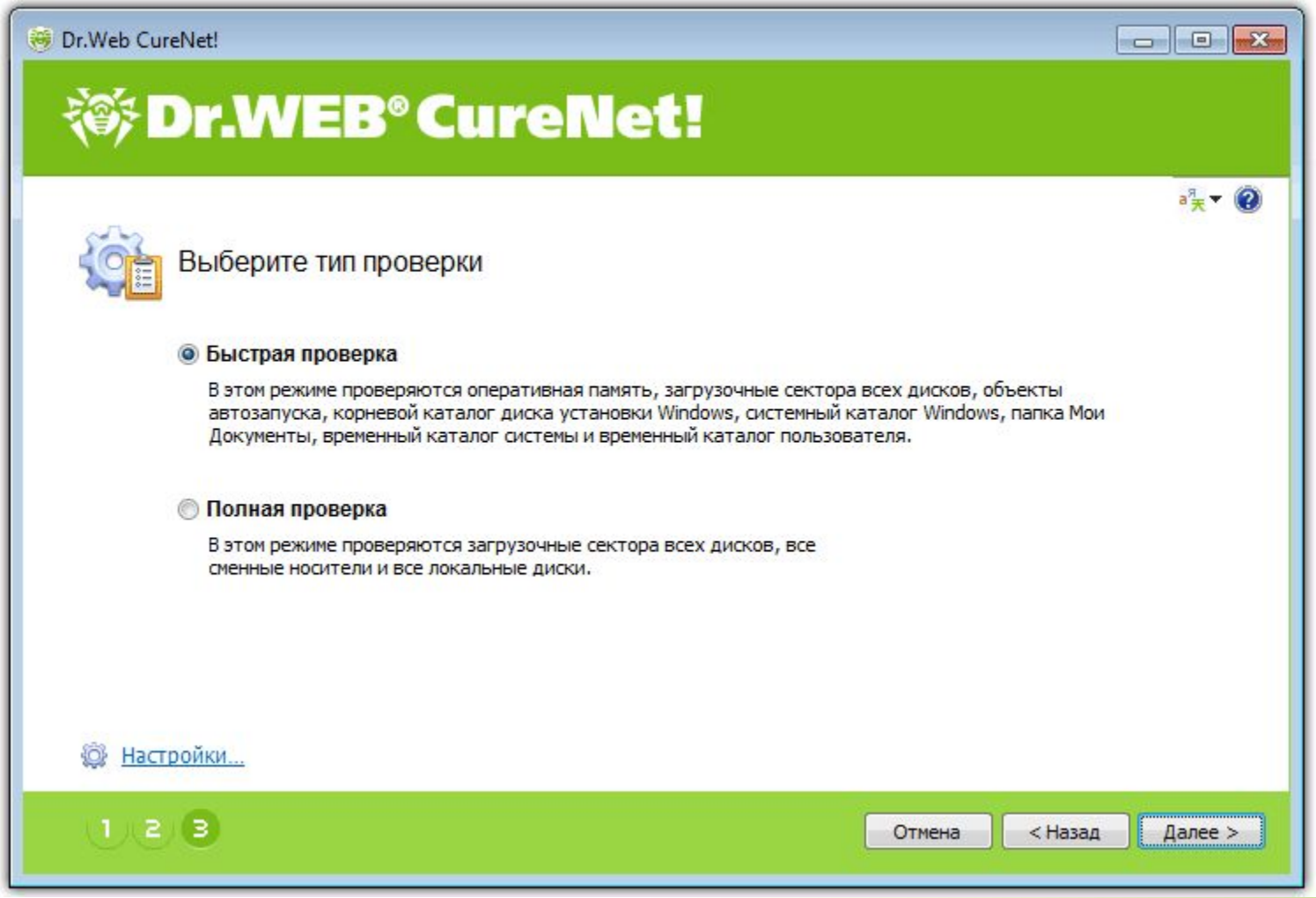
Учётные записи

Защити созданное



Dr.WEB®
www.drweb.com

Тип проверки

