Dr.WEB®
с 1992 года

Защити созданное

Продуктовая линейка Dr.Web® Security Suite

Руководство по лицензированию

Обновлено 20.11.2015

Содержание

Дата актуализации 20.11.2015

Дата актуализации 20.11.2015

О компании «Доктор Веб»

Компания «Доктор Веб» – известный российский разработчик средств информационной безопасности.

Антивирусные продукты Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ. Создание компании «Доктор Веб» в декабре 2003 года послужило началом стремительного роста продаж продуктов Dr.Web как в России, так и в других странах.

Сегодня «Доктор Веб» – это успешная, быстро растущая компания, которая играет одну из ведущих ролей на рынке средств информационной безопасности. Она располагает антивирусным ядром собственной разработки, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегическая задача компании, на которую нацелены усилия всех сотрудников, — создание средств антивирусной защиты, отвечающих всем современным требованиям. Не менее важна разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз. Линейка антивирусных продуктов компании «Доктор Веб» охватывает широчайший спектр операционных систем и совместимых приложений.

В распространении своих разработок компания опирается на партнерскую сеть, отказавшись от прямых продаж конечным пользователям.

Среди потребителей продуктов Dr.Web – домашние пользователи разных стран мира и крупные российские предприятия, небольшие организации и системообразующие корпорации, которым коллектив «Доктор Веб» благодарен за поддержку и многолетнюю преданность продукту. Государственные сертификаты и награды свидетельствуют о высоком доверии к антивирусу Dr.Web, созданному талантливыми российскими программистами.

Технологии Dr.Web

Антивирусы Dr.Web – семейство компьютерных программ, созданных талантливыми российскими программистами под руководством Игоря Данилова.

«Доктор Веб» – один из немногих антивирусных вендоров в мире, владеющих собственной уникальной технологией детектирования и лечения вредоносных программ. Компания имеет собственную службу вирусного мониторинга и аналитическую лабораторию. Благодаря этому специалисты могут быстро реагировать на новые вирусные угрозы и способны оказать помощь клиентам в решении проблем любой сложности в считанные часы.

Важной особенностью Dr.Web является его модульная архитектура. Все продукты и решения включают в себя единое антивирусное ядро, а также используют единую систему обновлений вирусных баз и глобальную систему технической поддержки. Технологии Dr.Web позволяют организовать надежную информационную защиту как в рамках крупных корпоративных сетей, так и на домашнем компьютере или в домашнем офисе.

Помимо вирусов и вредоносных программ, Dr.Web способен также обнаруживать и удалять с компьютера различные нежелательные программы (рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы, программы взлома – spyware/riskware), спам и нежелательные электронные письма (фишинг-, фарминг-, скамминг- и bounce-сообщения).

Дата актуализации 20.11.2015

Технологии

Качественный антивирус должен уметь не только находить вирусы, но и лечить их. Ведь одно дело – удалить инфицированные файлы вместе с ценной информацией, и совсем другое – вернуть их в первоначальное «здоровое» состояние. Dr.Web относится к файлам пользователя бережно.

Лечит от вирусов

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 уметь возвращать их в первоначальное «здоровое» состояние.

Технологически сложные и особо опасные вирусы, особенно созданные для извлечения коммерческой выгоды, вирусописатели проверяют на обнаружение по всем антивирусам перед тем как выпустить такой вирус в «живую природу», чтобы вирус существовал незамеченным антивирусами как можно дольше. До поступления образцов таких вирусов в лабораторию они не обнаруживаются ни одним антивирусом.

Dr.Web эффективно детектирует и лечит от вирусов

- Возможность установки и работы на уже инфицированном компьютере и исключительная вирусоустойчивость выделяют Dr.Web среди всех других аналогичных программ.
- Использование уникальных технологий обработки процессов в памяти и превосходные возможности по нейтрализации активного заражения позволяют успешно установить Dr.Web прямо на зараженную машину (без необходимости предварительного ее лечения) — даже с внешнего носителя без установки в систему (например, с USB-stick) и уже в ходе установки проводить лечение активных угроз.
- Интеграция установочного пакета (инсталлятора) с обновленным Антируткитом Dr.Web позволяет противостоять активным угрозам и уже во время установки проводить лечение ПК, даже если компьютер заражен сложными вредоносными программами.
- Подсистема фонового сканирования и нейтрализации активных угроз в рамках Антируткита Dr.Web (Anti-rootkit API, arkapi) постоянно находится в памяти и осуществляет поиск активных угроз в следующих критических областях Windows: объекты автозагрузки, запущенные процессы и модули, эвристики системных объектов, оперативная память, MBR/VBR дисков, системный BIOS компьютера. При обнаружении угроз подсистема осуществляет лечение и блокирует опасные воздействия.
- В Dr.Web реализована возможность обнаруживать и нейтрализовать вирусы, существующие в оперативной памяти и никогда не встречающиеся в виде отдельных файлов. **До сих пор лишь немногие антивирусы умеют их лечить.**
- Dr.Web способен выявлять с высочайшей степенью точности упакованные вредоносные объекты, даже упакованные неизвестным Dr.Web методом, разбирать их на отдельные компоненты и детально анализировать с целью обнаружения скрытых угроз.
- Только Dr.Web способен полностью проверять архивы любого уровня вложенности. Таким образом, даже если вредоносный объект был многократно заархивирован и при этом использовались разные типы архиваторов, Dr.Web обязательно обнаружит и обезвредит угрозу.

Высокий уровень самозащиты

Стойкий иммунитет к любым попыткам вредоносных программ вывести Dr.Web из строя обеспечивает не имеющий аналогов на антивирусном рынке компонент самозащиты **Dr.Web SelfPROtect**.

- **Dr.Web SelfPROtect** реализован в виде драйвера и действует на самом низком системном уровне. Выгрузка и остановка его работы невозможны до перезагрузки системы.

Дата актуализации 20.11.2015

- **Dr.Web SelfPROtect** ограничивает доступ вредоносных объектов к сети, файлам и папкам, некоторым веткам реестра и сменным носителям на уровне системного драйвера, защищает от попыток анти-антивирусных программ прекратить функционирование Dr.Web.
- В отличие от некоторых конкурирующих продуктов, модифицирующих ядро Windows (перехватывающих прерывания, подменяющих таблицы векторов, использующих недокументированные функции и т. д.), что может привести к серьезным проблемам в работе самой операционной системы, а также создает новые пути для использования уязвимостей, модуль защиты **Dr.Web SelfPROtect** является полностью самодостаточным.
- Возможность автоматического восстановления собственных модулей.

Передовые технологии Превентивной защиты

- **FLY-CODE** — не имеющая аналогов технология универсальной распаковки, которая позволяет обнаружить вирусы, упакованные даже неизвестными Dr.Web упаковщиками.
- Уникальная технология несигнатурного поиска **Origins Tracing**™ позволяет Dr.Web с высокой долей вероятности распознавать вирусы, еще неизвестные вирусной базе Dr.Web.
- **Эвристический анализатор Dr.Web** надежно детектирует все распространенные типы угроз, определяя их класс по результатам проведенного разбора и характерным признакам.
- **Dr.Web Process Heuristic** защищает от новых, наиболее актуальных вредоносных программ, разработанных с расчетом на необнаружение традиционными сигнатурными и эвристическими механизмами, которые еще не поступили на анализ в антивирусную лабораторию, а значит, неизвестны вирусной базе Dr.Web на момент проникновения в систему. Он анализирует поведение опасной программы и делает вывод о ее вредоносности, после чего принимаются необходимые меры по нейтрализации угрозы. Новая технология защиты данных от повреждения позволяет свести к минимуму потери от действий неизвестного вируса.
- **Комплексный анализатор упакованных угроз** значительно повышает уровень детектирования якобы «новых угроз» — известных вирусной базе Dr.Web, но скрытых под новыми упаковщиками, а также исключает необходимость добавления в базы все новых и новых записей об угрозах. Сохранение компактности вирусных баз Dr.Web в свою очередь не требует постоянного увеличения системных требований и обеспечивает традиционно малый размер обновлений — при все таком же традиционно высоком качестве детектирования и лечения.

Подробнее: http://products.drweb.ua/technologies/preventive_protection/

Полная проверка любого трафика

- Безопасный трафик — производится проверка любого трафика по всем портам, передаваемого по поддерживаемым Dr.Web протоколам, включая защищенные (если пользователь включил проверку SSL).
- Безопасный интернет-серфинг — при работе пользователя в поисковых системах Google, «Яндекс», Yahoo!, Bing, Rambler в результатах поиска отображаются только безопасные с точки зрения поисковиков и Dr.Web сайты благодаря активации в поисковиках функционала «Безопасный поиск» — небезопасный контент отсеивается самими поисковиками!
- Безопасное общение — фильтрация трафика в мгновенных сообщениях «Mail.ru Агент», ICQ, Jabber. Найденные ссылки, ведущие на вредоносные и фишинговые сайты, вырезаются из сообщений. Производится антивирусная проверка пересылаемых вложений, передача потенциально опасных вложений блокируется.

Мгновенная защита из «облака»

- В рамках Родительского контроля и веб-антивируса SpIDer Gate реализована возможность проверки URL на серверах компании «Доктор Веб» через сервис Dr.Web Cloud.
- При попытке перехода пользователя на веб-сайты, URL отправляются для проверки на серверы компании «Доктор Веб». Проверка производится в режиме реального времени — вне зависимости от состояния вирусных баз Dr.Web на компьютере пользователя и настроек обновления.

Дата актуализации 20.11.2015

- Никакой персональной информации, позволяющей идентифицировать пользователя, с компьютера не передается.

