

# Dr.Web Enterprise Suite

**Централизованно-управляемая комплексная защита  
рабочих станций, файловых и почтовых серверов  
корпоративных сетей **любого масштаба****

## История проекта

- **Начало разработки:** 2002
- **Задача:** разработка антивирусной защиты для рабочих станций и серверов с возможностью централизованного управления для Всероссийской сети ГАС «Выборы»
- **Сдача проекта:** начало 2003
- **Коммерческий выпуск Dr.Web Enterprise Suite:** август 2005

# Dr.Web Enterprise Suite

## Ключевые функции

Защити созданное

- **Централизованное управление** защитой рабочих станций Windows, файловых серверов Windows, **Новое!** почтовых серверов Unix
- **Централизованное управление** антивирусной сетью и получение информации о ней как с рабочих мест в корпоративной сети, так и удаленно через Интернет
- Удаленная **централизованная установка** (для компьютеров, работающих под управлением Windows 2000/XP/Vista)
- Настройка групповых политик
- **Централизованная настройка** антивирусного ПО, постановка/отмена задач рабочим станциям
- **Централизованный мониторинг** состояния антивирусной защиты сети, сбор и изучение информации о вирусных событиях на всех защищаемых объектах
- Система оповещения администратором групп пользователей, или отдельных пользователей
- Сервис «Офисный контроль»

## Исключительные возможности Dr.Web Enterprise Suite

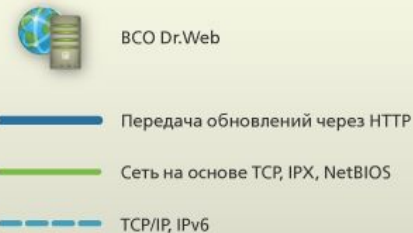
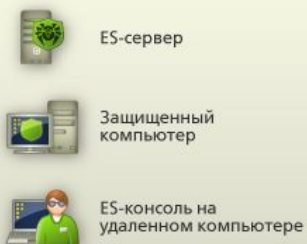
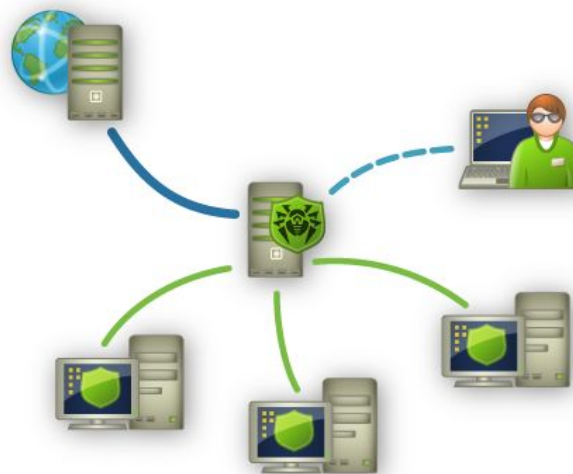
- **Кросс-платформенность** серверного ПО (Windows/Unix)
- **Работа в сетях:** TCP/IP(включая IPv6), IPX/SPX, NetBIOS
- **Безопасность передачи данных** - опция шифрования
- **Минимальный сетевой трафик** за счет механизмов сжатия
- Возможность **группирования** нескольких серверов Dr.Web Enterprise Suite с комплексной структурой взаимодействия между ними
- Возможность **установки консоли администратора** на любой ПК под управлением любой ОС
- Возможность **распределения нагрузки** между серверами

# Развертывание

**АВ-серверы:** Linux, FreeBSD (от 6.2 до 7.1), Solaris (x86 и Sparc) (для 32- и 64-битных систем).

**АВ-агенты:** 98/Me/NT/2000/XP/Vista (только для 32-битных систем).

**Сервер базы данных:** Oracle, PostgreSQL, Microsoft SQL Server или Microsoft SQL Server Compact Edition, любая СУБД с поддержкой SQL-92 через ODBC



## Развертывание

Защити созданное

Поддержка сетей различного типа	
Кросс-платформенность серверного программного обеспечения – возможность установки сервера как на ОС Microsoft Windows, так и ОС UNIX	✓
Возможность выбора типа базы данных сервера защиты	✓
Возможность построения иерархической системы серверов защиты	✓
Работа в сетях TCP/IP(включая IPv6), IPX/SPX, NetBIOS	✓
Наличие специальной политики для мобильных пользователей, в том числе возможность обновления через Интернет	✓
Возможность шифрования данных при обмене между различными компонентами системы	✓
Возможность автоматического распределения рабочих станций по нескольким серверам с уменьшением нагрузки на каждый из них, выбор сервера обновлений	✓
Размер защищаемой сети	Без ограничений

