

Современные вирусные угрозы Технологические новинки Dr.Web

14 мая 2010 г.

Валерий
Ледовской



План:

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

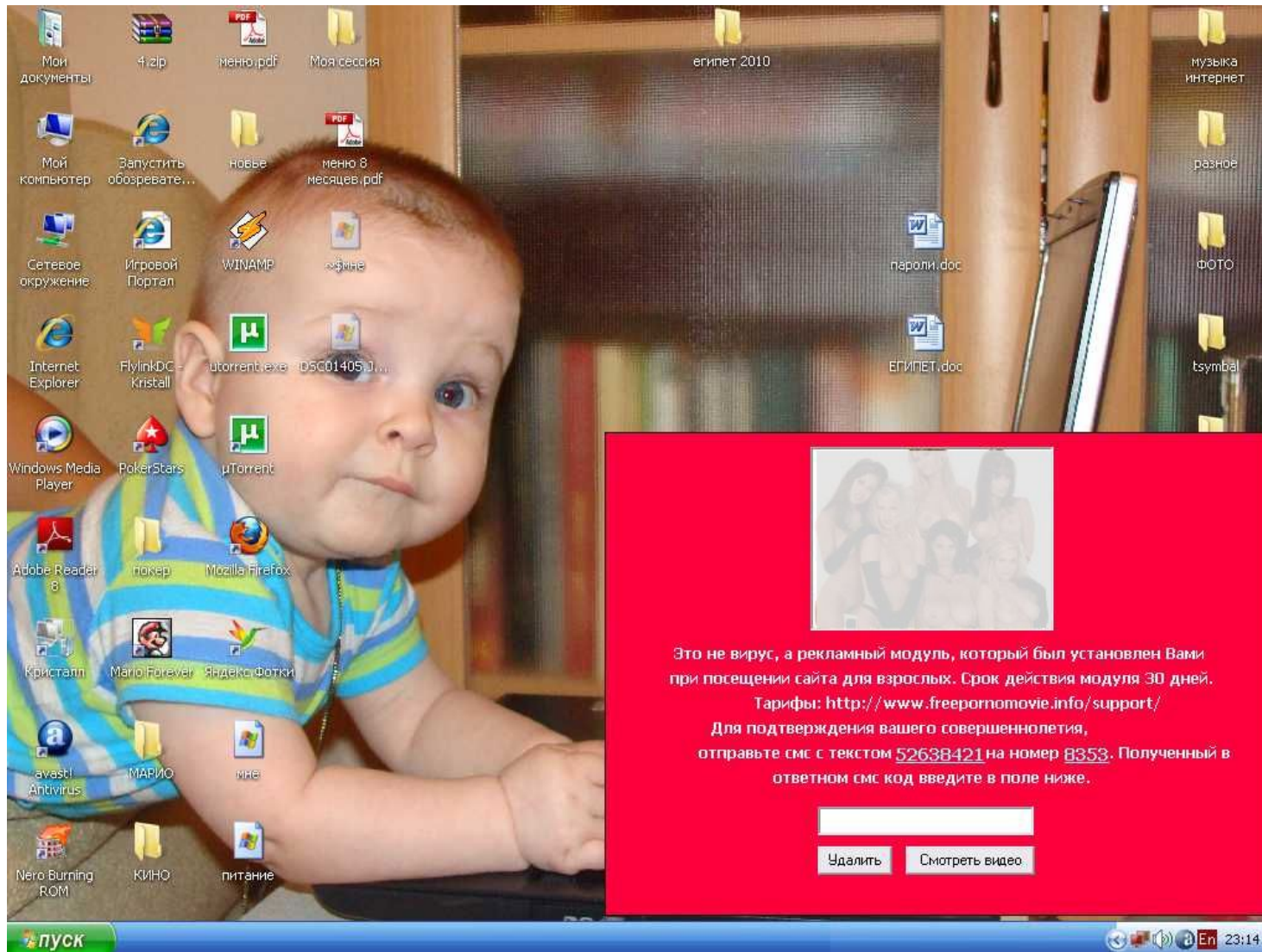
Пишут ли сотрудники АВ-компаний вирусы?



- 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**

Trojan.Winlock

Защити созданное



The screenshot shows a Windows XP desktop environment. The background is a photograph of a baby sitting at a desk. The desktop is cluttered with various icons, including folders like 'Мои документы', 'Мой компьютер', and 'Сетевое окружение', as well as application icons like 'Internet Explorer', 'FlylinkDC - Kristall', 'uTorrent', 'PokerStars', 'Adobe Reader 8', 'Кристалл', 'avast! Antivirus', and 'Nero Burning ROM'. A red dialog box is overlaid on the bottom right of the screen. It contains a small image of a group of women, followed by Russian text: 'Это не вирус, а рекламный модуль, который был установлен Вами при посещении сайта для взрослых. Срок действия модуля 30 дней. Тарифы: <http://www.freeromovie.info/support/> Для подтверждения вашего совершеннолетия, отправьте SMS с текстом 52638421 на номер 8353. Полученный в ответном SMS код введите в поле ниже.' Below the text is an empty input field and two buttons: 'Удалить' and 'Смотреть видео'. The Windows taskbar at the bottom shows the 'Пуск' button and system tray icons, including the clock showing 23:14.

К сожалению время бесплатного просмотра ПОРНО роликов закончилось.

Для продолжения просмотра Порно роликов, Вам необходимо совершить следующие действия:

В любом терминале оплаты пополните счет 892847490 на 390 рублей в платежной системе РВК Money

(платежные системы =>электронные деньги => РВК Money)

После оплаты, на выданном чеке будет находиться код который необходимо ввести в форму для ввода кода.

Просматривая бесплатную часть ПОРНО роликов Вы согласились с [правилами использования сайта](#)

Приятного просмотра!

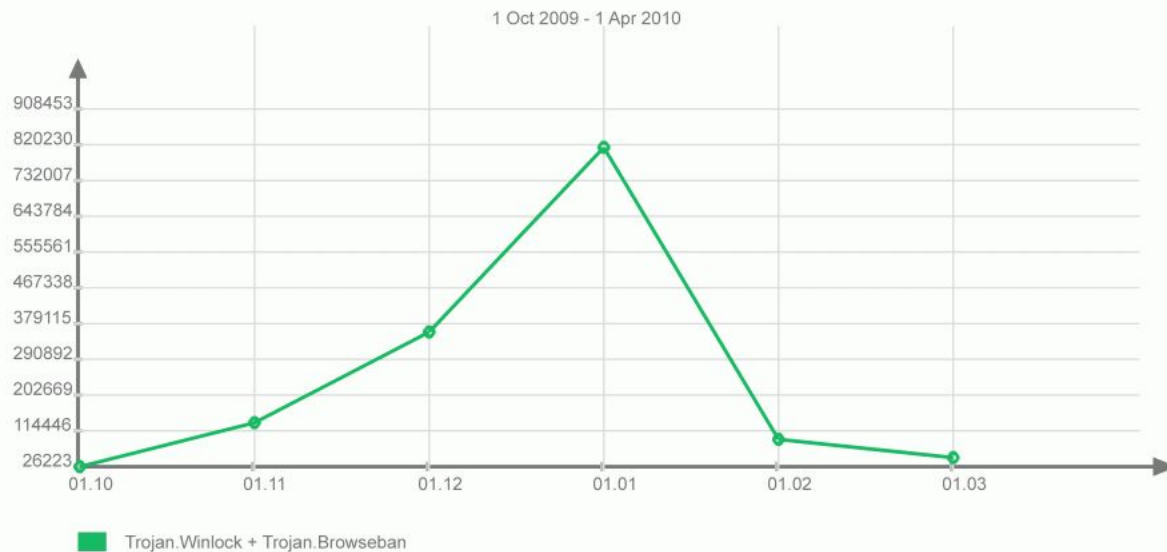
Ваш Код:

ВОЙТИ

ОТМЕНА

Масштабы Trojan.Winlock

Защити созданное



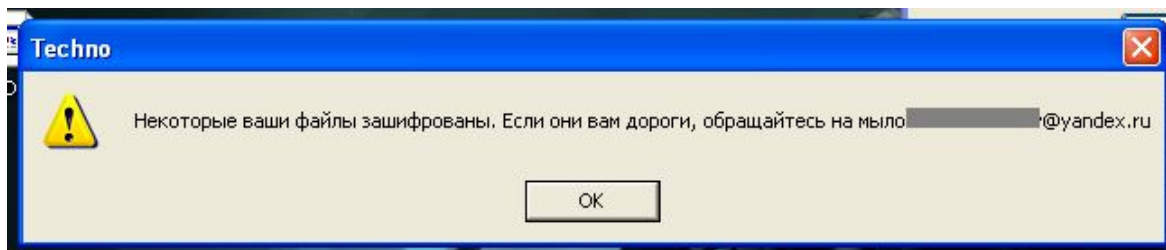
Январь 2010 (оценка):

**- количество пострадавших пользователей:
несколько млн.**

- доход злоумышленников: сотни миллионов рублей

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>



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

Дешифровка от Trojan.Encoder.68

Подробнее в новости [Trojan.Encoder.68 архивирует файлы с длинным паролем.](#)

ID:

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](#)

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).



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

Ботсеть

Trojan.Oficla

Описание:

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

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

FULL - Эта версия лoaderа 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 монетизацию их работы. Поэтому в эту версию лoaderа встроен лучший движок по пробиву фаерволов, 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 лoaderом будет жить максимально долго. Так же в этой версии лoaderа в админке присутствует Builder, для возможности клиентом получения лoaderа прямо из его админки с возможностью записи параметра adv. Данный параметр отвечает за уникальность специального номера билда. Таким образом клиент может сделать несколько билдов с разными параметрами adv и раздать билды разным адвертам. При прогрузке 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 urlа - 90\$

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

Защити созданное



Идентификатор:

Пароль:

Войти



Вопросы по работе Сбербанк Онл@йн: +7 (495) 500-5550 или 8-800-555-5550



Raiffeisen CONNECT

«Мы сохраняем уверенность в высоком потенциале Российской экономики. Группа Райффайзен всегда подержала неизменность выбранной в России стратегии и готовность всецело поддерживать развитие ЗАО «Райффайзенбанк», самого крупного и успешного дочернего банка в Группе Райффайзен Интернациональ».



Председатель правления, Райффайзен Интернациональ Банк-Холдинг АГ

Сегодня среда, 07 апреля 2010

[Правила обслуживания](#)

[Тарифы](#)

[Курсы валют](#)

[Помощь](#)

[PDA-версия](#)

**НАДЕЖНЫМ
ЛЮДЯМ –
ОТЛИЧНЫЕ
СТАВКИ!**

**СТАВКИ
СНИЖЕНЫ**

Добро пожаловать!

Для входа в систему необходимо ввести ваше имя пользователя, пароль доступа и авторизационный код (2), указанный на картинке:

Имя пользователя

Пароль

Авторизационный код



Новости Райффайзенбанка:

06.04.2010 ЗАО «Райффайзенбанк» открылся в центре Калуги

05.04.2010 ЗАО «Райффайзенбанк» сообщает об улучшении условий ипотечного кредитования

01.04.2010 Райффайзен вновь признан «Лучшим банком в Центральной и Восточной Европе» журналом Global Finance

[все новости](#)

Новости дистанционного обслуживания:

WebMoney  Enter

поиск

[RU/EN](#) | [Справочная служба](#) | [wiki](#)

Если вы уже зарегистрированы в системе WEBMONEY TRANSFER, введите

Email или WMID

пароль, указанный при регистрации

число, изображенное на картинке



Искать

или можете просто войти кипером, и мы поищем другие ваши регистрации

Войти и искать

Если вы еще не зарегистрированы - **ПРИСОЕДИНЯЙТЕСЬ!**

По указанным данным мы найдем ваши регистрации в системе WebMoney Transfer и для каждой создадим ярлык для быстрого запуска. Если вы не помните свои данные, можете использовать ссылки расположенные ниже.



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

Корпоративные сети:

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



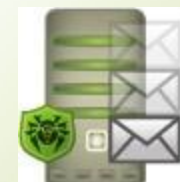
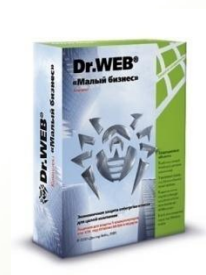
Защита рабочих станций:

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



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

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 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.



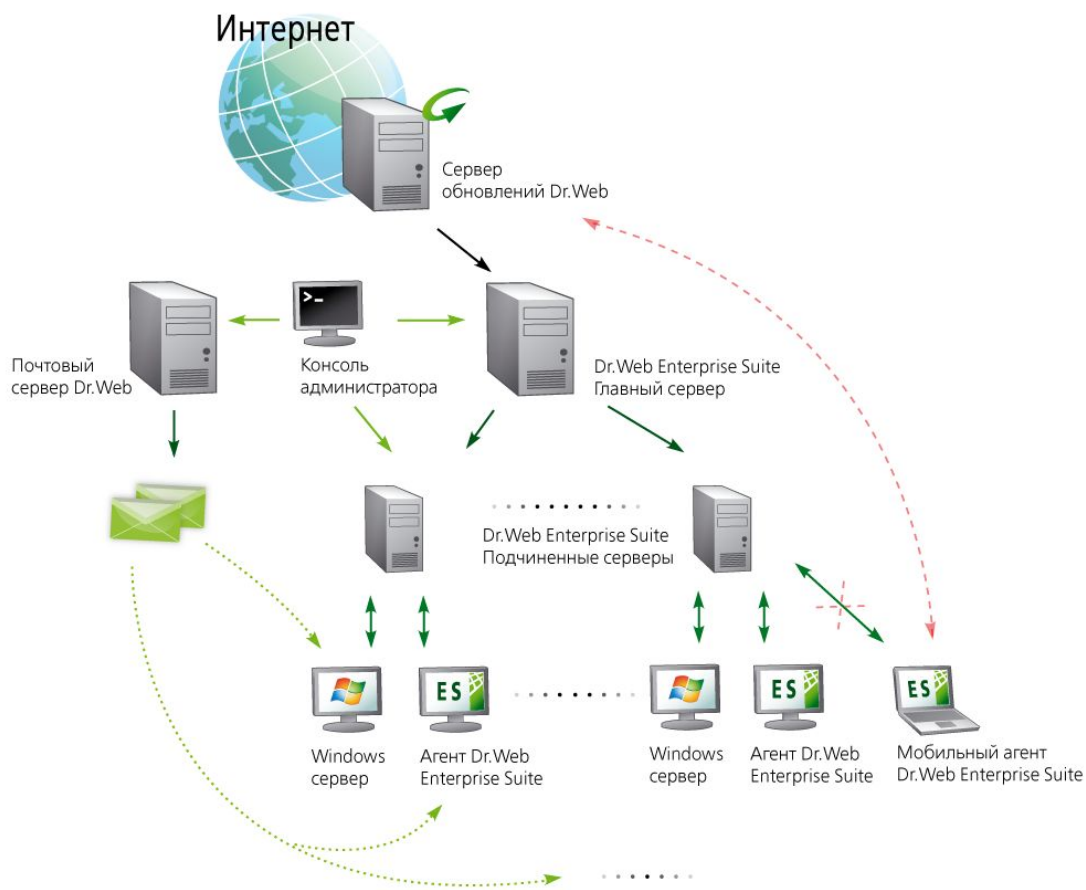
Повышение производительности труда путем снижения количества отвлекающих факторов.