Технологии антиспам-фильтрации

Технологии фильтрации Антиспама Dr.Web состоят из нескольких тысяч правил, которые условно можно разбить на несколько групп.

Эвристический анализ

Чрезвычайно сложная, высокоинтеллектуальная технология эмпирического анализа всех частей сообщения: поля заголовка, тела сообщения и т. д. Анализируется не только само сообщение, но и содержание вложения к нему, если таковое имеется. Эвристический анализатор постоянно совершенствуется, к нему постоянно добавляются новые правила. Эвристический анализатор работает «на опережение» и позволяет распознавать еще неизвестные разновидности спама нового поколения до выпуска соответствующего обновления.

Фильтрация противодействия

Фильтрация противодействия – одна из наиболее передовых и эффективных технологий Антиспама Dr.Web. Состоит в распознавании уловок, используемых спамерами для обхода антиспам-фильтров.

Анализ на основе HTML-сигнатур

Сообщения, в состав которых входит HTML-код, сравниваются с образцами библиотеки HTML-сигнатур Антиспама. Такое сравнение, в сочетании с имеющимися данными о размерах изображений, обычно применяемых спамерами, защищает пользователей от спам-сообщений с HTML-кодом, в которые часто включаются онлайн-изображения.

Технология детектирования спамерских приемов по конвертам сообщений

Детектирование подделок в «штемпелях» SMTP-серверов и в других элементах, содержащихся в заголовках почтовых сообщений, является новейшим направлением развития методов борьбы со спамом. Адресу отправителя электронного сообщения нельзя доверять, так как может быть указан фальшивый обратный адрес. Поддельные письма – это не только спам, это могут быть мистификации или средства давления на персонал, например, анонимки и даже угрозы. Специальные технологии Антиспама Dr.Web позволяют определять поддельные адреса и не принимать такие сообщения. Это позволяет экономить трафик и ограждать сотрудников от получения поддельных писем, которые могут подтолкнуть их к непредсказуемым действиям.

Семантический анализ

В ходе этого анализа производится сравнение слов и выражений сообщения со словами и идиомами, типичными для спама. Сравнение производится по специальному словарю, причем анализу подвергаются как видимые, так и скрытые для человеческого глаза специальными техническими уловками слова, выражения и символы.

Антискамминг-технология

Скамминг-сообщения (а также фарминг-сообщения – один из видов скамминга) – пожалуй, самая опасная разновидность спам-сообщений, к числу которых относятся т. н. «нигерийские письма», сообщения о выигрышах в лотерею, казино, поддельные письма банков и кредитных учреждений. Для их фильтрации в Антиспаме Dr.Web применяется специальный модуль.

Фильтрация технического спама

Так называемые bounce-сообщения возникают как реакция на вирусы или как проявление вирусной активности – например, в результате действия почтового червя, рассылающего письма, или в виде сообщений о недоставке письма - и не менее нежелательны, чем спам. Специальный модуль Антиспама Dr.Web определяет такие сообщения как нежелательные.

Дата актуализации 20.11.2015

Преимущества Антиспама Dr.Web

- Проверка поступающей и исходящей почты производится в режиме реального времени.
- Работа Антиспама не зависит от используемой почтовой программы и не увеличивает время приема почты.
- Антиспам не требует настроек и начинает автоматически действовать с приемом первого сообщения.
- Разные технологии фильтрации обеспечивают высокую вероятность распознавания спама, фишинг-, фарминг-, скамминг- и bounce-сообщений при близком к нулю проценте ложных срабатываний.
- Отфильтрованные письма не удаляются, а перемещаются в специальную папку вашей почтовой программы, где их можно проверить в удобное для вас время на наличие ложных срабатываний.
- Модуль спам-анализатора абсолютно автономен; для его работы не требуется связи с внешним сервером или доступа к какой-либо базе данных, что позволяет существенно экономить трафик.
- Обновления к Антиспаму Dr.Web выпускаются ежедневно. Уникальные технологии распознавания нежелательной почты на основе нескольких тысяч правил позволяют производить обновления не чаще одного раза в сутки и экономить трафик.

Особая организация вирусной базы Dr.Web

Размер вирусной базы Dr.Web – минимальный среди всех существующих антивирусных программ. Достигнуто это благодаря собственной технологии создания вирусной базы на основе очень гибкого языка, специально разработанного для описания баз. Малый размер вирусной базы обеспечивает экономию трафика, позволяет занимать гораздо меньше места на диске после установки и в оперативной памяти, чем базы других производителей. Небольшой размер вирусной базы позволяет взаимодействовать компонентам программы Dr.Web в высокоскоростном режиме, не оказывая чрезмерной нагрузки на процессор.

Что самое главное в антивирусе? Обеспечивать защиту от вирусов. Обеспечивается защита, среди прочего, внесением в вирусную базу записей (сигнатур), позволяющих детектировать вирусы. А вот количество записей в вирусной базе абсолютно ничего не говорит о том, сколько реально вирусов ловит та или иная антивирусная программа. Чтобы понять, почему число записей в вирусной базе Dr.Web меньше числа записей в вирусных базах некоторых других производителей, надо знать, что не все вирусы уникальны. Существуют целые семейства родственных (подобных) вирусов, есть вирусы, созданные вирусными конструкторами. Разработчиками некоторых других антивирусов каждый такой вирус-близнец наделяется отдельной записью в вирусной базе, что утяжеляет ее. Другой принцип применен в вирусной базе Dr.Web, где всего одна запись позволяет обезвреживать десятки или сотни, а иногда даже тысячи подобных друг другу вирусов.

Преимущества вирусной базы Dr.Web

- Рекордно малое число записей.
- Малый размер обновлений.
- Всего одна запись позволяет определять десятки, сотни и даже тысячи подобных вирусов.

Принципиальное отличие вирусной базы Dr.Web от вирусных баз ряда других программ состоит в том, что при меньшем числе записей она позволяет детектировать такое же (и даже большее) число вирусов и вредоносных программ.

Что дают пользователю малый размер базы Dr.Web и меньшее число записей в ней?

- Экономия места на диске.

Дата актуализации 20.11.2015

- Экономия оперативной памяти.
- Экономия трафика при скачивании базы.
- Высокая скорость установки базы и ее обработки при анализе вирусов.
- Возможность определять вирусы, которые еще только будут созданы в будущем путем модификации уже известных.

Глобальная система обновлений Dr.Web (Dr.Web GUS)

- Служба вирусного мониторинга Dr.Web производит сбор образцов вирусов по всему миру.
- «Горячие» обновления выпускаются немедленно после анализа новой вирусной угрозы и подготовки обновления.
- Перед выпуском обновления тестируются на огромном количестве «чистых» файлов.
- Обновления поступают к пользователям с нескольких серверов, находящихся в разных точках земного шара, что минимизирует время получения обновлений.
- Процесс обновления вирусных баз и программных модулей полностью автоматизирован.
- Обновления можно скачивать в виде заархивированных файлов.

Дата актуализации 20.11.2015

Лицензии и сертификаты

В отличие от большинства конкурирующих решений, программные продукты Dr.Web Enterprise Security Suite версии 6 имеют сертификаты соответствия ФСТЭК, ФСБ и Министерства обороны РФ. Это позволяет использовать их в организациях с повышенными требованиями к уровню безопасности.

Dr.Web сертифицирован ФСТЭК на соответствие:

- ТУ и НДВ 4 на применение в составе подсистемы антивирусной защиты в информационных системах персональных данных (ИСПДн) класса К1;
- требованиям (по уровню контроля не ниже 4) руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» и требованиям технических условий.

Dr.Web полностью соответствует требованиям закона «О персональных данных», предъявляемым к антивирусным продуктам в части защиты от несанкционированного доступа и централизованной защиты каналов передачи данных, и может применяться в сетях, соответствующих максимально возможному уровню защищенности.

Компания «Доктор Веб» имеет следующие лицензии и сертификаты:

- лицензии Федеральной службы по техническому и экспортному контролю РФ (ФСТЭК) на проведение работ, связанных с созданием средств защиты информации, а также на деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- лицензия Министерства обороны Российской Федерации на деятельность в области создания средств защиты информации;
- лицензии ФСБ России на проведение работ, связанных с использованием сведений, составляющих государственную тайну;
- лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на разработку и (или) производство средств защиты конфиденциальной информации;
- сертификаты соответствия ФСБ РФ;
- сертификаты соответствия ФСТЭК РФ.

Все лицензии и сертификаты «Доктор Веб»:
http://company.drweb.com/licenses_and_certificates

Упаковка продуктов, сертифицированных ФСТЭК

Специальный медиапакет «Dr.Web Сертифицированный»

Комплектация

- Медиапакет.
- Диск (поставляется с сертифицированным дистрибутивом).
- Формуляр.
- Голографическая наклейка ФСТЭК.

Дата актуализации 20.11.2015

Лицензионный сертификат Dr.Web

ЛИЦЕНСИОННЫЙ СЕРТИФИКАТ
Dr.WEB®

Настоящий сертификат удостоверяет, что данное программное обеспечение законно приобретено у разработчика и обладателя исключительных прав на антивирусное ПО семейства **Dr.WEB** – **ООО «Доктор Веб»**

Владелец лицензии

Лицензируемый продукт

Серийный номер

Серийный номер

Серийный номер

Защищаемые объекты

Рабочие станции	Серверы
Пользователи почты	Пользователи шлюза
Мобильные устройства	Центр управления

Срок лицензии	Поставщик

Генеральный директор ООО «Доктор Веб» Шаров Б.А.

«Доктор Веб» «Doctor Web, Ltd»

Dr.Web Enterprise Security Suite

Комплексная защита всех узлов корпоративной сети

Dr.Web Enterprise Security Suite – это комплекс продуктов Dr.Web, включающий элементы защиты всех узлов корпоративной сети и единый центр управления для большинства из них.