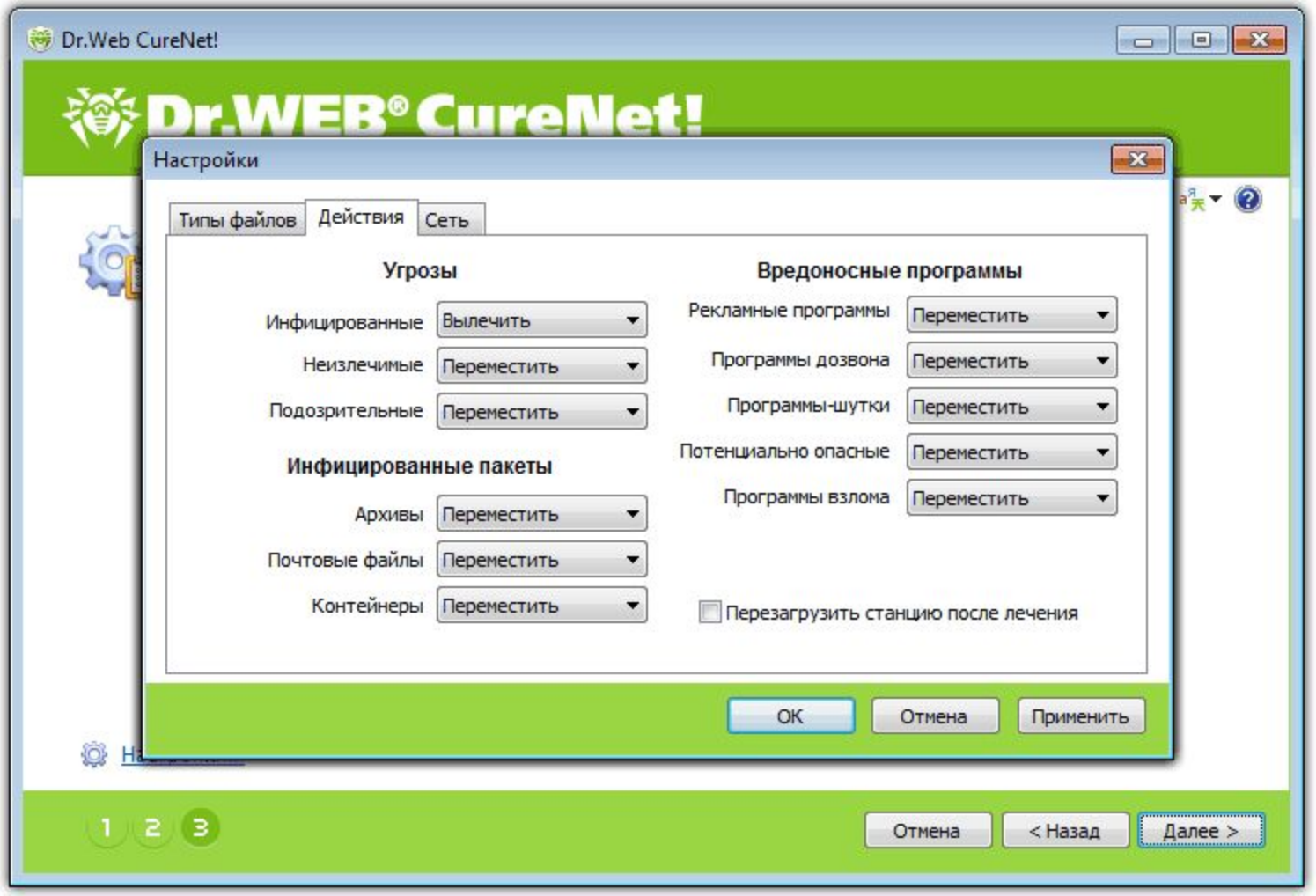


Защити созданное

Dr.WEB®
www.drweb.com

Настройки проверки