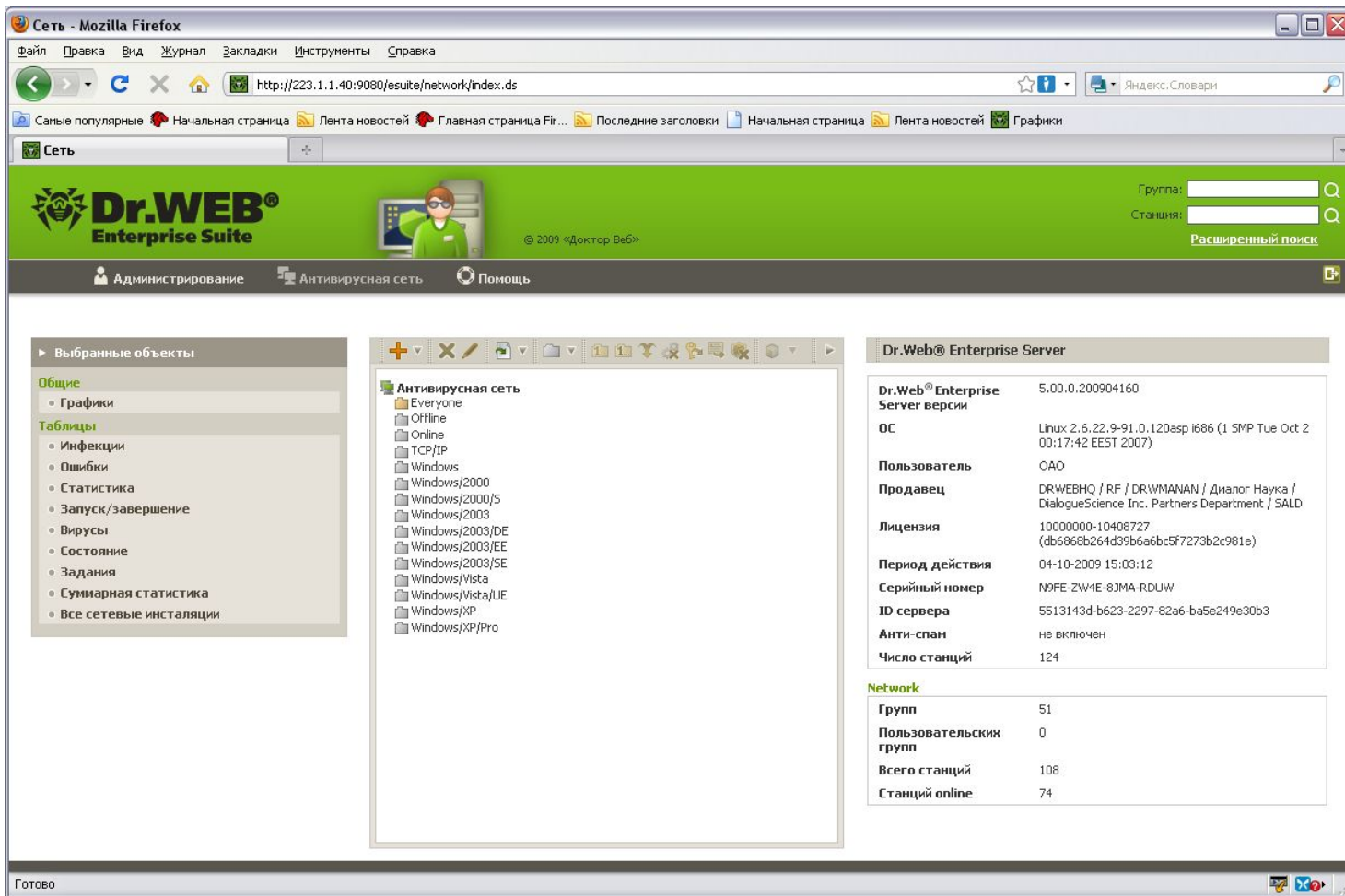
Оптимизация расходов на интернет-трафик и контроль за деятельностью сотрудников в сети Интернет.

Логическая схема работы Dr.Web Enterprise Suite

Защити созданное

Dr.Web® Enterprise Suite





Сеть - Mozilla Firefox
http://223.1.1.40:9080/esuite/network/index.ds

Сеть

Dr.WEB® Enterprise Suite © 2009 «Доктор Веб»

Администрирование | Антивирусная сеть | Помощь

Выбранные объекты

Общие

- Графики

Таблицы

- Инфекции
- Ошибки
- Статистика
- Запуск/завершение
- Вирусы
- Состояние
- Задания
- Суммарная статистика
- Все сетевые инсталляции

Антивирусная сеть

- Everyone
- Offline
- Online
- TCP/IP
- Windows
- Windows/2000
- Windows/2000/S
- Windows/2003
- Windows/2003/DE
- Windows/2003/EE
- Windows/2003/SE
- Windows/Vista
- Windows/Vista/UE
- Windows/XP
- Windows/XP/Pro

Dr.Web® Enterprise Server

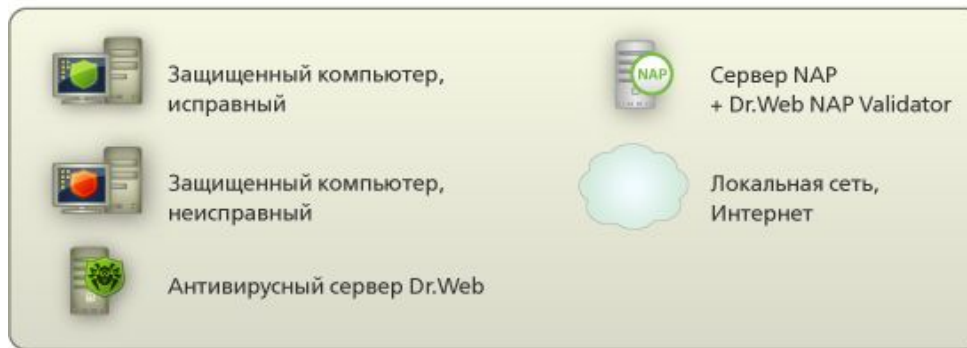
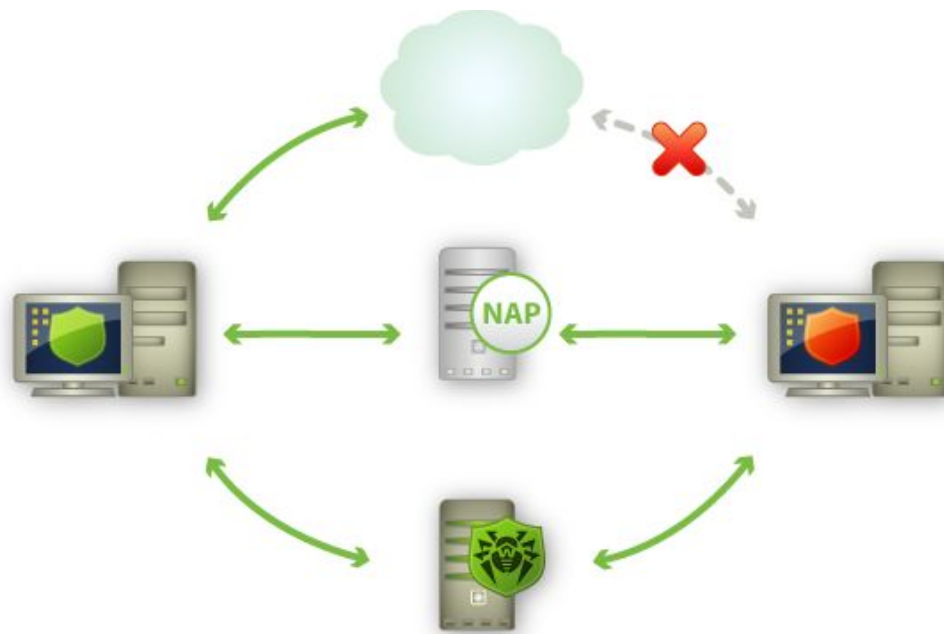
Dr.Web® Enterprise Server версии	5.00.0.200904160
ОС	Linux 2.6.22.9-91.0.120asr i686 (1 SMP Tue Oct 2 00:17:42 EEST 2007)
Пользователь	OAO
Продавец	DRWEBHQ / RF / DRWMANAN / Диалог Наука / DialogueScience Inc. Partners Department / SALD
Лицензия	1000000-10408727 (db6868b264d39b6a6bc5f7273b2c981e)
Период действия	04-10-2009 15:03:12
Серийный номер	N9FE-ZW4E-8JMA-RDUW
ID сервера	5513143d-b623-2297-82a6-ba5e249e30b3
Анти-спам	не включен
Число станций	124