Dr.Web® Desktop Security Suite Защита рабочих станций, клиентов терминальных и виртуальных серверов, клиентов встроенных систем	Windows, Linux, Mac OS X, MS DOS, OS/2
Dr.Web® Server Security Suite Защита файловых серверов и серверов приложений (в том числе, терминальных и виртуальных серверов)	Windows, Novell NetWare, Novell Storage Services, Mac OS X Server, Unix
Dr.Web® Mail Security Suite Защита почты	Unix, MS Exchange, Lotus, Kerio
Dr.Web® Gateway Security Suite Защита шлюзов	Unix, Kerio, MIMEsweeper, Qbik
Dr.Web® Mobile Security Suite Защита мобильных устройств	Android, Symbian OS, Windows Mobile

Бонусы

При покупке **Dr.Web Desktop Security Suite** предоставляется право бесплатного использования

- Dr.Web Mobile Security Suite
- Dr.Web CureIt!
- Dr.Web CureNet!

Лицензионный сертификат Dr.Web – это документальное подтверждение законности использования ПО Dr.Web для проверяющих органов.

ВАЖНО! Лицензионный сертификат Dr.Web не является основанием для продления лицензии и получения скидки на продление.

Сертификат обладает высокой степенью защиты. Благодаря специальной гильошированной сетке его подделка невозможна.

Поставка бланка Лицензионного сертификата с любыми продуктами Dr.Web для юридических лиц обязательна!

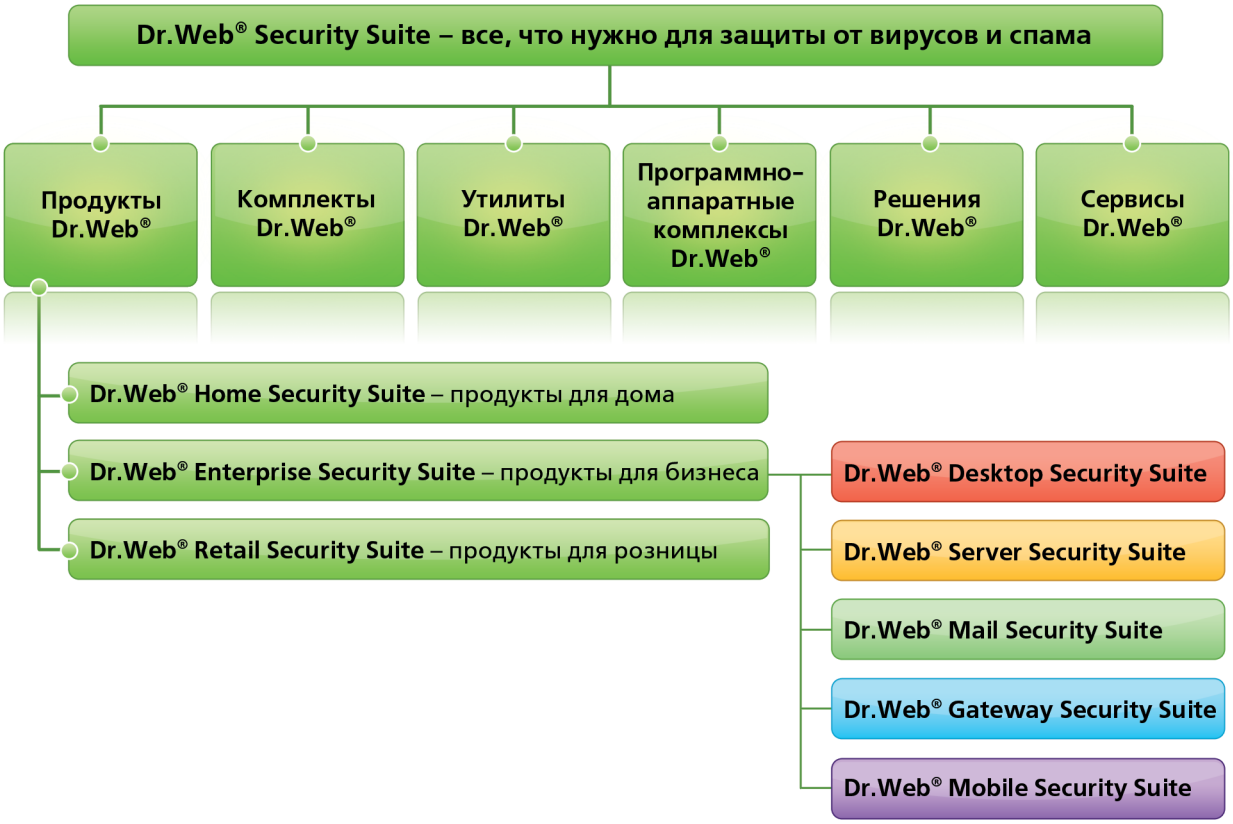
Электронную копию Лицензионного сертификата Dr.Web можно самостоятельно сгенерировать на странице

http://products.drweb.com/register/certificate.

Дата актуализации 20.11.2015

Продуктовая линейка Dr.Web Security Suite

Продуктовая линейка Dr.Web Security Suite состоит из коммерческих продуктов для дома, бизнеса и розницы, комплектов, утилит, программно-аппаратных комплексов, решений и сервисов.



Лицензирование продуктов Dr.Web

1. Продукты Dr.Web® лицензируются на 12, 24 и 36 месяцев. Dr.Web Security Space и Антивирус Dr.Web для Windows лицензируются также на 3 и 6 месяцев.
2. Продукты Dr.Web лицензируются по типу защищаемых объектов.
3. Защищаемые объекты включают в себя:
   - рабочие станции, клиенты терминальных серверов и клиенты встроенных систем;
   - файловые серверы и серверы приложений (включая терминальные серверы);
   - пользователей почты;
   - пользователей почтовых и интернет-шлюзов;
   - мобильные устройства.
4. Предусмотрено 2 типа **базовых лицензий**:
   1) Антивирус;
   2) Комплексная защита.
5. Базовая лицензия Комплексная защита предназначена только для продуктов для защиты рабочих станций под управлением ОС Windows.

Дата актуализации 20.11.2015

6. В лицензию Комплексная защита входят следующие компоненты: антивирус, антиспам, веб-антивирус, родительский (офисный) контроль, брандмауэр.
7. Необходимые покупателю дополнительные компоненты защиты добавляются к базовой лицензии. Продажа лицензии на один или несколько дополнительных компонентов отдельно от базовой лицензии невозможна.
8. Для каждого типа защищаемых объектов имеются свои виды базовых лицензий и свой набор дополнительных компонентов.

Продукт	Поддерживаемые ОС и платформы	Базовая лицензия	Дополнительные компоненты
Dr.Web® Desktop Security Suite Защита рабочих станций, клиентов терминальных серверов, клиентов виртуальных серверов и клиентов встроенных систем	Windows XP/2003/Vista/2008/7/8/2012/10 (32- и 64-битные системы)	Комплексная защита	■ Криптограф ■ Центр управления
		Антивирус	
	Linux glibc 2.7 и выше	Антивирус	■ Центр управления
	OS X 10.7 и выше		
	MS-DOS OS/2		
Dr.Web® Server Security Suite Защита файловых серверов и серверов приложений (в том числе, виртуальных и терминальных серверов)	Windows	Антивирус	■ Центр управления
	Novell NetWare		
	OS X Server		
	Unix (Samba)		
Dr.Web® Mail Security Suite Защита почты	Unix	Антивирус	■ Центр управления ■ Антиспам ■ SMTP proxy
	MS Exchange		
	Lotus (Windows/Linux)		■ Антиспам ■ SMTP proxy
	Kerio (Windows/Linux)		■ SMTP proxy
Dr.Web® Gateway Security Suite Защита шлюзов	Интернет-шлюзы Kerio (Windows/Linux)	Антивирус	■ Центр управления ■ Антиспам
	Интернет-шлюзы Unix		
	Qbik WinGate		
	MIMEsweeper		
	Microsoft ISA Server и Forefront TMG		
Dr.Web® Mobile Security Suite Защита мобильных устройств	Android OS 2.1 — 4.4	Комплексная защита	■ Центр управления ■ Антиспам
	Windows Mobile	Антивирус	■ Антиспам
	Symbian OS		

Дата актуализации 20.11.2015

Виды поставки продуктов Dr.Web

Программы Dr.Web поставляются в виде электронной лицензии или в виде медиакомплектов в упаковке.

1. Электронная лицензия Dr.Web

Поставляется в виде серийного номера Dr.Web:

- по электронной почте;
- на лицензионном сертификате.

2. Медиакомплект Dr.Web в картонной упаковке

Комплектация:

- картонная фирменная упаковка;
- лицензионный сертификат;
- краткое руководство по установке и регистрации;
- DVD-диск;
- фирменный конверт для диска;
- пломбировочная наклейка;
- наклейка «Защищено Dr.Web»;

3. Формируемое решение в картонной упаковке

Формируемое решение для одного или нескольких продуктов Dr.Web Enterprise Security Suite.

Комплектация:

- фирменная картонная коробка Dr.Web;
- бланк лицензионного сертификата;
- DVD-диск с дистрибутивами программ Dr.Web в фирменном конверте.

Дата актуализации 20.11.2015

4. Сертифицированный медиапакет

Формируемое решение для одного или нескольких продуктов Dr.Web Enterprise Security Suite, сертифицированных ФСТЭК России.

Комплектация:

- фирменная картонная коробка Dr.Web;
- бланк лицензионного сертификата;
- DVD-диск с дистрибутивами сертифицированных программ Dr.Web в фирменном конверте;
- формуляр с голографической наклейкой ФСТЭК.