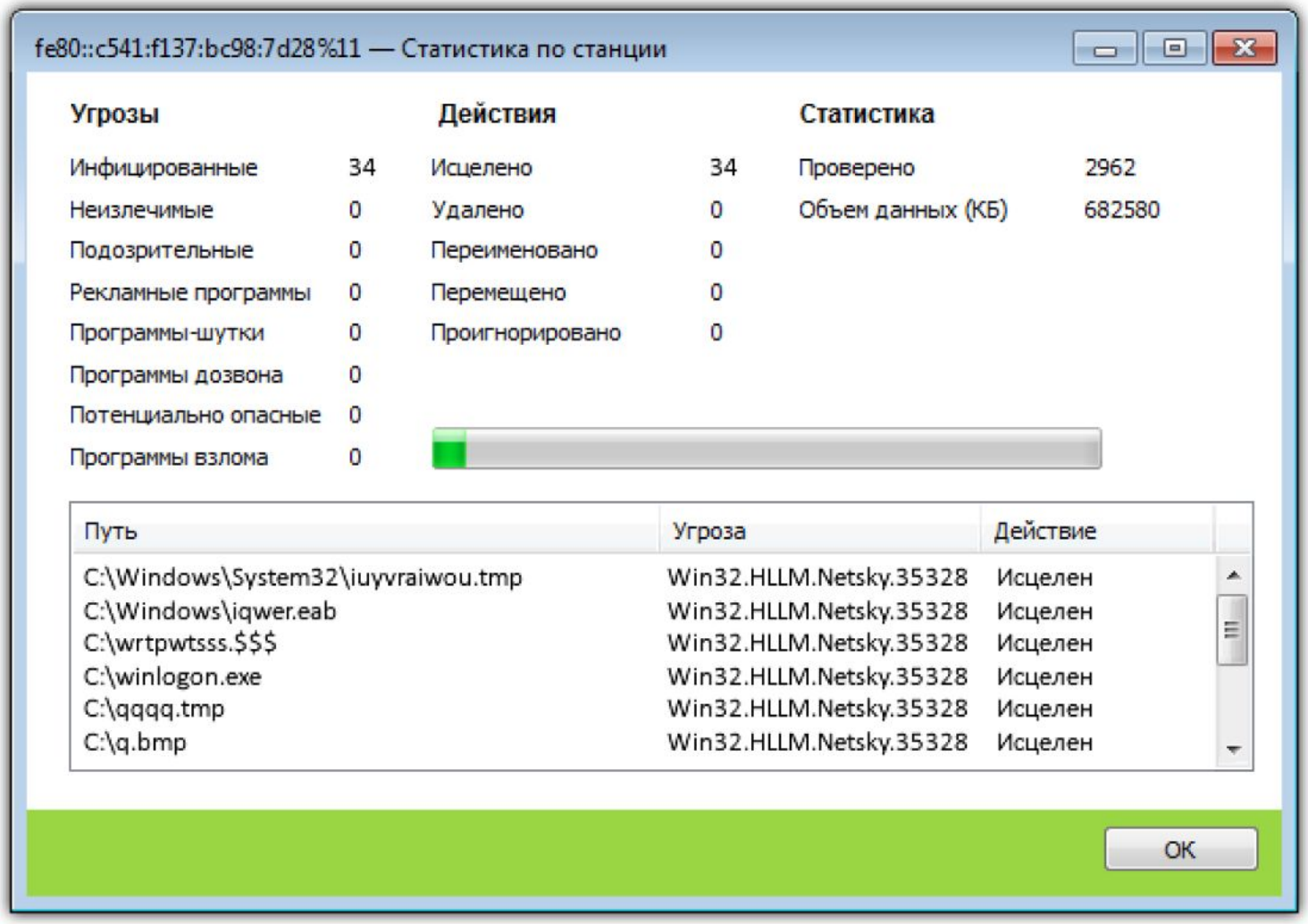
Защити созданное



Dr.WEB®
www.drweb.com

Статистика по станции