Network

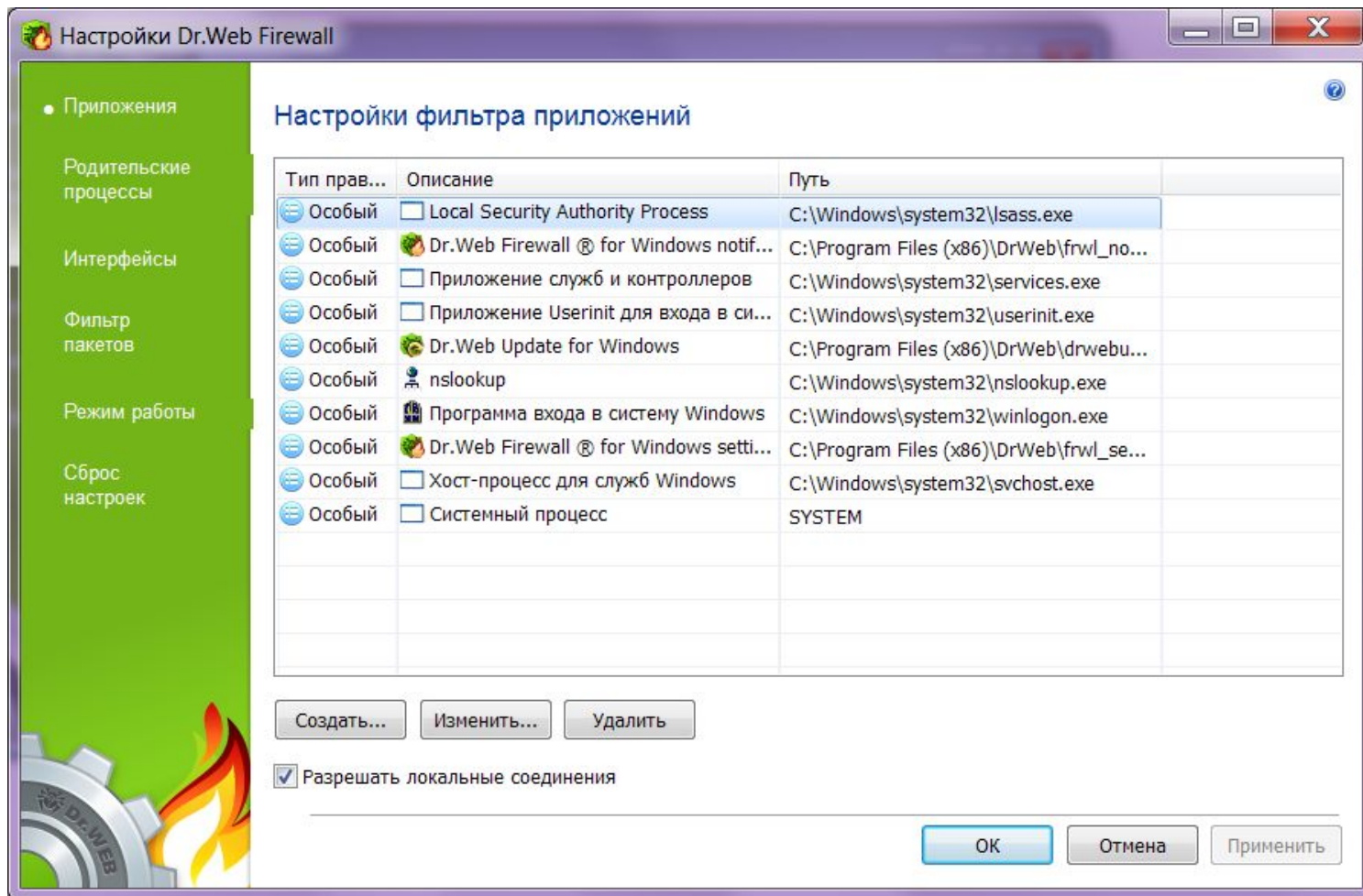
Групп	51
Пользовательских групп	0
Всего станций	108
Станций online	74

Готово

Поддержка технологии Microsoft Network Access Protection (NAP)



