



Программно-аппаратные комплексы Dr.Web® Office Shield

Комплексная антивирусная и антиспам-защита малых
и средних предприятий



Антивирус – важнейший фактор обеспечения бесперебойности функционирования бизнес-процессов предприятий

Сегодняшний мир невозможно представить без компьютеров, Интернета, разветвленных корпоративных интранет-сетей, мобильных решений. Однако практически безграничные возможности современных компьютерных технологий зачастую используются для того, чтобы воспрепятствовать нормальной работе предприятий, получить несанкционированный доступ к конфиденциальной информации и ресурсам компьютеров, расположенных в локальных сетях. Большое количество уязвимостей в программном обеспечении в сочетании с недостаточной грамотностью пользователей в сфере компьютерной безопасности создают серьезные помехи для нормальной бизнес-деятельности компаний.



Компании в среднем теряют из-за действий вирусов 68 дней рабочего времени в году. Эти убытки сравнимы лишь с убытками от отказа критически важных информационных систем или от потери конфиденциальной информации.

Уникальность антивирусного ПО состоит в том, что, в отличие от любого другого ПО (кроме операционной системы), оно должно использоваться на всех участках бизнеса – как в процессе управления предприятием, ведении бухгалтерского и финансового учета, так и непосредственно в процессах производства. Наличие антивируса на рабочих станциях и серверах является обязательным условием обеспечения бесперебойности функционирования предприятия. Современные антивирусные продукты построены на основе новейших технологий и, как правило, требуют для своего обслуживания квалифицированных, и, как следствие, высокооплачиваемых специалистов. Но что делать малым и средним компаниям, не имеющим возможности тратить значительные средства на создание и поддержание в работоспособном состоянии серьезной IT-инфраструктуры?

Выходом из ситуации является использование программно-аппаратных комплексов **Dr.Web Office Shield** – экономичных решений, предназначенных для организации централизованной антивирусной и антиспам-защиты малых и средних компаний с числом обслуживаемых рабочих станций от 10 до 250.

Dr.Web Office Shield – комплексное решение задачи антивирусной и антиспам-защиты малых и средних предприятий

Общеизвестно, что зачастую выбор системы защиты определяется не качеством реализации технологических решений, а эксплуатационными свойствами продукта – простотой и удобством установки, эффективностью технической поддержки.

Dr.Web Office Shield сочетает в себе традиционно высокое качество детектирования вредоносного ПО любого типа и удобную систему управления, доступную для администраторов любой квалификации.

Использование программно-аппаратных комплексов **Dr.Web Office Shield**, для управления которыми не требуется значительный опыт администрирования, оптимизирует затраты на информационную защиту, что положительно влияет на рост прибыли и усиление преимуществ перед конкурентами в стратегической перспективе. Эффективные механизмы антивирусной и антиспам-защиты, использованные в **Dr.Web Office Shield**, делают его по-настоящему эффективным инструментом реализации информационной политики компании.

Dr.Web Office Shield позволяет повысить эффективность труда персонала, сократить простой и снизить стоимость владения антивирусом на 30%.

Решаемые задачи

Уменьшение зависимости предприятий от низкого уровня квалификации IT-персонала

По мнению руководителей предприятий, наиболее значимым фактором, затрудняющим выполнение поставленных задач, является нехватка квалифицированных сотрудников.

Особенно остро эта проблема стоит для малых и средних предприятий. Как правило, такие предприятия вынуждены использовать либо входящих (обслуживающие сразу несколько компаний и в связи с этим не имеющие возможность оперативно реагировать на все запросы клиента) системных администраторов, либо нанимать системных администраторов недостаточно высокой квалификации.



Использование неквалифицированного персонала создает угрозу для информационной безопасности предприятия и повышает совокупную стоимость владения системами информационной безопасности.

Управление системой информационной защиты предприятия требует специальных знаний, которые отсутствуют у большинства IT-администраторов. Эффективность использования антивируса на предприятии едва ли не на 100% зависит от квалификации персонала, его администрирующего. Нередко предприятие вынуждено закупать не тот продукт, который является наиболее эффективным, а тот, с которым умеет работать администратор. В связи с этим многие полезные и нужные для предприятия функции ПО могут просто не использоваться либо из-за незнания об их существовании, либо из-за неумения их использовать. Все это приводит к тому, что возникающие инциденты, как правило, усугубляются неадекватными либо непрофессиональными действиями IT-персонала (например, из-за неверной или несвоевременной реакции на вирусные угрозы, ошибочных действий по восстановлению работоспособности сети после вирусных атак) и приводят к непредвиденным расходам.