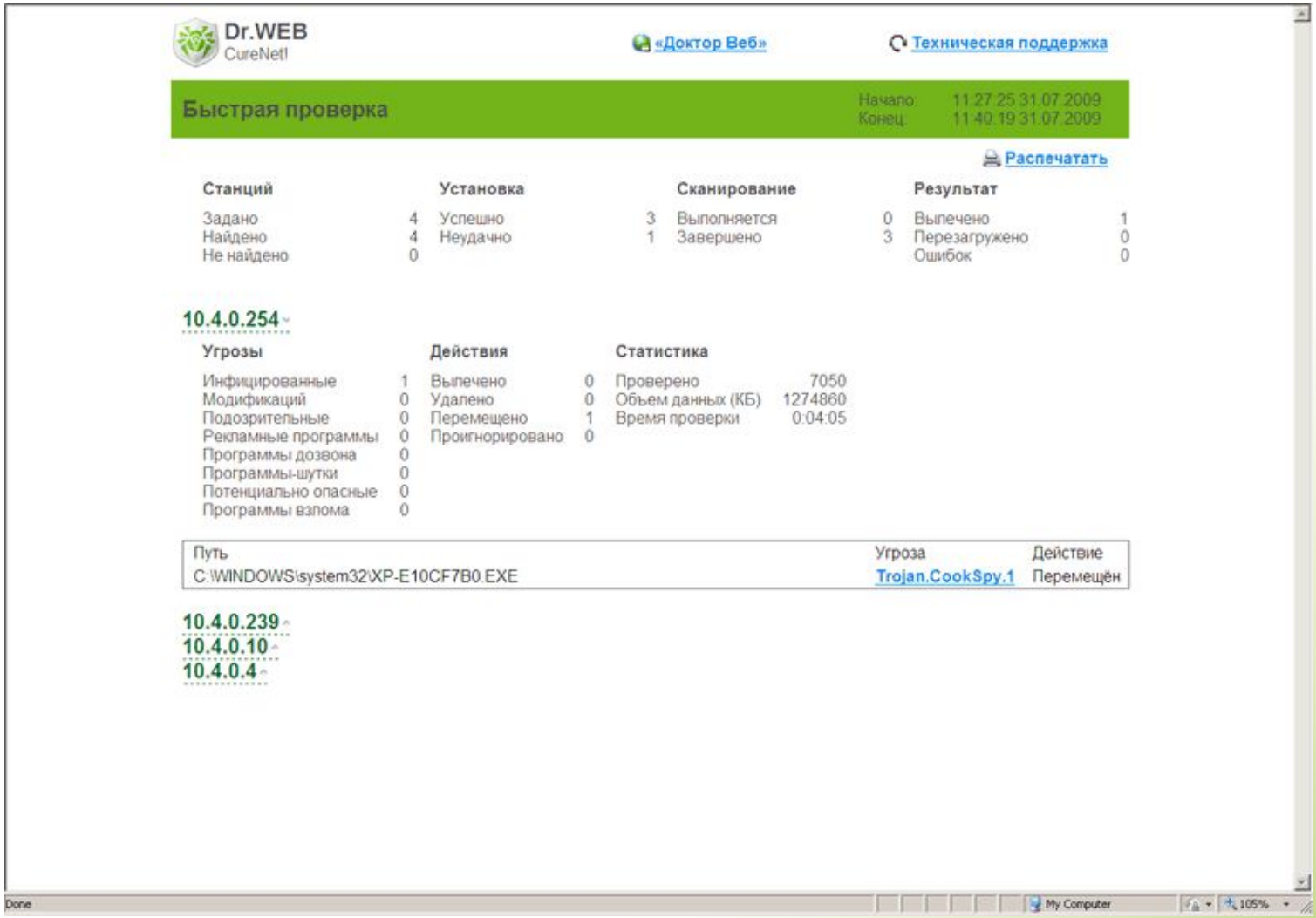
Защити созданное



Dr.WEB®
www.drweb.com

Отчёт

Защити созданное



Dr.WEB
CureNet!