# Функции установки

Защити созданное

Функция установки	
Централизованная удаленная (без необходимости непосредственного доступа персонала) установка компонентов защиты на рабочие станции и серверы	√
Добавление в продукты собственных компонентов, самостоятельное создание новых продуктов, для которых также будет выполняться синхронизация	√
Возможность установки продуктов сторонних производителей	√
Ввод пароля при установке	√
Удаленная установка с помощью политик Active Directory	√
Централизованная установка антивируса через Login Script	√
Установление соединения со стороны локального компьютера (в случае, если сервер не может устанавливать соединение с клиентом (соединение защищено межсетевым экраном, запрещено открывать порты на клиенте, неизвестен IP-адрес клиента, и т.д.)	√
Сканирование сети вручную автоматически для обнаружения незащищенных компьютеров. Поиск по IP-подсетям	√
Поиск и деинсталляция сторонних средств защиты	√/√
Выбор и настройка устанавливаемых компонентов до начала установки	√
Резервное копирование критических данных сервера защиты сети	√

## Dr.Web Enterprise Suite

### Использование политик безопасности гарантирует невозможность самостоятельного изменения пользователями настроек защиты

- Возможность централизованной настройки политик безопасности для любых типов пользователей, включая мобильных, и возможность настройки политик безопасности для любых станций – даже отсутствующих в данный момент в сети, позволяют обеспечить актуальность защиты в любой момент времени
- **Новое!** Возможность создания индивидуальных политик безопасности
- Возможность задавать персональные уровни доступа для различных администраторов и пользователей
- Возможность самостоятельной настройки пользователями в пределах делегированных прав
- Упрощенное управление рабочими станциями за счет использования механизма групп; репликация групп между серверами
- Возможность самостоятельного написания обработчиков событий на любом скриптовом языке, что дает прямой доступ к внутренним интерфейсам Dr.Web Enterprise Suite



## Компоненты Dr.Web Enterprise Suite

- Антивирусный сервер
- Консоль управления
- Веб-интерфейс администратора
- Антивирусные агенты

## Антивирусный сервер

Главная функция –  
централизованное  
администрирование  
информационной защиты сети  
предприятия включая:

- развертывание
- обновление вирусных баз и программных модулей компонентов
- мониторинг состояния сети
- извещения о вирусных событиях
- сбор статистики

## Антивирусный сервер Dr.Web Enterprise Suite – уникальные особенности

- Платформено-независимая архитектура серверной части ПО Dr.Web Enterprise Suite позволяет использовать его как на Windows, так и на UNIX-серверах - **это не позволяет делать ни одна другая аналогичная программа.**
- Обновление антивирусных агентов, в том числе вирусных баз, целиком ложится на антивирусный сервер, что приводит к **значительной экономии интернет-трафика** и отсутствию необходимости настраивать обновления вручную.



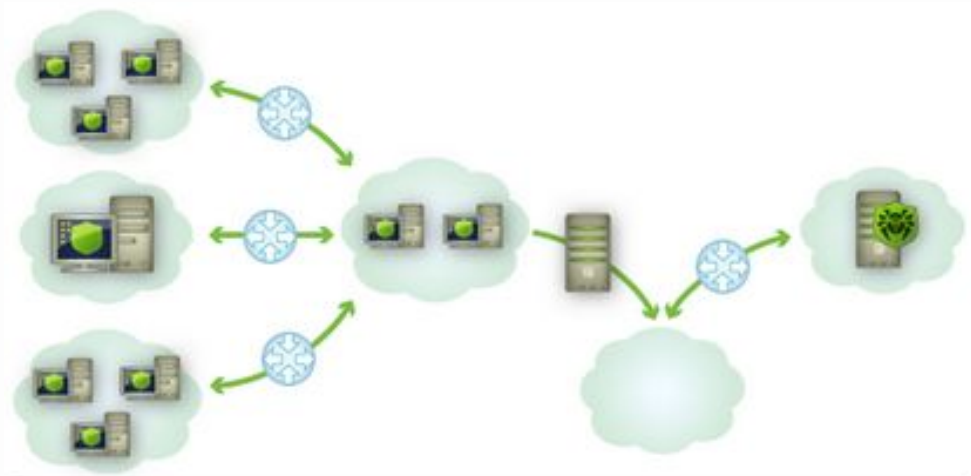
## Антивирусный сервер Dr.Web Enterprise Suite