5. Лицензионный пакет Dr.Web

Формируемое решение для одного или нескольких продуктов Dr.Web Enterprise Security Suite

Комплектация:

- фирменный картонный пакет Dr.Web;
- бланк лицензионного сертификата.

6. Скретч-карта

Карта с серийным номером Dr.Web, скрытым под скретч-полосой.

Дата актуализации 20.11.2015

7. OEM-продукты Dr.Web

Dr.Web OEM универсальный (однопользовательские лицензии)

Поставляется в виде OEM-карты со скретч-полосой, наклеенной на OEM-листовку. Обеспечивает защиту 1 ПК и 1 мобильного устройства в течение 3 месяцев.

Состав лицензии:

- Dr.Web Security Space
- Антивирус Dr.Web для OS X
- Антивирус Dr.Web для Linux
- Dr.Web Mobile Security
- Dr.Web для Android
- Dr.Web для Symbian OS
- Dr.Web для Windows Mobile

Продление

- Чтобы продлить срок действия OEM-лицензии Dr.Web, необходимо приобрести лицензию продления (в ее стоимость включена скидка на продление).
- Также продлить лицензию можно с помощью коробочных продуктов Dr.Web Security Space или Антивирус Dr.Web (без скидки на продление). В этом случае к сроку действия новой лицензии будут добавлены 300* бонусных дней.

* При условии покупки коробочного продукта Dr.Web с лицензией для защиты 2 ПК на 1 год и последовательной регистрации обоих серийных номеров для защиты 1 ПК.

Поставка

Поставка продукта Dr.Web OEM Универсальный партнерам «Доктор Веб» производится только в виде скретч-карт и в количестве от 250 шт. Поставка продукта в виде скретч-карт или электронных лицензий в количестве от 50 до 499 шт. производится только компаниям, имеющим статус Авторизованного сервисного центра Dr.Web (подробнее о программе для АСЦ — http://partners.drweb.com/service).

Для крупных поставщиков OEM-лицензий существует программа защиты продлений OEM-лицензий: https://pa.drweb.com/products/oem/universal/protection/.

Дата актуализации 20.11.2015

Dr.Web OEM Серверный (корпоративные лицензии)

Дает право на использование любых продуктов Dr.Web Enterprise Security Suite в течение 3 месяцев. Поставляется в виде медиапакета.

Состав лицензии:

- Центр управления Dr.Web Enterprise Security Suite;
- Dr.Web Desktop Security Suite – 100 ПК;
- Dr.Web Server Security Suite – 10 серверов;
- Dr.Web Mail Security Suite – 100 пользователей;
- Dr.Web Gateway Security Suite – 100 пользователей;
- Dr.Web Mobile Security Suite – 100 устройств.

Комплектация медиа-пакета:

- фирменный конверт Dr.Web CD-диск с презентацией обо всех продуктах Dr.Web;
- лицензионный сертификат Dr.Web с серийным номером на Dr.Web Enterprise Security Suite на 3 месяца;
- листовка «Dr.Web Enterprise Security Suite»;
- наклейка «Dr.Web OEM».

Продление

Чтобы продлить срок действия OEM-лицензии Dr.Web, необходимо приобрести лицензию, в цену которой включена 40% скидка за продление на 1 год.

Бонусная программа

Для поставщиков серверных OEM-лицензий предусмотрена специальная бонусная программа. Подробнее о ней можно узнать по адресу https://pa.drweb.com/products/oem/kod/bonuses.

Памятка OEM-поставщика:
https://st.drweb.com/static/new-www/files/Pamyatka_OEM_ru.pdf

Дата актуализации 20.11.2015

Dr.Web Home Security — продукты для дома

Состав продуктов

Dr.Web Security Space	Dr.Web Mobile Security
Защита любых устройств	Защита мобильных устройств
Программные продукты Dr.Web	
■ Dr.Web Security Space ■ Антивирус Dr.Web для Windows ■ Антивирус Dr.Web для OS X ■ Антивирус Dr.Web для Linux ■ Криптограф Atlansys Bastion Pro*	–
■ Dr.Web Security Space для Android ■ Dr.Web для Symbian OS ■ Dr.Web для Windows Mobile	■ Dr.Web Security Space для Android ■ Dr.Web для Symbian OS ■ Dr.Web для Windows Mobile

* Продукт лицензируется отдельно за дополнительную плату. Наценка за лицензирование криптографа — 20% от цены базовой лицензии. Разработчик криптографа — компания «Программные системы Атлансис» (www.atlansys.ru).

Компоненты защиты Dr.Web Security Space

Компоненты защиты	Windows	OS X	Linux
Антивирус	+	+	+
Антиспам	+		
Веб-антивирус	+	+	
Родительский контроль	+		
Брандмауэр	+		
Антивирусная сеть	+		
Криптограф*	+		
Сервисы для Windows			
Защита от потери данных (резервное копирование)	+		
Облако Dr.Web	+		
Блокировка съемных устройств	+		

* Продукт лицензируется отдельно за дополнительную плату.

Лицензирование Dr.Web Security Space

1. Продукт лицензируется по числу защищаемых ПК (1 — 5).
2. Варианты лицензий: Комплексная защита и Комплексная защита + Криптограф.

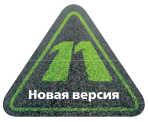
Дата актуализации 20.11.2015

3. Сроки коммерческих лицензий: 3, 6, 12, 24 или 36 месяцев. Сроки OEM-лицензий: 3 или 6 месяцев.
4. Применяются стандартные скидки на продление.
5. Никаких других скидок не предусмотрено.
6. Покупателям продукта предоставляется право бесплатного использования Dr.Web Mobile Security Suite. Количество защищаемых мобильных устройств равно количеству защищаемых ПК.

Расширение лицензии (дозакупка)

1. Расширение лицензии для Dr.Web Security Space заключается в: а) переходе с Антивируса Dr.Web на Dr.Web Security Space или Dr.Web Security Space + Криптограф или б) увеличении количества защищаемых объектов.
2. Активация лицензии дозакупки производится автоматически в момент ее генерации, с данными, указанными при регистрации прежней лицензии.
3. Если до конца срока действия лицензии остается **более 3 месяцев**, расширение производится по цене лицензии продления. Тип лицензии в коде такой лицензии — D. Лицензия продлевается автоматически.
4. Если до конца срока действия лицензии остается **менее 3 месяцев**:
   - расширение лицензии производится бесплатно через сервис бесплатного расширения;
   - прежняя лицензия блокируется через сутки после генерации новой;
   - в коде новой лицензии тип лицензии — C, а стоимость такой лицензии будет нулевой. Эту лицензию клиент впоследствии сможет продлить со скидкой;
   - для этого типа расширения переход на Dr.Web Security Space + Криптограф **не производится**.

Dr.Web Security Space



Комплексная защита для Windows, антивирус для OS X и Linux

- Улучшено! Комплексная защита ПК под управлением Windows от всех видов современных известных и новейших неизвестных интернет-угроз.
- Улучшено! Защита от наиболее актуальных вредоносных программ, разработанных с расчетом на необнаружение традиционными сигнатурными и эвристическими механизмами.
- Новое! Защита от атак эксплойтов через уязвимости «нулевого дня».
- Улучшено! Возможность установки и работы на уже инфицированном компьютере.
- Улучшено! Высокий иммунитет при попытках вредоносных программ вывести Dr.Web из строя.
- Улучшено! Высокая скорость сканирования благодаря использованию возможностей многопроцессорных систем.
- Улучшено! Защита в режиме онлайн без ущерба производительности ПК.
- Улучшено! Высокая скорость фильтрации веб-трафика и почты без задержки при онлайн-играх, воспроизведении потокового видео и прослушивании онлайн-радио.
- Новое! Абсолютно новый алгоритм создания и хранения резервных копий важных файлов с помощью компонента «Защита данных от повреждения». Минимальная нагрузка на систему в ходе создания резервных копий — при любых объемах данных!
- Полная проверка архивов любого уровня вложенности.
- Запрет доступа к сайтам, которые используются для распространения вредоносных или потенциально опасных программ, к фишинговым сайтам и сайтам, на которых используются методы социальной инженерии для обмана посетителей.
- Фильтрация спама и всех видов нежелательных сообщений без необходимости обучения антиспама.

Дата актуализации 20.11.2015

- Улучшено! Полная проверка «на лету» любого трафика по всем портам.
- Безопасный интернет-серфинг в поисковых системах Google, Yandex, Yahoo!, Bing, Rambler — небезопасный контент отсеивается самими поисковиками!
- Безопасное общение — фильтрация трафика в мгновенных сообщениях.
- Улучшено! Эффективная защита детей от нежелательного контента.
- Улучшено! Блокировка возможности несанкционированного использования съемных устройств и компьютера.
- Облачный сервис Dr.Web Cloud — мгновенная проверка URL на серверах компании «Доктор Веб».
- Новое! Облачный сервис репутационной проверки процессов на вредоносность.
- Защита от несанкционированного доступа извне, блокировка подозрительных соединений на уровне пакетов и приложений.
- Удаленное управление Dr.Web на других компьютерах в пределах одной локальной сети без установки Центра управления Dr.Web.