Простота администрирования и минимальные затраты на обслуживание

Использование **Dr.Web Office Shield** позволяет найти оптимальный выход из описанной ситуации. В разработке приложений, вошедших

в состав **Dr.Web Office Shield**, принимали участие высококвалифицированные специалисты, что позволило создать устройство, обеспечивающее информационную безопасность предприятия при минимальных требованиях к квалификации обслуживающего персонала. Для управления **Dr.Web Office Shield** не требуется специальной подготовки, достаточно базовых компьютерных знаний. За счет интуитивно понятного интерфейса процесс администрирования устройства прост и может осуществляться с помощью любого интернет-браузера. Дополнительно предусмотрено администрирование из обычной консоли, устанавливаемой на рабочую станцию администратора или через SSH-терминал, что позволяет провести тонкую настройку устройства. Высокая стабильность работы, предварительно настроенная конфигурация, функции автоматической диагностики и профилактики сводят к минимуму необходимость контроля администратора за работой **Dr.Web Office Shield**.

Максимально быстрое развертывание

Установка и ввод в эксплуатацию **Dr.Web Office Shield** состоят всего из нескольких интуитивно понятных и простых шагов. В большинстве случаев необходимо только сконфигурировать его под конкретные параметры локальной сети и устройство будет выполнять все возложенные на него задачи. Это стало возможно за счет использования оптимизированного программного обеспечения и удобной системы управления и настройки, применения предустановленного сценария антивирусной безопасности.

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



Простои составляют в среднем 2 часа в месяц на одного пользователя.

Чем выше служебное положение такого пользователя, тем выше стоимость его простоя.

Вирусы и спам являются основными угрозами информационной безопасности для организаций любого типа и размера. Анализ состояния корпоративной сети, работы по предотвращению вирусных атак и действия по преодолению последствий вирусных инцидентов – задачи, которыми приходится заниматься IT-персоналу каждый день. Снижение простоев, вызванных действиями вредоносных объектов, – одна из важнейших задач системных администраторов, от успеха решения которой зависят эффективность функционирования бизнес-процессов целого предприятия и его имидж надежного партнера. **Dr.Web Office Shield** является мощным инструментом снижения простоев, вызванных действиями вирусов и вредоносных объектов.

Высокая устойчивость к внешним атакам

Операционная система и основные программные модули антивирусного шлюза **Dr.Web Office Shield** недоступны для несанкционированной модификации как за счет реализации эффективной политики доступа, так и за счет использования предустановленного межсетевое экрана. Использование репозитория для проведения обновлений позволяет оперативно устранять выявленные уязвимости в используемом программном обеспечении и поддерживать высокий уровень защищенности **Dr.Web Office Shield**.

Контроль работоспособности

Наличие встроенных механизмов контроля работоспособности системы защиты позволяет автоматически восстанавливать работоспособность устройства в случае возникновения каких-либо проблем.

Снижение количества внеплановых остановок

Система оповещения администратора о проблемах, возникающих в антивирусной сети защищаемого предприятия, позволяет максимально оперативно реагировать на вирусные угрозы и активно им противодействовать.

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



В отдельные периоды рабочего дня (например, обеденный перерыв) сотрудники компании занимают до 80% пропускной способности канала на задачи, не связанные с работой. Использование Интернета в личных целях транслируется в потери 30 – 40% производительности труда.

Стоимость всего одного часа в день использования Интернета в личных целях каждым сотрудником компании составляет 12,5% от всех расходов компании на заработную плату.

Dr.Web Office Shield – эффективное средство фильтрации контента, которое позволяет контролировать расход рабочего времени и ресурсов предприятия сотрудниками. Устройство позволяет предотвращать несанкционированный расход трафика, пресекать в режиме реального времени попытки посещения нежелательных страниц – например, интернет-магазинов, дает возможность прописывать политики доступа к веб-ресурсам.

Dr.Web Office Shield позволяет реализовать систему отчетов о расходе каждым хостом организации сетевого трафика, что дает возможность оперативно корректировать политику безопасности, принятую на предприятии.