- Хранит дистрибутивы антивирусных пакетов для различных ОС, обновления вирусных баз и программных модулей пакетов, пользовательские ключи, настройки защищаемых компьютеров
- Содержит в своей базе данных настройки каждого агента, расположенного в антивирусной сети, статистику по сканированиям, проводимым каждым компонентом антивируса на каждом компьютере, входящем в антивирусную сеть и другую полезную информацию

# Dr.Web Enterprise Suite Группирование

Защити созданное

**1 ES-сервер + внешняя СУБД =  
любое количество ES-агентов**



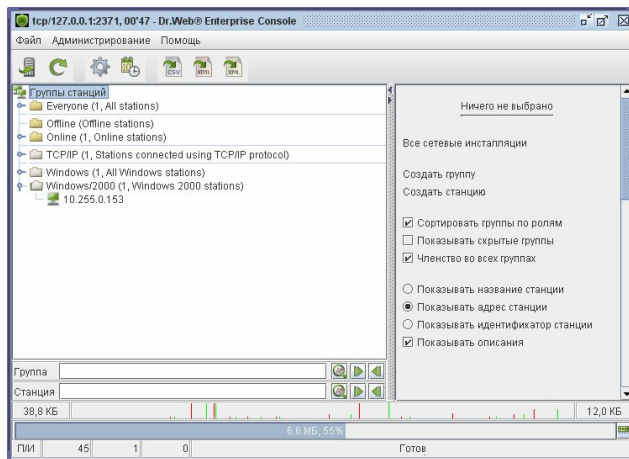
	Защищенный компьютер		Сеть на основе TCP, IPX, NetBIOS
	Антивирусный сервер		Маршрутизатор
	Прокси-сервер		

# Dr.Web Enterprise Suite

## Удобство администрирования

Защити созданное

### Консоль Dr.Web Enterprise Suite



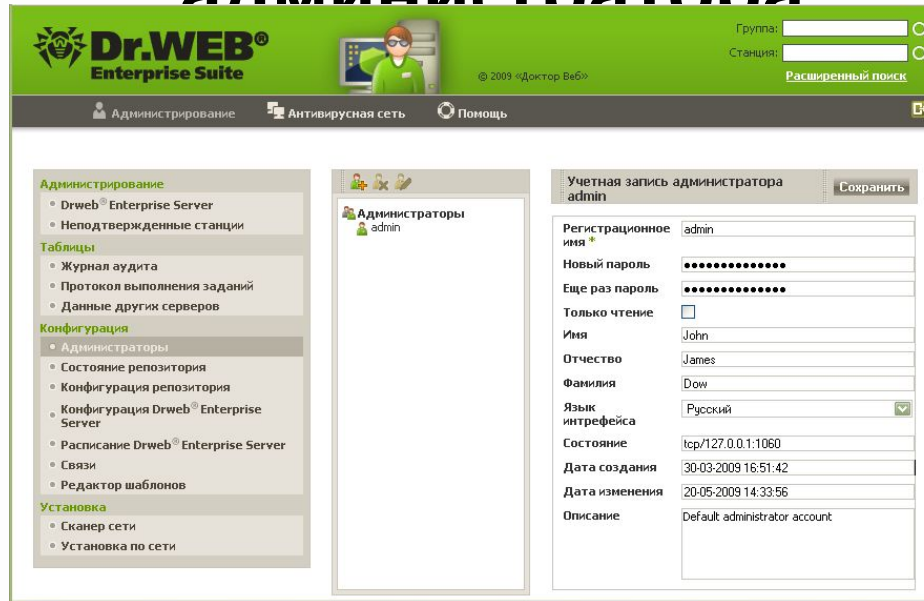
- Платформо-независимое приложение
- Может быть установлена на компьютере с любой ОС, поддерживающей виртуальную машину Java
- Связь между консолью и сервером обеспечивается по протоколу TCP/IP или IPv6
- Доступна всегда и везде, даже извне защищаемой сети
- Наглядный контроль за состоянием защиты станций, в том числе за счет группировки станций с различным состоянием защиты
- Шифрование данных обеспечивает безопасное администрирование через Интернет из любой точки мира

## Настройка расписаний

Администратор имеет возможность устанавливать:

- расписания сканирований
- уровни глубины сканирований
- списки исключений из проверки
- последовательность действий в случае обнаружения вируса

# Новое!!! Веб-интерфейс администратора



Защити созданное

- Не требует наличия дистрибутива java-консоли и инсталляции
- Работает со всеми популярными браузерами.
- Позволяет контролировать работу всех сервисов с любого компьютера даже не находясь физически в офисе
- **Интерфейс отправки сообщений** дает возможность отправлять информационные сообщения отдельным пользователям или группам пользователей.
- **Журнал аудита** действий администраторов дает возможность отслеживать все действия по установке и настройке системы.