«Доктор Веб» Техническая поддержка

Быстрая проверка

Начало: 11:27:25 31.07.2009
Конец: 11:40:19 31.07.2009

Распечатать

Станций		Установка		Сканирование		Результат	
Задано	4	Успешно	3	Выполняется	0	Вылечено	1
Найдено	4	Неудачно	1	Завершено	3	Перезагружено	0
Не найдено	0					Ошибок	0

10.4.0.254

Угрозы		Действия		Статистика	
Инфицированные	1	Вылечено	0	Проверено	7050
Модификаций	0	Удалено	0	Объем данных (КБ)	1274860
Подозрительные	0	Перемещено	1	Время проверки	0:04:05
Рекламные программы	0	Проигнорировано	0		
Программы дозвона	0				
Программы-шутки	0				
Потенциально опасные	0				
Программы взлома	0				

Путь	Угроза	Действие
C:\WINDOWS\system32\XP-E10CF7B0.EXE	Trojan.CookSpy.1	Перемещён

10.4.0.239
10.4.0.10
10.4.0.4

Done My Computer 105%

Dr.WEB®
www.drweb.com

Новые продукты

- Dr.Web для Windows, Dr.Web Security Space для Windows x64;
- Dr.Web для файловых серверов Windows (x64);
- Dr.Web для MS Exchange Server 2007;
- Dr.Web для Linux (с центром управления);
- Dr.Web LiveDemo;
- Dr.Web Security Space Pro (с файрволлом);
- Dr.Web для Symbian.

Защити созданное

Dr.WEB®
www.drweb.com

Бета-тестирование

- Dr.Web Enterprise Suite 6.0;
- Dr.Web для Qbik WinGate;
- Dr.Web FlyTrap (антиспам).

Защити созданное

Dr.WEB®
www.drweb.com

Бета-тестирование

Защити созданное

Новое в Dr.Web Enterprise Suite 6.0:

- Поддержка 64-битых систем Windows;
- Dr.Web Firewall;
- Централизованно управляемый карантин;
- Антивирусные агенты Novell Netware, Windows Mobile, Mac OS X, MS Exchange, Lotus;
- Группирование станций с произвольной вложенностью;
- Улучшение работы репозитория;
- Новый интерфейс сетевого инсталлятора;
- Только веб-консоль, java-консоль удалена

Dr.WEB®
www.drweb.com

Защити созданное

Технология Origins Tracing™

- Специальные записи в вирусной базе
- Функции поиска похожестей
- Сигнатурный детект

Dr.WEB®
www.drweb.com

Защити созданное

Технология FLY-CODE™

- Универсальный распаковщик
- Специальные записи в вирусной базе
- Эвристическое предположение

Dr.WEB®
www.drweb.com

Защити созданное

Антируткит Dr.Web® Shield™

- ✔ реализован в виде драйвера и действует на самом низком системном уровне;
- ✔ помогает компонентам антивируса Dr.WEB® для MS Windows™ обнаруживать вирусы, скрывающие своё присутствие в системе;
- ✔ позволяет антивирусу Dr.WEB® получать полный доступ к файлам, к которым обычно доступ запрещён системой;
- ✔ позволяет гораздо эффективнее, чем прежде, противодействовать активным вредоносным программам, находящимся в системе MS Windows™

Dr.WEB®
www.drweb.com

Защити созданное

Самозащита Dr.Web SelfPROtect™

ограничивает доступ вредоносных объектов:

- ✔ к сети;
- ✔ файлам и папкам;
- ✔ веткам реестра;
- ✔ сменным носителям;
- ✔ защищает от попыток антивирусных программ прекратить функционирование Dr.WEB®

Dr.WEB®
www.drweb.com

Защити созданное

Контактные данные:

Обратная связь компании «Доктор Веб»:

https://support.drweb.com/new/feedback

Образовательные программы:

http://training.drweb.com

Горячая лента угроз:

http://news.drweb.com/list/?c=23

E-mail: education@drweb.com

Спасибо за внимание!