Защити созданное



Родительские процессы

Защити созданное

Настройки Dr.Web Firewall

Приложения

Родительские процессы








Интерфейсы

Фильтр пакетов

Режим работы

Сброс настроек

Настройка родительских приложений

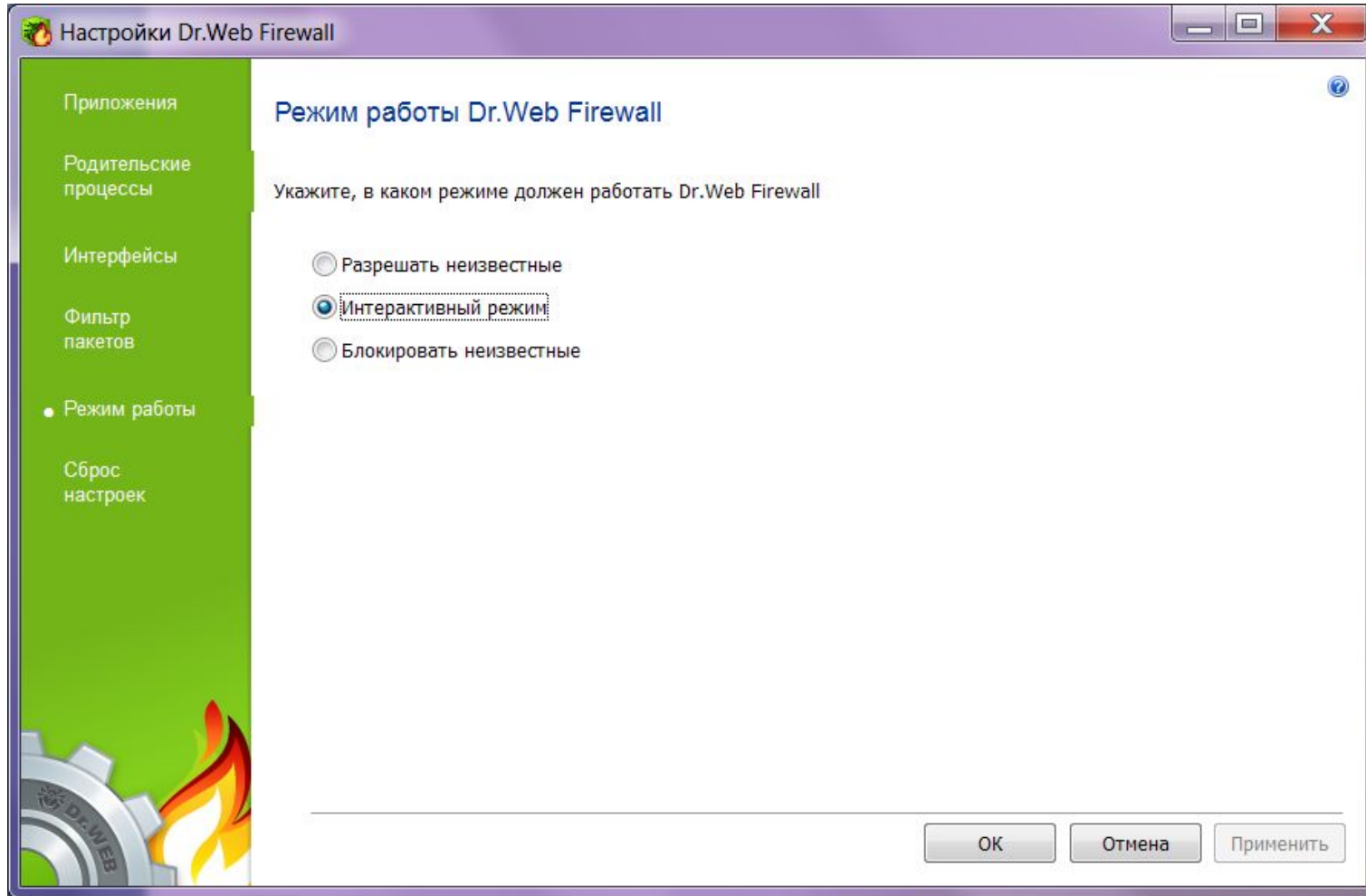
Приложение	Разрешить	Блокировать	Путь
 Dr.Web Firewall ® for Windows ...	<input checked="" type="radio"/>	<input type="radio"/>	C:\Program Files (x86)\DrWeb\frwl_no...
<input type="checkbox"/> Приложение служб и контролле...	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\system32\services.exe
<input type="checkbox"/> Диспетчер сеанса Windows	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\system32\smss.exe
<input type="checkbox"/> Приложение Userinit для входа ...	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\system32\userinit.exe
 SpIDer Agent for Windows	<input checked="" type="radio"/>	<input type="radio"/>	C:\Program Files (x86)\DrWeb\spidera...
 Программа входа в систему Win...	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\system32\winlogon.exe
 Программа завершающей стади...	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\SysWOW64\runonce.exe
 Программа завершающей стади...	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\system32\runonce.exe
 Проводник	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\explorer.exe
<input type="checkbox"/> Автозагрузка приложений Wind...	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\system32\wininit.exe
 Обработчик команд Windows	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\system32\cmd.exe
<input type="checkbox"/> Хост-процесс для служб Windows	<input checked="" type="radio"/>	<input type="radio"/>	C:\Windows\system32\svchost.exe
<input type="checkbox"/> SYSTEM	<input checked="" type="radio"/>	<input type="radio"/>	SYSTEM

Создать... | Удалить

OK | Отмена | Применить

Режимы работы


Защити созданное





Обучение Dr.Web Firewall


Защити созданное

Уведомление Dr.Web Firewall

 **Internet Explorer**

Dr.Web Firewall обнаружил попытку доступа к сети

Приложение	 Internet Explorer
Путь к приложению:	C:\program files\internet explorer\iexplore.exe
Цифровая подпись:	 Microsoft Corporation
Целевой адрес:	tcp://65.55.17.26
Порт:	80 (www-http)
Направление:	Исходящее

 **Внимание:**
- Отсутствует сетевое правило для приложения

Создание своего правила

Защити созданное

Добавить пакетное правило

Общее

Имя правила: Новое правило

Описание: Описание правила

Состояние: Направление:

Действие: Журналирование:

Сетевой протокол

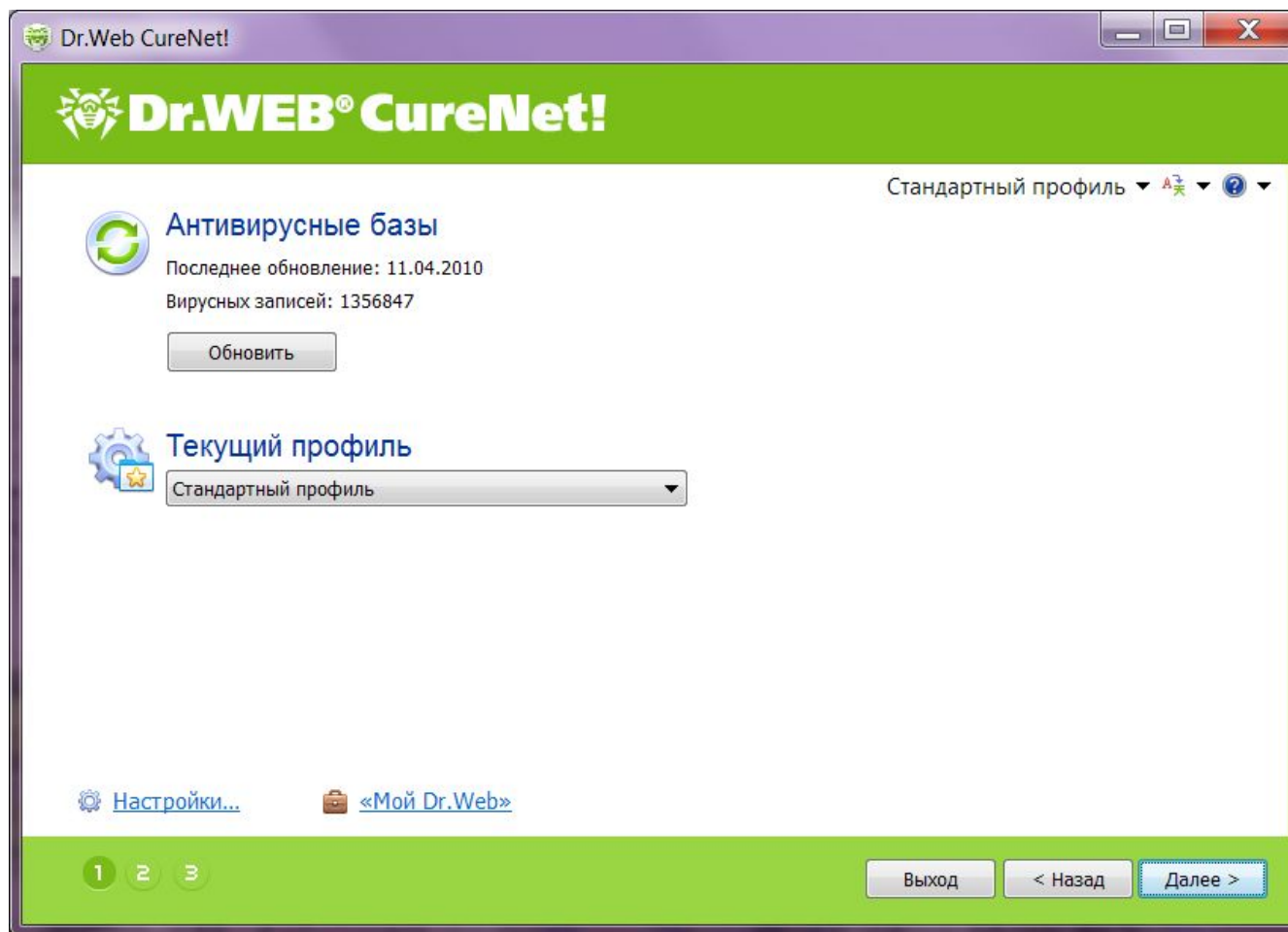
Локальный IP адрес: Удалённый IP адрес:

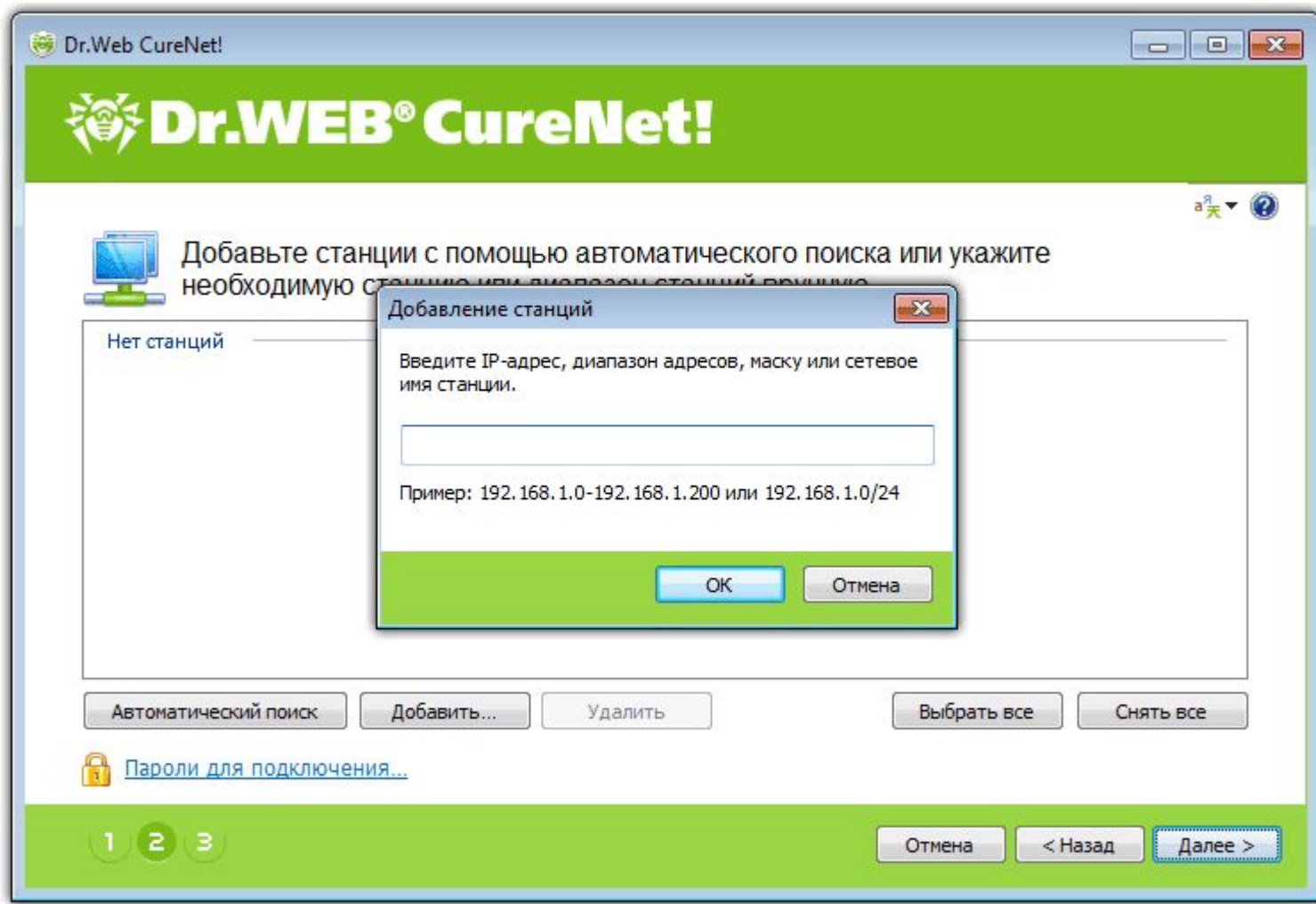
Транспортный протокол:

Настройки MAC

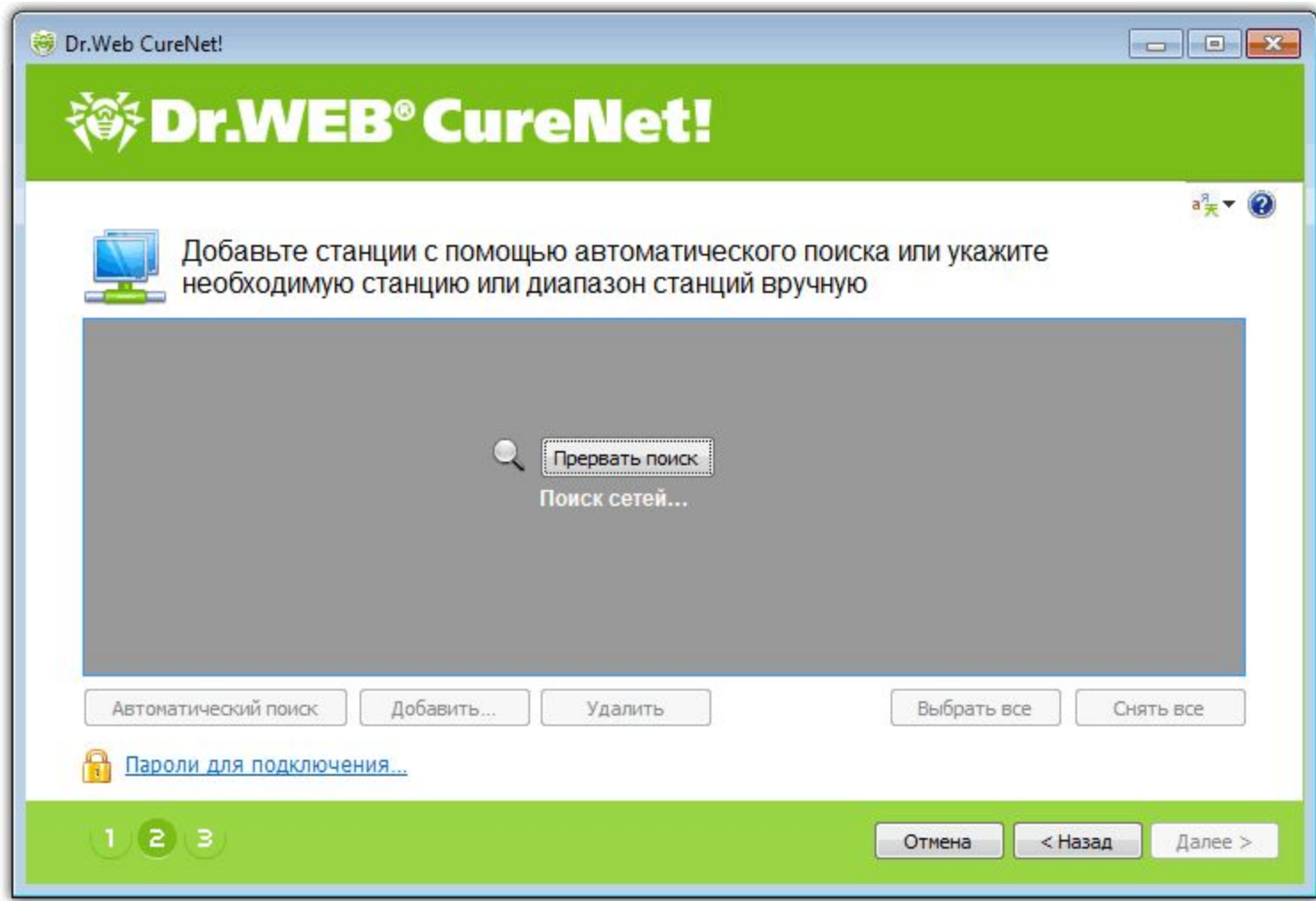
Обновление и первоначальные настройки

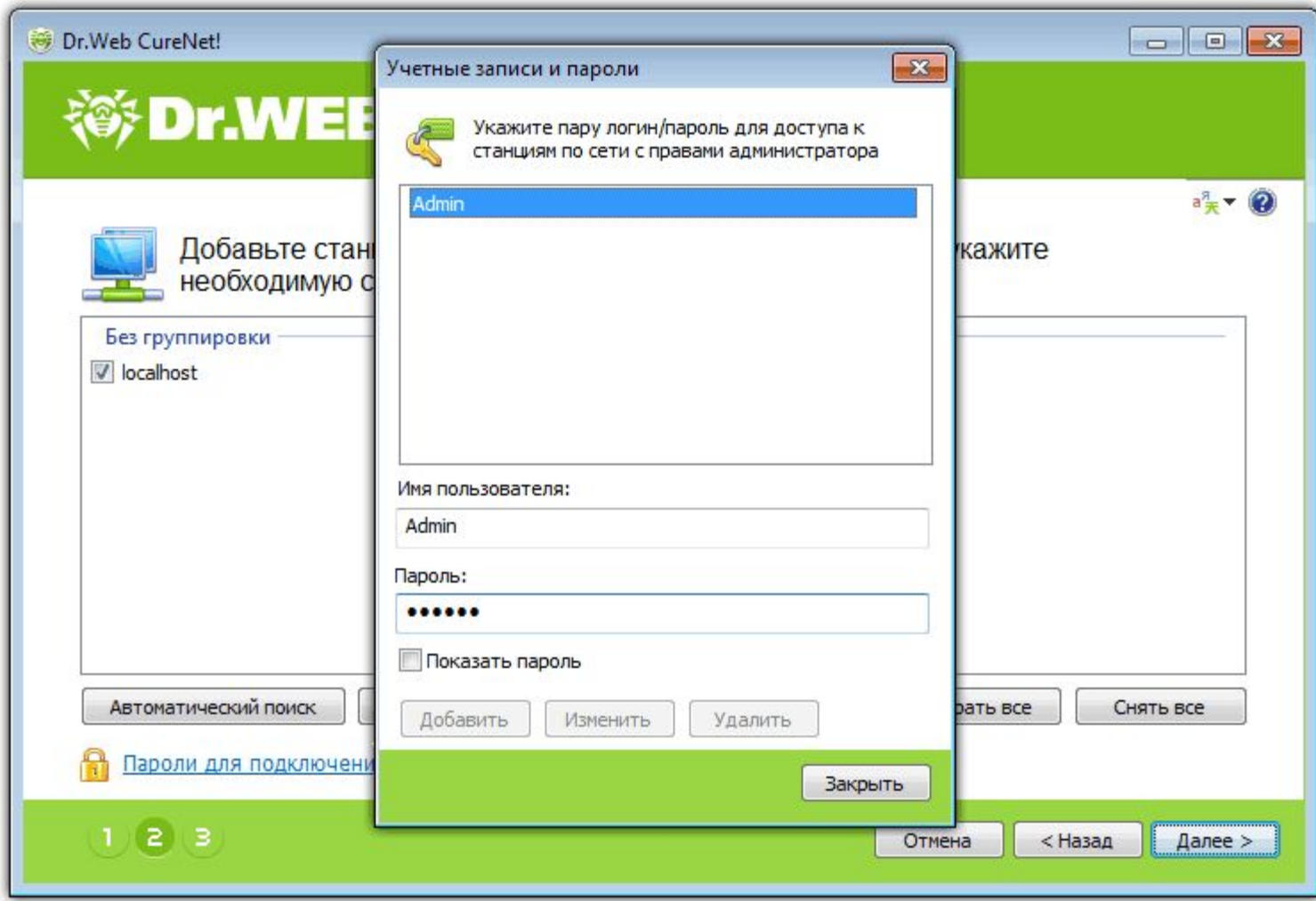
Защити созданное

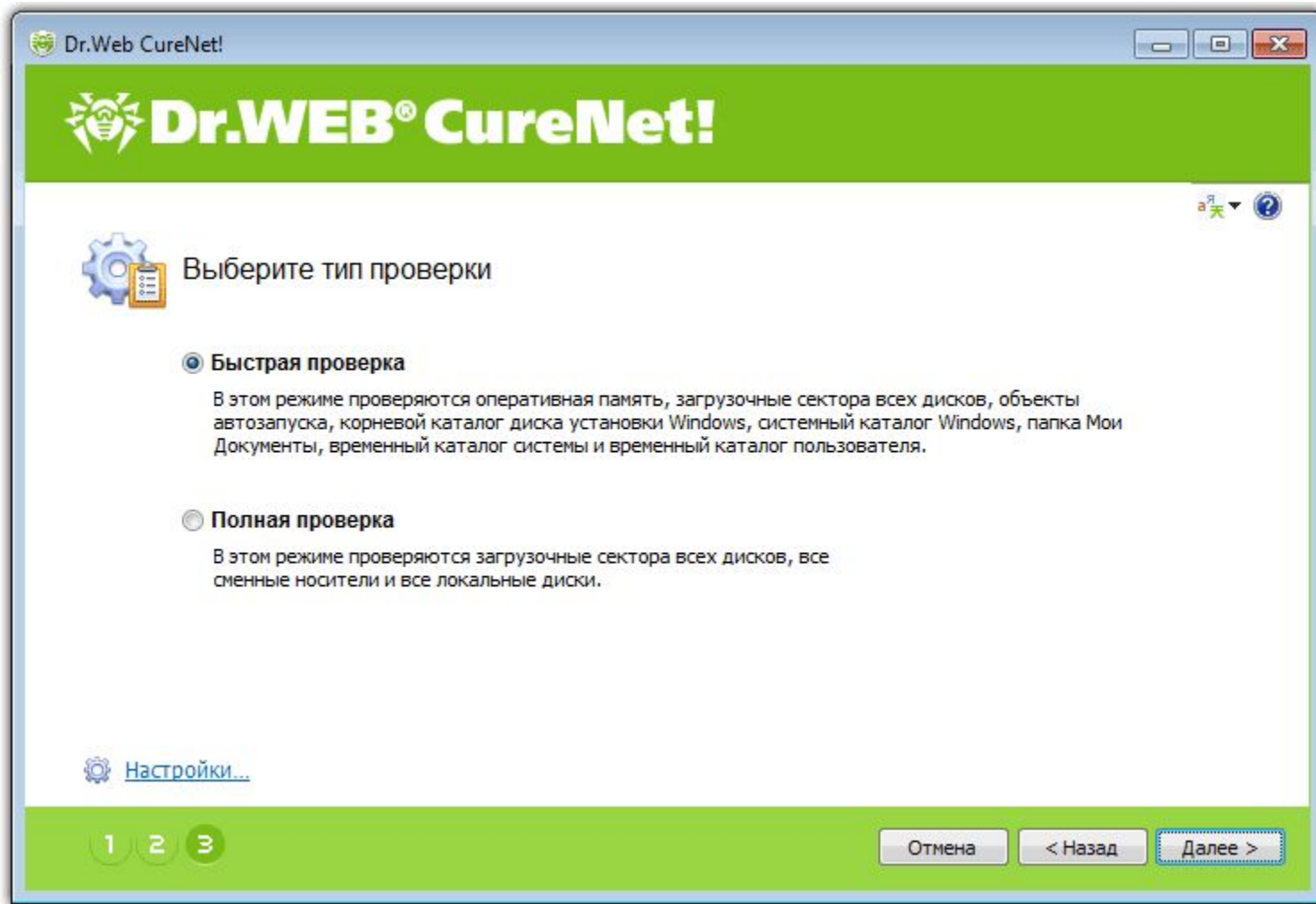


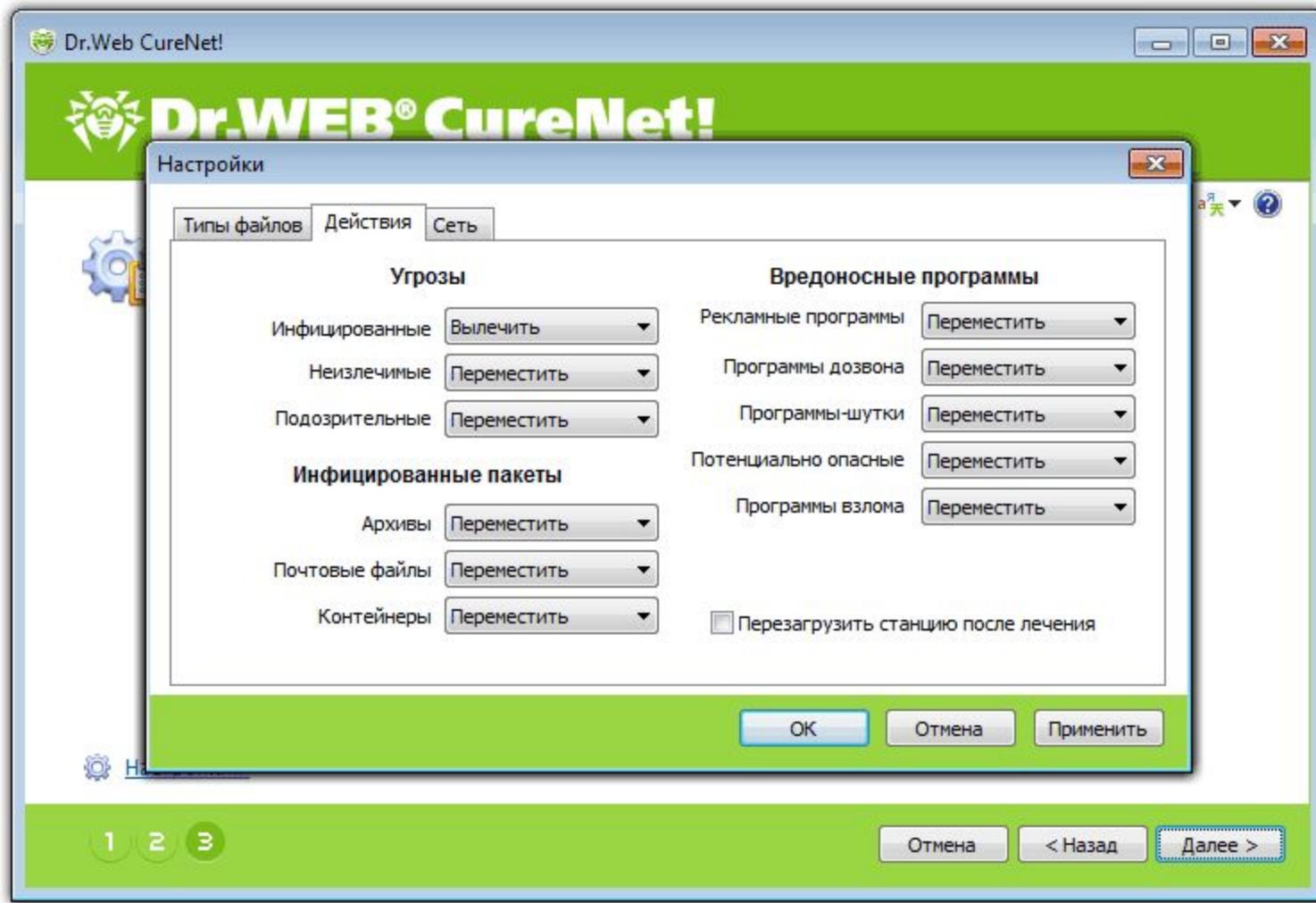


The screenshot shows the Dr.Web CureNet! application window. The title bar reads "Dr.Web CureNet!". The main header features the Dr.WEB® CureNet! logo. Below the header, there is a section with a computer icon and the text: "Добавьте станции с помощью автоматического поиска или укажите необходимую станцию или диапазон станций вручную". A modal dialog box titled "Добавление станций" is open in the center. It contains the instruction: "Введите IP-адрес, диапазон адресов, маску или сетевое имя станции." followed by a text input field. Below the field, it provides an example: "Пример: 192.168.1.0-192.168.1.200 или 192.168.1.0/24". At the bottom of the dialog are "ОК" and "Отмена" buttons. In the background, the main interface shows a list with the text "Нет станций" and several buttons: "Автоматический поиск", "Добавить...", "Удалить", "Выбрать все", and "Снять все". At the bottom of the window, there are navigation buttons: "1", "2", "3", "Отмена", "< Назад", and "Далее >".










fe80::c541:f137:bc98:7d28%11 — Статистика по станции

Угрозы		Действия		Статистика	
Инфицированные	34	Исцелено	34	Проверено	2962
Неизлечимые	0	Удалено	0	Объем данных (КБ)	682580