## Статистика и отчетность

- Версии антивирусных пакетов/ перечень компонентов, запущенных на защищаемых ПК
- Время и даты установки и обновлений ПО антивирусной рабочей станции с указанием версии ПО
- Время и даты входа в систему и данные о временных отключениях от антивирусного сервера
- Время и даты обновлений вирусных баз с указанием их версий
- Версия ОС, установленная на защищаемом ПК, тип процессора, расположение системных каталогов ОС и т. п.
- Конфигурация и режимы работы антивирусных пакетов
- Информация о вирусных событиях
- Возможность создания отчетов в заданное администратором время/отправка их на e-mail
- Формирование графиков активности вирусов, статистики по найденным типам вредоносных объектов, произведенных над ними действий

## Оповещения

<b>Оповещение администраторов и пользователей об угрозах различного типа</b>	
Оповещения пользователей	√
Редактирование шаблонов оповещений	√
Оповещение в случае срабатывания одного из predetermined правил (включая возможность самостоятельного написания обработчиков событий на любом скриптовом языке)	√
Выбор реакции на инциденты (послать письмо администратору и/или уведомить его средствами NetSend)	√/√

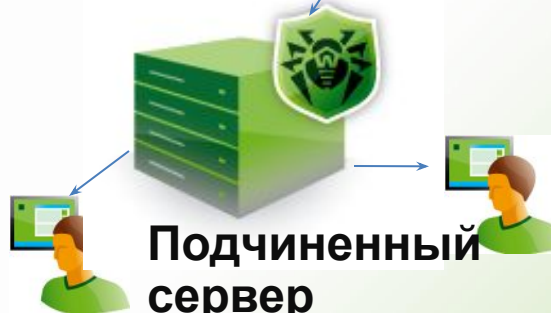
# Dr.Web Enterprise Suite

## Распределение обновлений

Защити созданное

Главный сервер  
Dr.Web ES

Подчиненный  
сервер  
Dr.Web ES



Сервер BCO  
Dr.Web

Подчиненный  
сервер  
Dr.Web ES

**Экономия трафика!!!**

# Обновления

Защити созданное

Опции обновлений	
Возможность получения обновлений через один антивирусный сервер с последующей передачей на остальные серверы напрямую или через промежуточные звенья	√
Минимизация трафика за счет применения специальных алгоритмов сжатия	√
Централизованное обновление вирусных баз и программного обеспечения на защищаемых компьютерах	√
Возможность принудительных обновлений, в том числе и после возникновения ошибок	√/√
Обновления по требованию	√
Автоматические обновления	√
Экстренные обновления	
Возможность настройки расписания обновлений	√
Откат обновлений	√
Контроль перехода на новые версии, выбор обновляемых компонент, выбор уровня контроля протокола обмена между рабочими станциями	√

# Гибкость управления

Защити созданное

<b>Гибкость при выборе политик информационной безопасности</b>	
Централизованная настройка параметров защиты, в том числе тогда, когда рабочая станция временно недоступна	√/√
Упрощенное управление рабочими станциями за счет использования механизма групп; репликация групп между серверами	√
Использование политик; выбор применяемых политик; возможность запретить пользователям менять настройки защиты	√
Возможность задавать персональные уровни доступа для различных администраторов и пользователей	√
Возможность самостоятельной настройки пользователями в пределах делегированных прав	√