Повышение производительности труда путем снижения количества отвлекающих факторов

Во времена перепроизводства информации человеческое внимание – ценный и почти невозобновляемый ресурс. Обилие и даже переизбыток информации, ее большая доступность в связи с появлением Интернета, поглощают внимание людей. Чистка почтового ящика от спама, закрытие всплывающих окон и рекламных баннеров – все это рассеивает внимание, снижает уровень концентрации, негативно влияет на эмоциональное и психическое состояние человека. Информационные потоки, которые необходимо ежедневно обрабатывать персоналу, нарастают день ото дня. В противоположность этому производительность сотрудников – величина, склонная к уменьшению в условиях перегрузки побочными действиями. В итоге для предприятий стоимость поддержания необходимой производительности труда сотрудника оказывается дороже стоимости вычислительных ресурсов.



Сотруднику, чье внимание отвлечено от решения текущей бизнес-задачи, необходимо до 15 минут, чтобы заново сконцентрировать внимание.



Являясь эффективным средством борьбы с многочисленными отвлекающими факторами, **Dr.Web Office Shield** помогает конвертировать внимание сотрудников в доходную статью бюджета предприятия.

Dr.Web Office Shield позволяет минимизировать потери рабочего времени. Используемая система антиспама позволяет максимально эффективно бороться со спамом и нежелательными сообщениями. В противовес обучаемым антиспам-системам, использование которых со временем достигает высокого уровня точности фильтрации, но требует ежедневной работы системного администратора, интеллектуальная система фильтрации антиспама **Dr.Web** позволяет использовать его прямо «из коробки» – в режиме «установил и забыл». При этом эффективность отсева спама достигает 97 – 99%.

Высокопродуктивная фильтрация

Разработчики антиспама ориентировались на создание решения для корпоративных серверов, поэтому именно высокая скорость фильтрации сообщений была одной из самых приоритетных задач при его разработке.

Разные технологии детектирования для разного вида нежелательных сообщений

В антиспаме **Dr.Web** для каждого вида нежелательных писем – спама, фишинг-, фарминг-, скамминг-, bounce-сообщений – предусмотрены разные технологии фильтрации, что обеспечивает высокую вероятность распознавания. Так, для некириллического спама эта цифра достигает 99%. При вынесении вердикта – спам/не спам – изучается совокупность очень большого числа признаков сообщения.

Регулярные обновления

Обновления к антиспаму **Dr.Web** выпускаются ежедневно и автоматически загружаются пользователям с помощью утилиты автоматического обновления **Dr.Web**. Уникальные технологии распознавания нежелательной почты на основе нескольких тысяч правил позволяют производить обновления не чаще одного раза в сутки и экономить трафик на скачивании громоздких и частых обновлений.

Защита репутации компании

«Изобретательность» рядовых сотрудников компании зачастую является причиной того, что компьютеры компании сами становятся источником спама, что не только вредит престижу компании среди ее партнеров, но и приводит к отключению ее от сети Интернет, что, в свою очередь, может полностью парализовать ее работу. **Dr.Web Office Shield** позволяет не допустить такой ситуации.

Преимущества программно-аппаратных комплексов Dr.Web Office Shield

Исключительная надежность

Dr.Web Office Shield создан на аппаратной платформе, предназначенной для использования во встроенных системах высокой степени надежности. Использование пассивного охлаждения позволяет избежать проблем, связанных с выходом вентилятора из строя, расширить список мест установки устройства и значительно сократить затраты на обслуживание системы за счет отказа от ряда обязательных процедур профилактики работы. Отсутствие вентиляторов сводит к минимуму возможность выхода Dr.Web Office Shield из строя в процессе непрерывной длительной эксплуатации.

Устойчивость к неблагоприятной среде

Dr.Web Office Shield обладает низким энергопотреблением и тепловыделением, неприхотлив к перепадам температур и влажности. Испытания показали, что стабильная работа процессора с полной загрузкой обеспечивается даже при температуре окружающей среды 60°C.

Автоматическое восстановление и легкая переносимость

Используя встроенные инструменты резервного копирования можно создать копию работающего сервера, в том числе и по расписанию. Администратор может легко распространить созданную конфигурацию на другие устройства за счет возможности сохранения всех настроек системы в единый архивный файл.

Отсутствие необходимости унифицировать компьютерный парк предприятия

Широчайший спектр поддерживаемых операционных систем, а также уникальная система обновлений компонентов и вирусных баз Dr.Web Office Shield не требуют от предприятия единообразия платформ защищаемых рабочих станций. В отличие от большинства других антивирусных программ Dr.Web Office Shield может использоваться на предприятиях, эксплуатирующих устаревшие ОС Windows.