Компоненты защиты

Эффективное детектирование и очистка системы от всех видов угроз (Сканер Dr.Web)

- Новое в версии 11! Еще более быстрая проверка объектов на наличие угроз благодаря оптимизации модуля Dr.Web Scanning Engine.
- Высокая скорость сканирования благодаря использованию нескольких потоков проверки в многопроцессорных системах.
- Максимально тщательная проверка оперативной памяти, загрузочных секторов, жестких дисков и сменных носителей на вирусы, троянские программы и другие виды вредоносных объектов.
- Детектирование только работоспособных вирусных угроз.
- Обширные базы для детектирования шпионского, потенциально опасного, рекламного ПО, хакерских утилит и программ-шуток.
- Используемый Сканером антируткит Dr.Web Shield™ определяет сложные вирусы, использующие руткит-технологии и умеющие скрывать свое пребывание в инфицированной системе.
- Консольный сканер, который также входит в состав компонентов Dr.Web, рассчитан на опытных пользователей и позволяет проводить проверку в режиме командной строки. Он содержит большие возможности настройки и рассчитан в том числе на работу в многопроцессорных системах.

Защита в режиме реального времени (файловый монитор SpIDer Guard®)

- Файловый монитор SpIDer Guard осуществляет постоянный мониторинг здоровья компьютера — перехватывает «на лету» обращения к файлам на дисках, дискетах, CD/DVD/Blu-ray-дисководах, флеш- и смарт-картах.
- Обладает высокой устойчивостью к попыткам вредоносных программ препятствовать функционированию SpIDer Guard или остановить его работу.
- Реализованные в антивирусном ядре Dr.Web технологии динамически отслеживают наличие свободных ресурсов и ограничивают «аппетит» антивируса без снижения эффективности защиты.
- Высокая производительность работы на машинах с интенсивным файловым потоком (при интенсивной работе с файловыми системами, например, при скачивании файлов с торрент и шаринг-трекеров, компиляции и рендеринге).

Дата актуализации 20.11.2015

Защита от неизвестных угроз (Превентивная защита)

Комплекс технологий, входящих в Превентивную защиту Dr.Web, усиливает традиционную сигнатурную защиту Dr.Web, дополняя ее новейшими несигнатурными (поведенческими) инструментами. Благодаря Превентивной защите Dr.Web способен:

- Защищать от проникновения новейших, наиболее опасных вредоносных программ, разработанных с расчетом на необнаружение традиционными сигнатурными и эвристическими механизмами, — объектов, которые еще не поступили на анализ в антивирусную лабораторию, а значит, не известны вирусной базе Dr.Web на момент проникновения в систему;
- Распознавать нежелательные изменения пользовательских файлов, отслеживая работу всех процессов системы в поисках действий, характерных для процессов вредоносных программ (например, действий троянцев-шифровальщиков), не позволяя вредоносным объектам внедриться в процессы других программ;
- Обнаруживать и нейтрализовать новейшие, еще не известные вирусной базе Dr.Web угрозы: троянцев-вымогателей (шифровальщиков), инжекторы, удаленно управляемые вредоносные объекты (распространяемые для организации ботнетов и шпионажа), а также вирусные упаковщики.

Высокий уровень самозащиты

Стойкий иммунитет к любым попыткам вредоносных программ вывести Dr.Web из строя обеспечивает не имеющий аналогов на антивирусном рынке компонент самозащиты Dr.Web SelfPROtect.

- Dr.Web SelfPROtect реализован в виде драйвера и действует на самом низком системном уровне. Выгрузка и остановка его работы невозможны до перезагрузки системы.
- Dr.Web SelfPROtect ограничивает доступ вредоносных объектов к сети, файлам и папкам, некоторым веткам реестра и сменным носителям на уровне системного драйвера, защищает от попыток анти-антивирусных программ прекратить функционирование Dr.Web.
- В отличие от некоторых конкурирующих продуктов, модифицирующих ядро Windows (перехватывающих прерывания, подменяющих таблицы векторов, использующих недокументированные функции и т. д.), что может привести к серьезным проблемам в работе самой операционной системы, а также создает новые пути для использования уязвимостей, модуль защиты Dr.Web SelfPROtect является полностью самодостаточным.
- SelfPROtect имеет возможность автоматического восстановления собственных модулей.

Новое в версии 11! **Новый компонент Dr.Web HyperVisor** позволил усовершенствовать систему обнаружения и лечения угроз, а также усилить самозащиту Dr.Web путем использования возможностей современных процессоров. Компонент запускается и работает на минимально возможном уровне операционной системы, что обеспечивает контроль всех программ, процессов и работы самой ОС, а также невозможность перехвата вредоносными программами контроля над защищаемой Dr.Web системой.

Такой подход позволил разработчикам Dr.Web преодолеть ограничения, накладываемые на антивирусы особенностями 64-битных операционных систем, вынуждавших антивирус функционировать на том же уровне, что и вредоносные программы.

Обеспечивается совместимость с системами виртуализации VirtualBox, VmWare, Hyper-V, Parallels.

Фильтрация интернет-трафика (веб-антивирус SplDer Gate)

- Новое в версии 11! Благодаря переработке системы антивирусной проверки трафика Dr.Web Net filtering Service процесс скачивания больших файлов существенно ускорен; переработан процесс сканирования потокового мультимедийного контента — онлайн-просмотр видео и прослушивание интернет-радио теперь происходят без задержек. Нагрузка на процессор значительно уменьшилась при работе как через популярные браузеры, так и через менеджеры закачек. Поклонники Dr.Web и сетевых игр заметят разницу в скорости проверки!

Дата актуализации 20.11.2015

- Новое в версии 11! Новые параметры настроек исключений для ускорения сканирования. Так, из проверки могут быть исключены:
  - данные, передаваемые по защищенному протоколу HTTPS;
  - трафик доверенных приложений, имеющих валидную цифровую подпись.

  Новые возможности позволят без существенных потерь в безопасности избегать конфликтов Dr.Web со сторонним программным обеспечением при фильтрации трафика.
- Веб-антивирус SpIDer Gate в режиме реального времени прозрачно сканирует входящий HTTP-трафик, перехватывает все HTTP-соединения, производит фильтрацию данных, автоматически блокирует зараженные страницы в любых веб-браузерах, проверяет файлы в архивах (например, загружаемые через менеджеров загрузки, и многие другие приложения, обменивающиеся данными с веб-серверами), защищает от фишинговых и других опасных интернет-ресурсов.
- Безопасный интернет-трафик — производится проверка любого трафика по всем портам, передаваемого по поддерживаемым Dr.Web протоколам, включая защищенные (если пользователь включил проверку SSL).
- Безопасный интернет-серфинг — при работе пользователя в поисковых системах Google, Yandex, Yahoo!, Bing, Rambler в результатах поиска отображаются только безопасные с точки зрения поисковиков и Dr.Web сайты благодаря активации в поисковиках функционала «Безопасный поиск» — небезопасный контент отсеивается самими поисковиками!
- Безопасное общение — фильтрация трафика в мгновенных сообщениях Mail.Ru Agent, ICQ, Jabber. Найденные ссылки, ведущие на вредоносные и фишинговые сайты, вырезаются из сообщений. Производится антивирусная проверка пересылаемых вложений, передача потенциально опасных вложений блокируется.
- Проверка шифрованных SSL-соединений (HTTPS).
- Запрет доступа к сайтам, которые используются для распространения вредоносных или потенциально опасных программ, к фишинговым сайтам и сайтам, на которых используются методы социальной инженерии для обмана посетителей.
- Отдельная база сайтов, распространяющих нелицензионный контент, — защита правообладателей контента.
- Отключение проверки исходящего или входящего трафика, а также формирование списка тех приложений, HTTP-трафик которых будет проверяться в любом случае и в полном объеме (черный список). Также существует возможность исключения из проверки трафика отдельных приложений (белый список).
- Настройка приоритетности сканирования трафика (баланса проверки). Балансировка влияет на распределение ресурсов процессора ПК и скорость работы с сетью Интернет.
- Работа SpIDer Gate не зависит от используемого браузера.
- Фильтрация практически не сказывается на производительности ПК, скорости работы с Интернетом и количестве передаваемых данных.
- В режиме «по умолчанию» не требуется никакой настройки: SpIDer Gate начинает сканирование сразу же после установки в системе.
- Проверка URL на серверах компании «Доктор Веб» через сервис Dr.Web Cloud. При попытке перехода пользователя на веб-сайты URL отправляются для проверки на серверы компании «Доктор Веб». Проверка производится в режиме реального времени — вне зависимости от состояния вирусных баз Dr.Web на компьютере пользователя и настроек обновления

Почта без вирусов, спама и нежелательных сообщений (почтовый антивирус SpIDer Mail + антиспам)

- Проверка любого трафика по всем портам, передаваемого по поддерживаемым Dr.Web протоколам, включая защищенные (если пользователь включил проверку SSL).

Дата актуализации 20.11.2015

- Почтовый антивирус SpIDer Mail проверяет почту до поступления письма в почтовый клиент и не дает вредоносным программам — разносчиком которых является в основном спам — воспользоваться уязвимостями в программном обеспечении.
- Проверка почты на вирусы и спам в режиме реального времени по протоколам SMTP/POP3/NNTP/IMAP4.
- Проверка шифрованных SSL-соединений (SMTPS/POP3S/IMAP4S).
- Проверка не влияет на работу используемой почтовой программы и практически не увеличивает время приема почты.
- Применяются индивидуальные правила обработки для каждого типа вредоносных программ — вирусов, потенциально опасного и рекламного ПО, хакерских утилит, программ платного дозвона, программ-шуток.
- Защита от массовых рассылок сообщений почтовыми червями благодаря анализу состава и времени отправления исходящих писем, по которым может быть сделан вывод о вирусной активности.

Антиспам

- Антиспам не требует настроек и начинает автоматически действовать с приемом первого сообщения.
- Разные технологии фильтрации обеспечивают высокую вероятность распознавания спама, фишинг-, фарминг-, скамминг- и bounce-сообщений.
- Защита от попадания в ботнеты — провайдер не отключит вам доступ к Интернету за рассылку спама.
- Отфильтрованные письма не удаляются, а перемещаются в специальную папку вашей почтовой программы, где их можно проверить в удобное для вас время на наличие ложных срабатываний.
- Модуль спам-анализатора абсолютно автономен; для его работы не требуется связи с внешним сервером или доступа к какой-либо базе данных, что позволяет существенно экономить трафик.