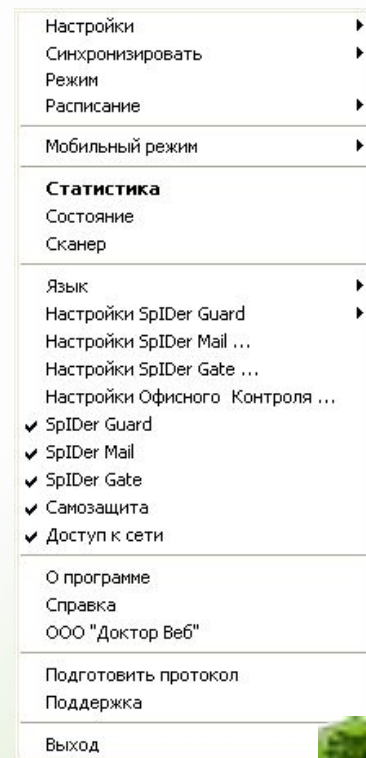
# Удобство контроля

Защиты созданное

Удобство контроля состояния сети	
Возможность управления защитой сети практически с любого компьютера – использование платформонезависимых систем управления	✓
Наличие веб-интерфейса администратора	✓
Наличие консоли администратора	✓
Наглядный контроль за состоянием защиты станций, в том числе за счет группировки станций с различным состоянием защиты	✓
Мониторинг вирусных событий, а также состояния антивирусных пакетов и ОС на всех защищаемых компьютерах	✓
Контроль хода проверки рабочих станций администратором	✓
Поиск станций в сети, в том числе с использованием регулярных выражений	✓
Поиск компьютеров с определенными свойствами или проблемами	✓
Мониторинг трафика	✓
Проверка соответствия рабочих станций установленным политикам	NAP Validator
Возможность доступа к консоли только на чтение	✓
Централизованное управление локальными хранилищами файлов на локальных машинах	*
Аудит действий администраторов	✓

## Компоненты ES-агента

- Сканер
- Файловый монитор SpIDer Guard
- Почтовый монитор SpIDer Mail со встроенным модулем антиспама\*
- Веб-антивирус SpIDer Gate\*
- Модуль «Офисный контроль»\*



\* в лицензии Dr.Web Enterprise Suite.  
Комплексная защита

# Dr.Web для Windows 5.0

## Улучшено!!! Лечит от вирусов

- **Значительно улучшен!** Антивирусное ядро обеспечивает снижение нагрузки на компьютер пользователя на 30% при возросшем качестве распознавания вредоносных программ.
- **Значительно улучшено!** Dr.Web имеет самый высокий в антивирусной индустрии процент эффективного лечения активного заражения.
- **Значительно улучшено!** Использование уникальных технологий обработки процессов в памяти и превосходные возможности по нейтрализации активного заражения позволяют устанавливать Dr.Web прямо на зараженную машину (без необходимости предварительного ее лечения).
- Высокая вероятность успешного запуска процесса сканирования на зараженном ПК – даже с внешнего носителя без установки в систему (например, с USB-stick).
- **Улучшено!** Dr.Web - недосягаемый для всех без исключения конкурентов лидер в детектировании и нейтрализации сложных вирусов, таких как MaosBoot, Rustock.C, Sector.
- Лучший в детектировании и нейтрализации сложных вирусов, таких как MaosBoot, Rustock.C, Sector.
- Только Dr.Web способен полностью проверять архивы любого уровня вложенности.
- Технологии проверки памяти позволяют блокировать активные вирусы до появления их копий на жестком диске компьютера .





## Dr.Web для Windows 5.0

# Борьба с неизвестными угрозами

Передовые технологии Dr.Web позволяют программе работать на «опережение», блокируя даже еще неизвестные угрозы

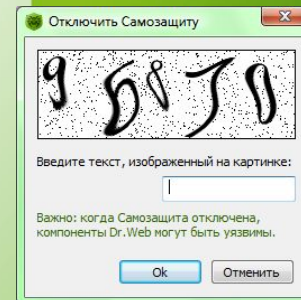
- **Новое!** FLY-CODE – не имеющая аналогов технология универсальной распаковки. Позволяет распаковывать неизвестные Dr.Web упаковщики.
- **Значительно улучшено!** Уникальная технология несигнатурного поиска **Origins Tracing™** – высокая вероятность распознавания вирусов, еще не известных вирусной базе Dr.Web.
- **Улучшено!** Эвристический анализатор Dr.Web надежно ловит все распространенные типы угроз, определяя их класс по результатам проведенного разбора и характерным признакам.



## Dr.Web для Windows 5.0

### Новое!!! Модуль самозащиты 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
- Реализован в виде драйвера и действует на самом низком системном уровне
- Выгрузка и остановка его работы невозможны до перезагрузки системы
- Постоянный мониторинг работающей системы обеспечивает защиту файлов и каталогов системы защиты Dr.Web от несанкционированного или ненамеренного удаления, модификации пользователем и вредоносным ПО
- **Является полностью самодостаточным** (в отличие от некоторых конкурирующих продуктов, модифицирующих ядро Windows, которые перехватывают прерывания, подменяют таблицы векторов, используют недокументированные функции и т.д., что может привести к серьезным проблемам в работе самой операционной системы, а также создает новые пути для использования уязвимостей)



## Dr.Web для Windows 5.0

### **Улучшено!!!** Dr.Web® Shield™

- Реализован в виде драйвера и действует на самом низком системном уровне.
- Помогает компонентам антивируса Dr.Web 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 для Windows 5.0