Компактность

Традиционно высоконадежные программно-аппаратные комплексы выполняются в формате, требующем размещения их в специально оборудованных помещениях, имеющих системы кондиционирования и бесперебойного питания. Необходимость иметь такие помеще-

ния повышает затраты предприятия на информационные технологии, в том числе и за счет нерационального использования арендуемых помещений. Традиционная надежность и неприхотливость решений компании Dr.Web позволила создать решение, выполненное в компактном корпусе, который может быть расположен в самых различных местах – даже там, где обычный компьютер разместить невозможно.

Компактность и нетребовательность к квалификации обслуживающего персонала позволяют использовать Dr.Web Office Shield даже домашним пользователям (например, для организации домашних сетей)!

Варианты использования

Dr.Web Office Shield является высокопроизводительным и отказоустойчивым сервером централизованной антивирусной и антиспам-защиты рабочих станций и файловых серверов Windows, почтового и интернет-трафика. Модульность решения и гибкость системы лицензирования позволяет использовать устройство в самых различных конфигурациях локальных сетей предприятий и организаций, реализуя их внутреннюю политику безопасности. В частности, Dr.Web Office Shield может быть использован:

- в качестве сервера демилитаризованной зоны – максимально изолированного от внутренней сети устройства, отвечающего за антивирусную и антиспам-защиту предприятия;
- прокси-сервера (шлюза доступа пользователей внутренней интранет-сети к ресурсам сети Интернет), предназначенного для обеспечения защиты почтового и интернет-трафика от вирусов, разного рода вредоносных объектов и спама.

Использование Dr.Web Office Shield в качестве шлюза значительно снижает затраты компаний на организацию безопасного доступа пользователей корпоративной интранет-сети к ресурсам сети Интернет и позволяет существенно экономить интернет-трафик;

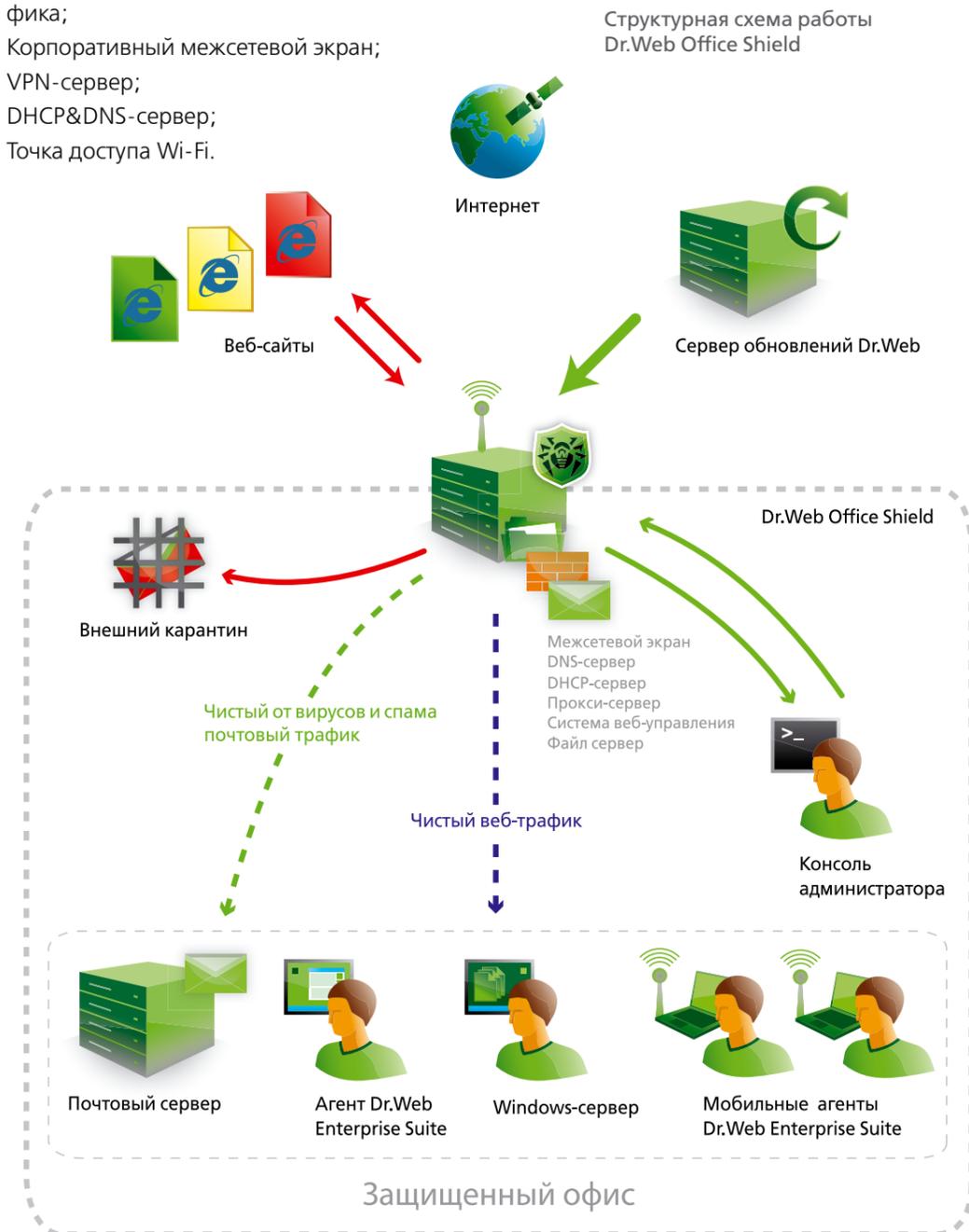
- внутреннего сервера локальной сети, обеспечивающего централизованную защиту рабочих станций и файловых серверов Windows.