Подозрительные	0	Переименовано	0		
Рекламные программы	0	Перемещено	0		
Программы-шутки	0	Проигнорировано	0		
Программы дозвона	0				
Потенциально опасные	0				
Программы взлома	0				

Путь	Угроза	Действие
C:\Windows\System32\iuyvraiwou.tmp	Win32.HLLM.Netsky.35328	Исцелен
C:\Windows\iqwer.eab	Win32.HLLM.Netsky.35328	Исцелен
C:\wrtpwtsss.\$\$\$	Win32.HLLM.Netsky.35328	Исцелен
C:\winlogon.exe	Win32.HLLM.Netsky.35328	Исцелен
C:\qqqq.tmp	Win32.HLLM.Netsky.35328	Исцелен
C:\q.bmp	Win32.HLLM.Netsky.35328	Исцелен

OK


«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
Найдено	4 Неудачно	1 Завершено	3 Перезагружено
Не найдено	0		0 Ошибка

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 Пропигнорировано	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%

**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.



Бета- тестирование

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




Бета- тестирование

Новое в Dr.Web Enterprise Suite 6.0:

- Поддержка 64-битных 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



Технология **Origins** **Tracing™**

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

Защити созданное

Технология

FLY-CODE™



- Универсальный распаковщик



- Специальные записи в вирусной базе



- Эвристическое предположение

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™

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®

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