Забота о безопасности детей и близких. Контроль за интернет-серфингом и блокировка доступа (Родительский контроль Dr.Web)

Безопасный интернет-трафик

- Проверка любого трафика по всем портам.
- Проверка URL на серверах компании «Доктор Веб» через сервис Dr.Web Cloud в режиме реального времени — вне зависимости от состояния вирусных баз Dr.Web на компьютере пользователя и настроек обновления (подробнее).
- Блокировка веб-сайтов по 10 тематическим группам (оружие, наркотики, игры, порнография и др.).
- Защита детей от посещения нежелательных страниц.

Ограничение доступа к ПК и Интернету

- Ограничение времени работы пользователя в сети Интернет и за компьютером.
- Блокировка изменения системного времени и часового пояса — исключает возможность работы ребенка за компьютером в несанкционированное родителями время.
- Новое в версии 11! «Интервальное ограничение времени» (с получасовым шагом) — возможность задавать время, которое ребенок может провести за компьютером в течение дня.
- Новое в версии 11! Автоматическая блокировка доступа к ПК на ночь.
- Новое в версии 11! Профили для настройки «Ограничение времени».

Дата актуализации 20.11.2015

Блокировка доступа к файлам и папкам

- Запрет использования отдельных файлов и каталогов — дополнительная возможность обезопасить свои данные и важную информацию от удаления или похищения злоумышленниками.
- Новое в версии 11! Настройка типа доступа к указанным объектам (блокировать доступ или разрешать только чтение) — расширение возможности ограничения доступа к файлам и папкам.

А также:

- Профили настроек Родительского контроля отдельно для каждого пользователя.
- Возможность копировать настройки между учетными записями пользователей.
- Возможность отключать Родительский контроль для конкретной учетной записи.

Блокировка устройств для перекрытия всех путей возможного проникновения угроз

- Ограничение доступа к устройствам — дисковым накопителям, приводам DVD/CD-ROM, клавиатуре, компьютерной мыши, сетевым картам, устройствам проигрывания звука и видео, игровым устройствам, USB-устройствам, COM/LPT-портам.
- Запрет использования переносных хранилищ информации (флеш-дисков, USB-устройств), сетевых устройств, а также отдельных файлов и каталогов — дополнительная возможность обезопасить свои данные и важную информацию от удаления или похищения злоумышленниками.
- Белые списки доверенных устройств защитят от несанкционированного подключения съемного устройства к защищенному Dr.Web компьютеру, сохранят конфиденциальные данные от похищения через флешки, не позволят вирусам проникнуть в систему через этот популярный сегодня источник распространения.
- Улучшено в версии 11! Управление белыми списками блокируемых устройств для более гибкой настройки доступа к объектам системы.
- Экспорт/импорт белых списков.
- Запрет отправки заданий на печать — защита от несанкционированной печати конфиденциальных документов или расходования бумаги.

Защита от сетевых атак (Брандмауэр Dr.Web)

- Защита от несанкционированного доступа извне, предотвращение утечек важных данных по сети, блокировка подозрительных соединений на уровне пакетов и приложений.
- Брандмауэр Dr.Web использует собственную базу доверенных приложений. Доверенность приложения базируется на цифровом сертификате — все программы, легитимные с точки зрения Dr.Web, могут соединяться с любым адресом и по любому порту. Исключение: если приложение не имеет валидной подписи, имеет недействительную цифровую подпись или не имеет ее вовсе (например, «самописное» или open source) — выдается запрос на создание правила.
- Контроль подключений на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам и регистрировать информацию о попытках доступа в журнале приложений.
- Фильтрация на уровне пакетов позволяет контролировать доступ к сети Интернет вне зависимости от программ, инициирующих подключение. Журнал пакетного фильтра хранит информацию о пакетах, переданных через сетевые интерфейсы.
- Так называемый «игровой режим», при включении которого окно с запросом на создание правила появляется поверх любого приложения, запущенного в полноэкранном режиме.
- Мониторинг приложений, которые используют сеть в реальном времени, с возможностью принудительно завершить соединение.

Дата актуализации 20.11.2015

Управление защитой всех компьютеров в вашей семье (Антивирусная сеть)

- В компоненте Антивирусная сеть реализованы удаленное управление и настройка антивирусов Dr.Web, установленных на компьютерах в пределах одной локальной сети.
- Для удаленного управления не требуется установка Центра управления Dr.Web.
- Подключение возможно с любого компьютера к любому другому компьютеру.
- Возможности управления включают: получение статистики и логов с удаленной станции, чтение и изменение настроек модулей на ней, их запуск и остановку. Также доступны регистрация серийного номера и замена ключевого файла на удаленной станции.
- Для удаленного доступа требуется включение разрешения такого доступа на удаленной станции.

Сохранность информации и удаление ненужных вам данных без возможности восстановления (Криптограф Atlansys Bastion Pro*)

- Шифрование информации в специальных файловых контейнерах, к которым невозможно получить доступ без знания пароля.
- Поддержка работы большинства известных алгоритмов шифрования.
- Подключенный секретный диск доступен как обычный логический диск системы.
- Безопасная работа с зашифрованной информацией как на отдельно стоящем компьютере, так и при его подключении к сети.
- Удаление ненужных файлов без возможности восстановления содержавшейся в них информации.
- Для работы не требуется специальных знаний. Подробная система подсказок позволяет быстро освоить различные возможности системы.

* Только в лицензии Dr.Web Security Space + Криптограф. Разработчик криптографа Atlansys Bastion Pro — компания «Программные системы Атлансис» (www.atlansys.ru).

Системные требования

Для Dr.Web Security Space

- Windows 10/8/7/Vista (64-битные системы) и Windows 10/8/7/Vista/XP SP2 (32-битные системы).
- Оперативная память: не менее 512 МБ.
- Свободное пространство на жестком диске: ~1 ГБ. Временные файлы, создаваемые в ходе установки, потребуют дополнительного места.

Дополнительно: доступ к сети Интернет для регистрации и получения обновлений.

Лицензирование

Виды лицензий

- По числу защищаемых рабочих станций.

Варианты лицензий

- Комплексная защита.
- Комплексная защита + Криптограф.

Описание: http://products.drweb.com/win/security_space

Дата актуализации 20.11.2015

Антивирус Dr.Web для Windows

Минимальная защита от вредоносных программ для Windows, OS X, Linux

- Улучшено! Защита от наиболее актуальных современных известных и новейших неизвестных интернет-угроз и вредоносных программ, разработанных с расчетом на необнаружение традиционными сигнатурными и эвристическими механизмами.
- Улучшено! Защита от наиболее актуальных вредоносных программ, разработанных с расчетом на необнаружение традиционными сигнатурными и эвристическими механизмами.
- Новое! Защита от атак эксплойтов через уязвимости «нулевого дня».
- Улучшено! Возможность установки и работы на уже инфицированном компьютере.
- Улучшено! Высокий иммунитет при попытках вредоносных программ вывести Dr.Web из строя.
- Улучшено! Высокая скорость сканирования благодаря использованию возможностей многопроцессорных систем.
- Улучшено! Защита в режиме онлайн без ущерба производительности ПК.
- Полная проверка архивов любого уровня вложенности.
- Защита от несанкционированного доступа извне, блокировка подозрительных соединений на уровне пакетов и приложений.

Эффективное детектирование и очистка системы от всех видов угроз (Сканер Dr.Web)

- Новое в версии 11! Еще более быстрая проверка объектов на наличие угроз благодаря оптимизации модуля Dr.Web Scanning Engine.
- Высокая скорость сканирования благодаря использованию нескольких потоков проверки в многопроцессорных системах.
- Максимально тщательная проверка оперативной памяти, загрузочных секторов, жестких дисков и сменных носителей на вирусы, троянские программы и другие виды вредоносных объектов.
- Детектирование только работоспособных вирусных угроз.
- Обширные базы для детектирования шпионского, потенциально опасного, рекламного ПО, хакерских утилит и программ-шуток.
- Используемый Сканером антируткит Dr.Web Shield™ определяет сложные вирусы, использующие руткит-технологии и умеющие скрывать свое пребывание в инфицированной системе.
- Консольный сканер, который также входит в состав компонентов Dr.Web, рассчитан на опытных пользователей и позволяет проводить проверку в режиме командной строки. Он содержит большие возможности настройки и рассчитан в том числе на работу в многопроцессорных системах.

Защита в режиме реального времени (файловый монитор SpIDer Guard®)

- Файловый монитор SpIDer Guard осуществляет постоянный мониторинг здоровья компьютера – перехватывает «на лету» обращения к файлам на дисках, дискетах, CD/DVD/Blu-ray-дисководах, флеш- и смарт-картах.
- Обладает высокой устойчивостью к попыткам вредоносных программ препятствовать функционированию SpIDer Guard или остановить его работу.
- Реализованные в антивирусном ядре Dr.Web технологии динамически отслеживают наличие свободных ресурсов и ограничивают «аппетит» антивируса без снижения эффективности защиты.
- Высокая производительность работы на машинах с интенсивным файловым потоком (при интенсивной работе с файловыми системами, например, при скачивании файлов с торрент- и шаринг-трекеров, компиляции и рендеринге).