В состав Dr.Web Office Shield входят:

- Dr.Web Enterprise Suite, обеспечивающий централизованную защиту рабочих станций и файловых серверов Windows, а также почтовых серверов Unix;
- Dr.Web для интернет-шлюзов Unix, обеспечивающий защиту доступа пользователей внутренней интранет-сети к ресурсам сети Интернет;
- Dr.Web Mail Gateway, обеспечивающий антивирусную и антиспам-защиту почтового трафика;
- Корпоративный межсетевой экран;
- VPN-сервер;
- DHCP&DNS-сервер;
- Точка доступа Wi-Fi.



Важной особенностью Dr.Web Office Shield является то, что он может быть как установлен в уже существующую сеть, так и использован в качестве основы для вновь создаваемой сети – наличие работающих сервисов DHCP и DNS позволит провести эту работу с минимальными усилиями.



Ключевые функции

Антивирусная и антиспам-защита рабочих станций и файловых серверов Windows

- Комплексная защита компьютеров под управлением Windows от вирусов и спама;
- Централизованная установка антивирусных агентов (с возможностью настройки ПО агентов на сервере до его установки на клиентские машины);
- Упрощенное управление рабочими станциями антивирусной сети за счет использования механизма групп;
- Возможность использования на антивирусной станции спам-фильтра;
- Быстрое и эффективное распространение сервером Dr.Web Enterprise Suite обновлений вирусных баз и программных модулей на защищаемые рабочие станции;
- Минимизация сетевого трафика локальных сетей, построенных на основе протоколов TCP/IP, IPX, за счет применения специальных алгоритмов сжатия;
- Возможность шифрования данных при обмене между различными компонентами системы.

Антивирусная проверка интернет-трафика в режиме прокси

- Антивирусная проверка FTP- и HTTP-трафика;
- Изоляция зараженных объектов в карантине;
- Выбор типа проверяемых объектов;
- Выбор действия для различных типов файлов;
- Возможность регулировать доступ к определенным веб-ресурсам, производить сортировку по mime-типу и размеру запрашиваемых файлов;
- Возможность оптимизации проверки трафика за счет использования технологии Preview;
- Возможность обработки нескольких запросов в ходе одного соединения;
- Возможность работы как с протоколом IPv4, так и с протоколом следующего поколения IPv6;
- Удобная система отчетности;
- Отражение действий, проведенных антивирусом по защите безопасности сети, в журналах системы;
- Система оповещения пользователя о попытках загрузки вредоносной страницы или об обнаружении вируса;

- Наличие системы защиты от несанкционированного доступа;
- Наличие системы мониторинга и автоматического восстановления работы системы;
- Работа в режиме «прозрачного» прокси.