## Новые функциональные ВОЗМОЖНОСТИ

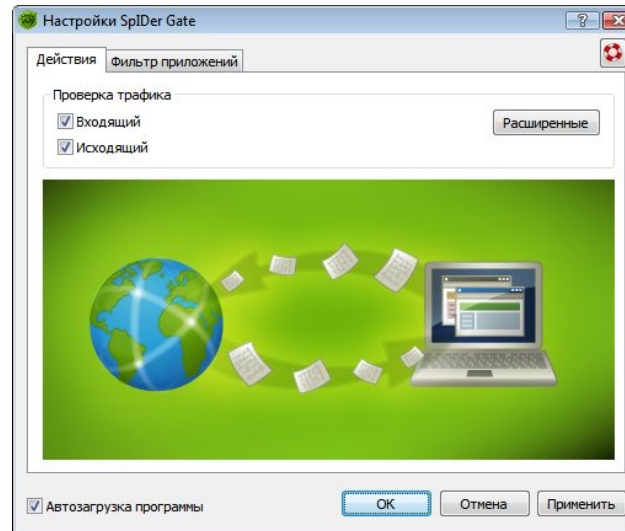
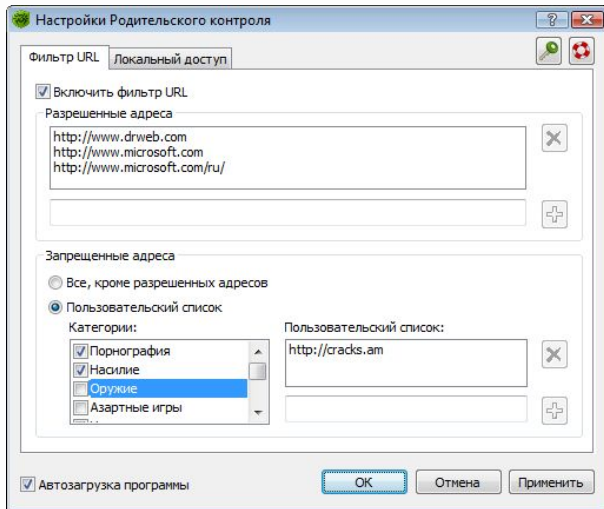
Защити созданное

Комплексная защита	Антивирус
Антивирус	Антивирус
<b>Новое!</b> Веб-антивирус	Антируткит
Антируткит	Антишпион
Антишпион	
Антиспам	
<b>Новое!</b> Офисный контроль	
<b>Широчайший набор функций!</b>	<b>Классика отрасли!</b>

# Dr.Web для Windows 5.0

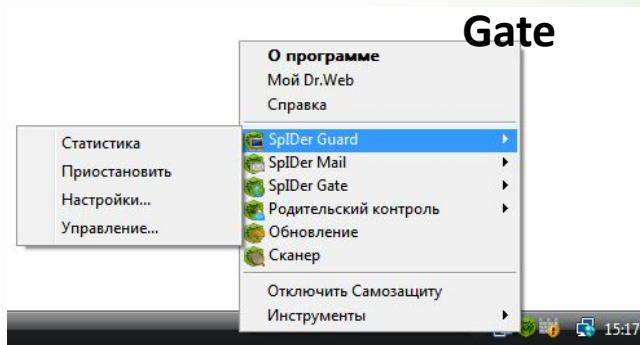
## Больше компонентов

Защити созданное



**Новое!!! «Офисный контроль»**

**Новое!!! SpiDer Gate**



**Новое!!! SpiDer**



**Dr.WEB®**  
www.drweb.com

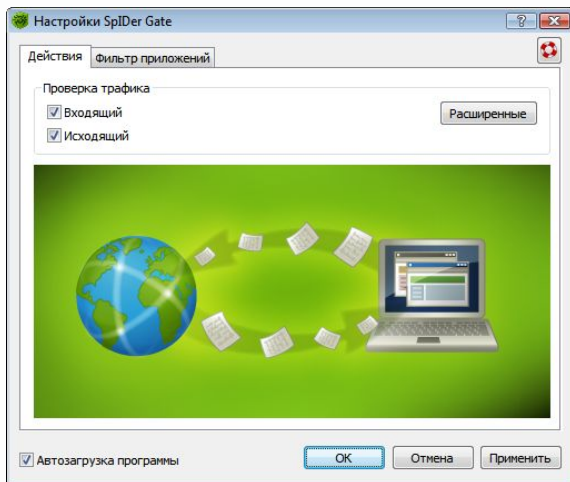
# Новое!!! Веб-антивирус SpIDer Gate™

## Только чистый интернет-контент + контроль за деятельностью сотрудников в сети

### Интернет

• Сканирует входящий и исходящий HTTP-трафик

- Фильтрация всех типов данных, поступающих из Интернета – файлов, апплетов, скриптов
- Не зависит от используемого браузера
- Фильтрация практически не сказывается на производительности ПК, скорости работы с Интернетом и количестве передаваемых данных
- Модуль поддерживает версию протокола HTTP/1.1, постоянные соединения, сжатие данных и т.д.
- В режиме «по умолчанию» не требуется никакой настройки: Dr.Web SpIDer Gate начинает сканирование сразу же после установки в системе
- Блокировка фишинговых и других опасных сайтов производится по записям в соответствующих базах ссылок