Дата актуализации 20.11.2015

Защита от неизвестных угроз (Превентивная защита)

Комплекс технологий, входящих в Превентивную защиту Dr.Web, усиливает традиционную сигнатурную защиту Dr.Web, дополняя ее новейшими несигнатурными (поведенческими) инструментами. Благодаря Превентивной защите Dr.Web способен:

- Защищать от проникновения новейших, наиболее опасных вредоносных программ, разработанных с расчетом на необнаружение традиционными сигнатурными и эвристическими механизмами, — объектов, которые еще не поступили на анализ в антивирусную лабораторию, а значит, не известны вирусной базе Dr.Web на момент проникновения в систему;
- Распознавать нежелательные изменения пользовательских файлов, отслеживая работу всех процессов системы в поисках действий, характерных для процессов вредоносных программ (например, действий троянцев-шифровальщиков), не позволяя вредоносным объектам внедриться в процессы других программ;
- Обнаруживать и нейтрализовать новейшие, еще не известные вирусной базе Dr.Web угрозы: троянцев-вымогателей (шифровальщиков), инжекторы, удаленно управляемые вредоносные объекты (распространяемые для организации ботнетов и шпионажа), а также вирусные упаковщики.

Высокий уровень самозащиты

Стойкий иммунитет к любым попыткам вредоносных программ вывести Dr.Web из строя обеспечивает не имеющий аналогов на антивирусном рынке компонент самозащиты Dr.Web SelfPROtect.

- Dr.Web SelfPROtect реализован в виде драйвера и действует на самом низком системном уровне. Выгрузка и остановка его работы невозможны до перезагрузки системы.
- Dr.Web SelfPROtect ограничивает доступ вредоносных объектов к сети, файлам и папкам, некоторым веткам реестра и сменным носителям на уровне системного драйвера, защищает от попыток анти-антивирусных программ прекратить функционирование Dr.Web.
- В отличие от некоторых конкурирующих продуктов, модифицирующих ядро Windows (перехватывающих прерывания, подменяющих таблицы векторов, использующих недокументированные функции и т. д.), что может привести к серьезным проблемам в работе самой операционной системы, а также создает новые пути для использования уязвимостей, модуль защиты Dr.Web SelfPROtect является полностью самодостаточным.
- SelfPROtect имеет возможность автоматического восстановления собственных модулей.

Новое в версии 11! **Новый компонент Dr.Web HyperVisor** позволил усовершенствовать систему обнаружения и лечения угроз, а также усилить самозащиту Dr.Web путем использования возможностей современных процессоров. Компонент запускается и работает на минимально возможном уровне операционной системы, что обеспечивает контроль всех программ, процессов и работы самой ОС, а также невозможность перехвата вредоносными программами контроля над защищаемой Dr.Web системой.

Такой подход позволил разработчикам Dr.Web преодолеть ограничения, накладываемые на антивирусы особенностями 64-битных операционных систем, вынуждавших антивирус функционировать на том же уровне, что и вредоносные программы.

Обеспечивается совместимость с системами виртуализации VirtualBox, VmWare, Hyper-V, Parallels.

Почта без вирусов (Почтовый антивирус SpIDer Mail)

- Проверка любого трафика по всем портам, передаваемого по поддерживаемым Dr.Web протоколам, включая защищенные (если пользователь включил проверку SSL).
- Почтовый антивирус SpIDer Mail проверяет почту до поступления письма в почтовый клиент и не дает вредоносным программам — разносчиком которых является в основном спам — воспользоваться уязвимостями в программном обеспечении.

Дата актуализации 20.11.2015

- Проверка почты на вирусы и спам в режиме реального времени по протоколам SMTP/POP3/NNTP/IMAP4.
- Проверка шифрованных SSL-соединений (SMTPS/POP3S/IMAP4S).
- Проверка не влияет на работу используемой почтовой программы и практически не увеличивает время приема почты.
- Применяются индивидуальные правила обработки для каждого типа вредоносных программ — вирусов, потенциально опасного и рекламного ПО, хакерских утилит, программ платного дозвона, программ-шуток.
- Защита от массовых рассылок сообщений почтовыми червями благодаря анализу состава и времени отправления исходящих писем, по которым может быть сделан вывод о вирусной активности.

Защита от сетевых атак (Брандмауэр Dr.Web)

- Защита от несанкционированного доступа извне, предотвращение утечек важных данных по сети, блокировка подозрительных соединений на уровне пакетов и приложений.
- Брандмауэр Dr.Web использует собственную базу доверенных приложений. Доверенность приложения базируется на цифровом сертификате — все программы, легитимные с точки зрения Dr.Web, могут соединяться с любым адресом и по любому порту. Исключение: если приложение не имеет валидной подписи, имеет недействительную цифровую подпись или не имеет ее вовсе (например, «самописное» или open source) — выдается запрос на создание правила.
- Контроль подключений на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам и регистрировать информацию о попытках доступа в журнале приложений.
- Фильтрация на уровне пакетов позволяет контролировать доступ к сети Интернет вне зависимости от программ, инициирующих подключение. Журнал пакетного фильтра хранит информацию о пакетах, переданных через сетевые интерфейсы.
- Так называемый «игровой режим», при включении которого окно с запросом на создание правила появляется поверх любого приложения, запущенного в полноэкранном режиме.
- Мониторинг приложений, которые используют сеть в реальном времени, с возможностью принудительно завершить соединение.

Системные требования

- Windows 10/8/7/Vista (64-битные системы) и Windows 10/8/7/Vista/XP SP2 (32-битные системы).
- Оперативная память: не менее 512 МБ.
- Свободное пространство на жестком диске: ~750 МБ. Временные файлы, создаваемые в ходе установки, потребуют дополнительного места.
- OS X 10.7 и выше (32- и 64-битные системы).
- Linux 2.6 и выше (32- и 64-битные системы).

Дополнительно: доступ к сети Интернет для регистрации и получения обновлений.

Лицензирование

Виды лицензий

- По числу защищаемых рабочих станций.

Варианты лицензий

- Антивирус (лицензия включает следующие компоненты защиты: антивирус и брандмауэр).

Дата актуализации 20.11.2015

Dr.Web Katana

Несигнатурный антивирус

для превентивной защиты от новейших активных угроз, целевых атак и попыток проникновения, в том числе через уязвимости «нулевого дня», которые еще не известны вашему антивирусу.

Преимущества

- Нейтрализует новейшие, еще не известные вашему антивирусу угрозы, разработанных с расчетом на необнаружение традиционными сигнатурными и эвристическими механизмами.
- Обеспечивает безопасность практически с момента запуска операционной системы — Dr.Web Katana начинает защищать еще до завершения загрузки традиционного сигнатурного антивируса!
- В отличие от традиционного антивируса Dr.Web Katana практически не потребляет ресурсов.
- Контролирует все процессы системы, по характерному поведению выявляет вредоносные и блокирует их. Анализирует поведение каждой запущенной программы «на лету», сверяясь с постоянно обновляемым репутационным облаком Dr.Web, и на основе актуальных знаний о том, как ведут себя вредоносные программы, делает вывод о ее опасности, после чего принимает необходимые меры по нейтрализации угрозы.
- Не требует никакой настройки и начинает эффективно действовать сразу после установки.
- Защищает даже без доступа ПК к Интернету.

Функциональные возможности

- Защищает критически важные участки системы от модификаций вредоносными программами.
- Выявляет и прекращает вредоносные, подозрительные или ненадежные сценарии и процессы.
- Распознает нежелательные изменения файлов, отслеживая работу всех процессов в системе в поисках действий, характерных для поведения вредоносных программ (например, действий троянцев-вымогателей), не позволяя вредоносным объектам внедриться в процессы других программ.
- Обнаруживает и нейтрализует новейшие угрозы: троянцев-вымогателей (шифровальщиков), инжекторы, удаленно управляемые вредоносные объекты (распространяемые для организации ботнетов и шпионажа), а также вирусные упаковщики.
- Защищает от эксплойтов — вредоносных объектов, пытающихся для проникновения в систему использовать уязвимости, в том числе еще не известные никому, кроме вирусописателей (т. н. уязвимости «нулевого дня»).
- Контролирует работу не только наиболее популярных браузеров, но и любых плагинов к ним; защищает от блокировщиков браузеров.
- Блокирует возможность изменения вредоносными программами загрузочных областей диска с целью невозможности запуска (например, троянцев) на компьютере.
- Предотвращает отключение безопасного режима Windows, блокируя изменения реестра.
- Не позволяет вредоносным программам добавлять в логику работы операционной системы исполнение новых задач, нужных злоумышленникам. Блокирует ряд параметров в реестре Windows, что не дает, например, изменить вирусам нормальное отображение Рабочего стола или скрыть присутствие троянца в системе при помощи руткита.

Дата актуализации 20.11.2015

- Не позволяет вредоносному ПО изменить правила запуска программ.
- Пресекает загрузки новых или неизвестных драйверов без ведома пользователя.
- Блокирует автозапуск вредоносных программ, а также определенных приложений, например, анти-антивирусов, не давая им зарегистрироваться в реестре для последующего запуска.
- Блокирует ветки реестра, которые отвечают за драйверы виртуальных устройств, что делает невозможной установку нового виртуального устройства.
- Блокирует коммуникации между компонентами шпионского ПО и управляющим ими сервером.
- Не позволяет вредоносному ПО нарушить нормальную работу системных служб, например, вмешаться в штатное создание резервных копий файлов.

Системные требования

- Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32-битные системы)
- Windows 10/8/8.1/7/Vista SP2 (64-битные системы)
- Оперативная память: не менее 512 МБ.
- Свободное пространство на жестком диске: ~150 МБ. Временные файлы, создаваемые в ходе установки, потребуют дополнительного места.

Лицензирование

Виды лицензий

- По числу защищаемых рабочих станций.

Варианты лицензий

- Katana (лицензия включает следующие компоненты защиты: антивирус и Облако Dr.Web).