Антивирусная и антиспам-проверка почтового трафика в режиме прокси

- Детектирование и нейтрализация вирусов и вредоносных кодов различного типа, спама, фишинг-, фарминг-, скамминг- и bounce-сообщений;
- Корректная обработка большинства известных типов архивов, в том числе многотомных и самораскрывающихся (SFX);
- Защита работы собственных модулей от сбоев;
- Отправка уведомлений о результатах проверки как получателям, так и другим лицам;
- Изоляция зараженных объектов и спама в карантине;
- Ведение статистики, учитывающей все аспекты работы системы;
- Активная защита от атак спамеров и хакеров;
- Проверка подлинности IP-адреса;
- Защита от спам-ловушек;
- Защита от malformed-писем;
- Экономия интернет-трафика за счет проведения ряда проверок до полной загрузки сообщения;
- Возможность регулирования доступа к Open Relays серверам.

Контентная фильтрация

- Фильтрация доступа к ресурсам сети Интернет по типу (mime), по размеру файлов, по названию хоста;
- Регулирование доступа к веб-ресурсам различного типа.

Внешний подключаемый карантин

- Использование USB-дисков или флэш-накопителей в качестве внешнего подключаемого карантина - размер карантина ограничен только емкостью подключенных дисков;
- Возможно подключение до двух USB-устройств.

Резервное копирование настроек и пользовательских данных

- Создание резервных копий работающего сервера, включая критически важные данные.

Анализ статистики использования ресурсов сети Интернет

- Анализ использования сетевых ресурсов по компьютерам, наиболее посещаемым сайтам и периодам времени;
- Просмотр отчетов в табличном или графическом виде.

Сетевые службы и сервисы

- Межсетевой экран (firewall)
- DNS-сервер

- DHCP-сервер
- Прокси-сервер
- Система веб-управления
- Файл-сервер

Поддержка работы в беспроводных сетях

- Наличие WI-FI превращает Dr.Web Office Shield в точку доступа для офисных компьютеров (прежде всего – ноутбуков), что позволяет создать безопасную внутриофисную сеть без сетевых проводов.

Модельный ряд Dr.Web Office Shield

Модель корпуса	Форм-фактор	Системная конфигурация		Рекомендуемое количество пользователей
		Компонент	Параметры	
Neo 	50x275x172	Плата	Ci945a-4rxx	от 10 до 50*
		Чипсет	Intel 945	
		Процессор	Intel CeleronM 1.86 ГГц	
		Память	1 x DDR II SDRAM (1 GB)	
		Накопитель	SATA 1 x 2.5" 160 GB	
		Сеть	4 x 100 Mb	
		Беспроводная сеть	802.11g	
Twister 	75x300x173	Плата	Ci945a-4rxx	от 50 до 250
		Чипсет	Intel 945	
		Процессор	Intel Core 2 Duo 2.6 ГГц	
		Память	2 x DDR2 SODIMM (2 GB)	
		Накопитель	SATA 1 x 3.5" 160 GB	
		Сеть	4 x 100 Mb	
		Беспроводная сеть	802.11g	

* в случае использования Dr.Web Office Shield только для обеспечения защиты почтового и интернет-трафика максимальное рекомендуемое количество пользователей – 150.

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 и лечения вредоносных программ, соответствуют мировым стандартам безопасности.

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, дает возможность оказать помощь клиентам в решении проблем любой сложности в считанные часы.

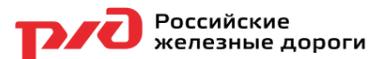
Опыт крупных проектов

С 1992 года развивается и совершенствуется линейка корпоративных решений Dr.Web. Антивирусным решениям компании «Доктор Веб» доверяют Государственная Дума, Министерство Обороны и Министерство Иностранных Дел Российской Федерации, Федеральная служба безопасности, ОАО «РЖД», а так же множество крупных предприятий и промышленных групп, учебных заведений и научно-исследовательских институтов.

Лицензии и сертификаты

Высокое качество антивирусов Dr.Web подтверждено сертификатами соответствия ФСБ и ФСТЭК РФ. Dr.Web имеет лицензию Федеральной службы по техническому и экспортному контролю РФ на проведение работ, связанных с созданием средств защиты информации, лицензию на разработку и производство средств защиты конфиденциальной информации, лицензию Министерства обороны РФ на деятельность в области создания средств защиты информации, лицензии ФСБ России на проведение работ, связанных с использованием сведений, составляющих государственную тайну, и на разработку и производство средств защиты конфиденциальной информации.

Лицензии и сертификаты, а также обширная география пользователей Dr.Web свидетельствуют о высокой степени доверия к продуктам компании.





© ООО «Доктор Веб», 2008 – 2010

125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп. 12а

Телефон: +7 (495) 789-45-87 (многоканальный)

Факс: +7 (495) 789-45-97

www.drweb.com

www.av-desk.com