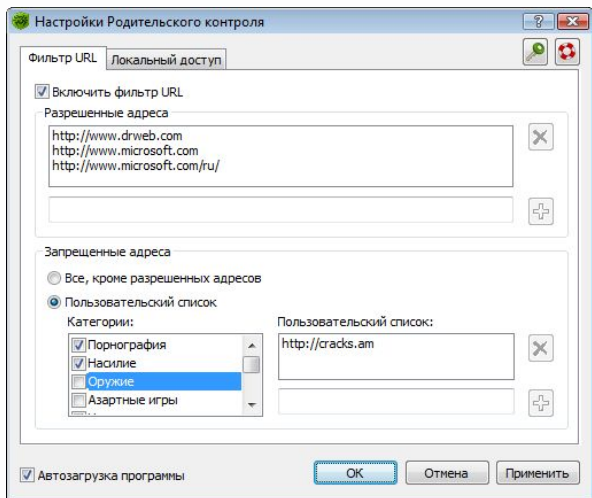
# Dr.Web для Windows 5.0

## Новое!!! «Офисный контроль»

Защити созданное

Блокировка веб-сайтов по следующим тематическим группам:

1. Порнография, эротика
2. Наркотики
3. Жестокость
4. Нецензурная лексика
5. Оружие
6. Азартные игры
7. Чаты
8. Интернет-почта
9. Социальные сети
10. Экстремизм, терроризм.



# Dr.Web для Windows 5.0

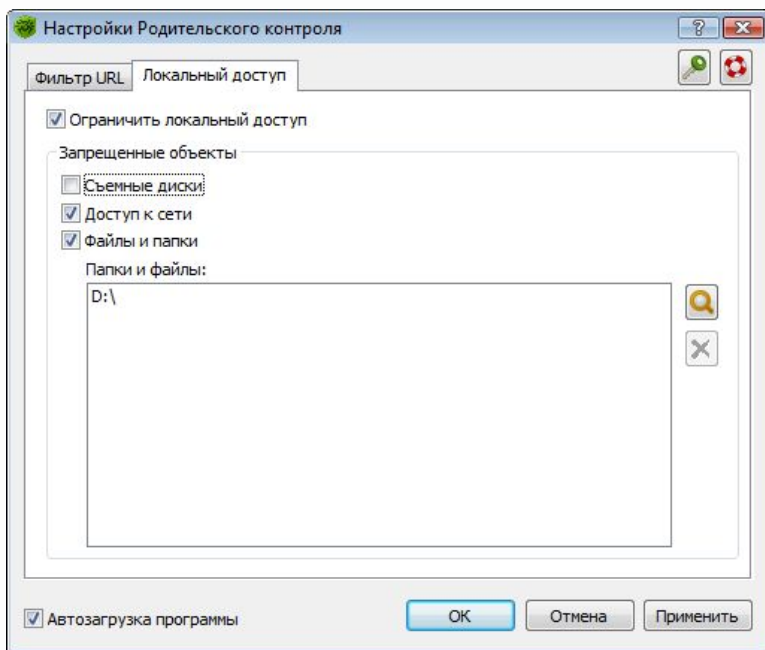
## Новое!!! «Офисный контроль»

### Защита от инсайдеров

Запрет использования переносных хранилищ информации (флэш-дисков, USB-устройств), сетевых устройств, а также отдельных файлов и каталогов – защита данных от удаления или похищения.

**НЕТ аналогов у конкурентов!**

**В лицензии «Комплексная защита»**

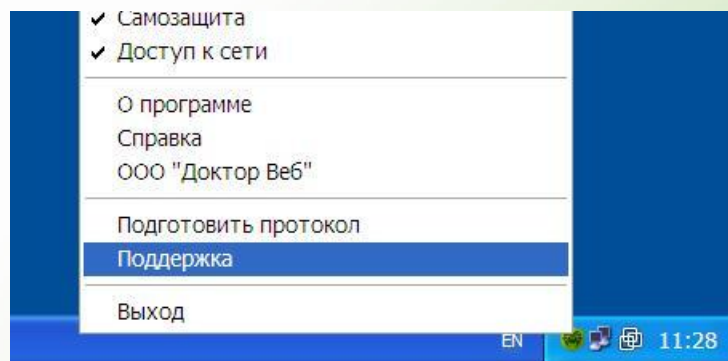




## Оперативная техподдержка



Сбор информации о  
ПК «одной кнопкой»  
и упаковка файла  
отчета



Защити созданное

## Лицензирование Dr.Web Enterprise Suite

- **Минимальная лицензия:** от 5 станций
- **Максимальная лицензия:** не ограничена
- **Сроки лицензий:** 1, 2 или 3 года
- **Виды лицензий:** антивирус, комплексная защита

### Варианты лицензий

- Dr.Web Enterprise Suite –защита рабочих станций
- Dr.Web Enterprise Suite + Dr.Web для файловых серверов Windows
- Dr.Web Enterprise Suite + Dr.Web для почтовых серверов Unix (на базе MailD)

## Специальные предложения при покупке Dr.Web Enterprise Suite

Защити созданное

1. Dr.Web Enterprise Suite + файловый сервер	2. Dr.Web Enterprise Suite + защита почты
От 15 ПК и выше – файловый сервер по цене <b>1 000 рублей</b>	Защита ПК со скидкой <b>50%</b>

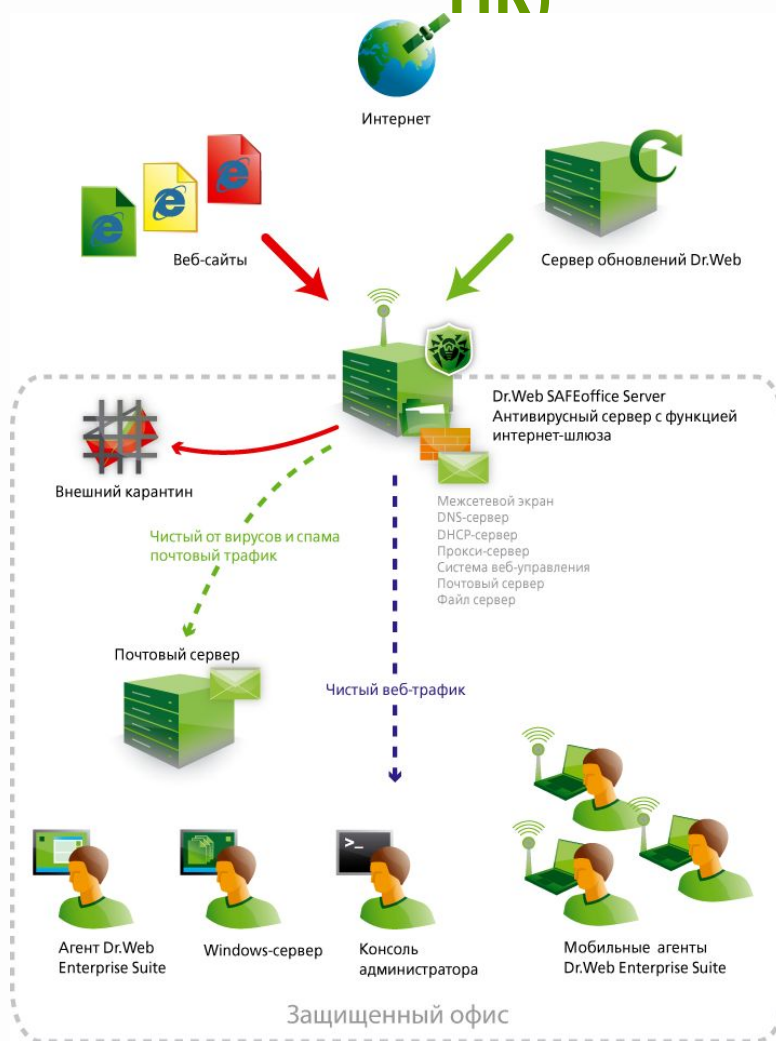
## Комплекты Dr.Web для малого и среднего бизнеса

Комплект	Защищаемые объекты
Dr.Web «Малый бизнес»	5 ПК/1 сервер/5 адресов почты + Dr.Web для Windows Mobile <b>в подарок</b>
Dr.Web «Универсальный»	5-100 ПК + сервер / почта / пользователи шлюза
Комплекты для школ	5,10, 25 ПК + 1 сервер

Защити созданное

# Dr.Web Office Shield – комплексная защита

## малых и средних предприятий (10-150 ПК)



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  
контроль за деятельностью сотрудников в сети Интернет.



# Вопросы?

## Благодарим за внимание!

[www.pilot-partner.ru](http://www.pilot-partner.ru)