Дата актуализации 20.11.2015

Антивирус Dr.Web для OS X

Защита от вредоносного ПО, созданного для инфицирования не только OS X, но и других операционных систем.

Этот продукт доступен в составе лицензий Dr.Web Security Space и Антивирус Dr.Web.

Функциональные возможности

- Проверка объектов автозапуска, сменных носителей информации, сетевых и логических дисков, почтовых форматов, файлов и каталогов, включая упакованные и находящиеся в архивах.
- Выбор типа сканирования: быстрое, полное и выборочное.
- Антивирусная проверка вручную, автоматически или по заранее составленному расписанию.
- Защита настроек монитора SpIDer Guard® паролем от несанкционированного изменения.
- Применение действий для зараженных, подозрительных объектов и объектов другого типа, включая лечение, перемещение в карантин и удаление, в том числе в случае если выбранное ранее действие оказалось невозможным.
- Исключение из проверки путей и файлов по запросу пользователя.
- Обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками.
- Регистрация времени события, объекта проверки и типа воздействия на него.
- Новинка версии 10! Веб-антивирус Dr.Web SpiDer Gate® — проверка HTTP-трафика и контроль доступа к интернет-ресурсам.
- Новинка версии 10! Защита от посещения нежелательных веб-сайтов (сайтов, посвященных насилию, азартным играм и т. п.).
- Загрузка обновлений автоматически (по расписанию) или по требованию.
- Автоматическое оповещение (в том числе с помощью звуковых уведомлений) о вирусных событиях.
- Изоляция зараженных файлов в карантине с возможностью задания времени хранения объектов в карантине и его максимального размера.
- Лечение, восстановление или удаление перемещенных в карантин объектов
- Ведение подробного отчета о работе.
- Доступность модулей в виде утилит командной строки, с возможностью их встраивания в используемые для обслуживания системы Apple Scripts.

Системные требования

Антивирус Dr.Web для OS X

- OS X 10.7 и выше.
- Оперативная память — в соответствии с требованиями ОС.
- Доступ к сети Интернет: для регистрации и получения обновлений.

Описание: http://products.drweb.com/mac

Дата актуализации 20.11.2015

Антивирус Dr.Web для Linux

Минимально необходимая защита от вирусов

Ключевые функции

- Детектирование и нейтрализация вирусов и вредоносных объектов на жестких дисках и сменных носителях.
- Определение вирусов в архивах любой степени вложенности и в упакованных объектах.
- Проверка файлов, сжатых упаковщиками, в том числе неизвестными, с помощью технологи FLY-CODE™.
- Защита от неизвестных угроз при помощи технологии несигнатурного поиска Origins Tracing™ и интеллектуального эвристического анализатора Dr.Web.
- Быстрая, полная, выборочная или пользовательская проверка.
- Постоянный мониторинг здоровья компьютера – перехват «на лету» обращений к файлам на дисках, дискетах, CD/DVD/Blu-ray-дисководах, флеш- и смарт-картах.
- Защита собственных компонентов от попыток вредоносных программ препятствовать работе антивируса.
- Изоляция зараженных объектов в карантине с возможностью их восстановления; функция ограничения размера карантина.
- Сбор полной статистики о работе антивируса.
- Автоматические обновления по расписанию и по требованию.

Преимущества

- Удобный центр управления.
- Возможность проверки «на лету».
- Настройка пользовательских проверок.
- Управляемый карантин.
- Автоматические обновления.
- Стильный интерфейс.

Системные требования

- Операционная система: дистрибутивы GNU/Linux, работающие на платформе Intel x86/amd64 на основе ядра 2.6.37 (и выше) и использующие библиотеку glibc версии 2.13 (и выше).
- Не менее 512 МБ свободного дискового пространства.
- Доступ к сети Интернет для регистрации и получения обновлений.

Описание: http://products.drweb.com/linux

Консольные сканеры Dr.Web

Антивирусная защита с расширенными возможностями ее автоматизации для опытных пользователей.

Консольные сканеры Dr.Web без графического интерфейса используют общую вирусную базу и поисковый модуль Dr.Web и предназначены для работы в операционных системах MS DOS, OS/2 и Windows. Для управления антивирусной защитой необходимы навыки работы с командной строкой.

Преимущества

- Минимальные системные требования – сканеры прекрасно работают даже на встроенных системах и способны надежно защитить маломощные компьютеры прежних поколений.

Дата актуализации 20.11.2015

- Удобство проверки – администратор может выбрать «ручное» сканирование или проверку по расписанию.
- Лечение зараженных рабочих станций и серверов, в том числе недоступных по сети.
- Высокая вирусоустойчивость и возможность установки на зараженный компьютер.
- Автоматизация повседневных работ с использованием богатых возможностей командной строки.
- Гарантированное удаление вирусов, неизвестных Dr.Web или помещенных в архивы с неизвестными форматами.
- Запуск с любого внешнего носителя (компакт-диска или USB-накопителя).

Описание: http://products.drweb.com/console

Dr.Web Mobile Security

Защита мобильных устройств

Компоненты защиты Dr.Web Mobile Security

Компоненты защиты	Android	Symbian OS	Windows Mobile	Blackberry
Антивирус	+	+	+	+
Антиспам	+	+	+	
Антивор	+			
URL-фильтр	+			
Брандмауэр	+			
Аудитор безопасности	+			+

Лицензирование Dr.Web Mobile Security

1. Продукт лицензируется по числу защищаемых мобильных устройств (1 – 5).
2. Сроки коммерческих лицензий: 12, 24 или 36 месяцев. Сроки OEM-лицензий: 3 или 6 месяцев.
3. Никаких скидок для этого продукта не предусмотрено, в том числе скидок на продление. Чтобы продолжить пользоваться продуктом после того, как истекла лицензия, или чтобы увеличить количество защищаемых устройств (произвести дозакупку), необходимо приобрести новую лицензию без скидки.

Dr.Web для Android

Функции и преимущества

- Быстрое или полное сканирование файловой системы, а также проверка сканером отдельных файлов и папок по запросу пользователя.

  Проверка файловой системы в режиме реального времени монитором SplDer Guard при попытке сохранения файлов в памяти устройства.
- Детектирование новых, неизвестных вредоносных программ с помощью уникальной технологии Origins Tracing™.

Дата актуализации 20.11.2015

- Защита SD-карты от инфицирования файлами автозапуска и Exploit.Cpllnk, представляющими опасность для Windows-устройств.
- Перемещение обнаруженных угроз в карантин с возможностью восстановления файлов оттуда.
- Минимальное влияние на скорость работы операционной системы.
- Бережное расходование ресурсов аккумулятора.
- Экономия трафика благодаря малому размеру обновлений вирусных баз, что особенно важно для пользователей лимитных тарифов мобильной связи.
- Подробная статистика о работе антивируса.

Удобные и информативные виджеты рабочего стола для доступа к приложению.

Антиспам

Оградит от нежелательных звонков и СМС-сообщений.

- Выбор режимов фильтрации звонков и сообщений.
- Возможность создания собственных профилей фильтрации.
- Редактирование черного списка (номеров, с которых вы хотите заблокировать входящие звонки и сообщения).
- Просмотр заблокированных звонков и сообщений.

Антивор

Поможет найти мобильное устройство в случае его утери или кражи и при необходимости удаленно стереть с него конфиденциальную информацию.

- Блокировка телефона после перезагрузки.
- Блокировка телефона с требованием ввести пароль разблокировки (число попыток ввода пароля ограничено).
- Разблокировка с помощью СМС.
- Получение GPS-координат устройства в виде ссылки на Google Maps.
- Возможность удаленно стереть данные в телефоне и на SD-карте.
- Включение на устройстве громкого звукового сигнала и блокировка экрана.
- Возможность задать собственный текст, который будет отображаться на экране заблокированного устройства.
- Возможность создать список номеров близких вам людей, которые будут получать уведомления о смене сим-карты на утерянном устройстве. С этих номеров можно будет управлять Антивором и в том числе разблокировать телефон, если вы забыли пароль разблокировки.

URL-фильтр Cloud Checker

Облачный фильтр Cloud Checker ограничит доступ к нежелательным интернет-ресурсам. Блокировка доступа к нерекомендуемым и потенциально опасным сайтам производится по следующим категориям:

- Наркотики.
- Известные источники вирусов.
- Нецензурная лексика.
- Терроризм.
- Насилие.
- Оружие.
- Сайты для взрослых и др.

Дата актуализации 20.11.2015

ВАЖНО!

Некоторые конкуренты Dr.Web заявляют о наличии в составе их продуктов для защиты ОС Android компонента Родительского контроля.

Создать полноценный контроль для этой операционной системы в данный момент НЕВОЗМОЖНО.

Настройки по умолчанию браузера для Android и браузера Google Chrome для Android не позволяют использовать Родительский контроль в полном смысле этого слова, т.к. любой пользователь может открыть страницу в анонимном режиме, и никакое ПО не сможет отследить его действия.

Поэтому, в отличие от конкурентов, «Доктор Веб» не позиционирует URL-фильтр Cloud Checker как Родительский контроль.

Аудитор безопасности

- Произведет диагностику, выявит проблемы безопасности и предложит решения для их устранения.

Новинка! Разблокировка от вредоносных приложений

Позволяет разблокировать устройство, инфицированное троянцами-блокировщиками. Возможности:

- завершение вредоносных процессов даже при полной блокировке телефона;
- противодействие даже тем блокировщикам, которых нет в вирусной базе Dr.Web;
- сохранность данных без необходимости выплаты выкупа злоумышленникам.

Брандмауэр

Проконтролирует сетевую активность приложений.

- Фильтрация внешнего сетевого трафика приложений, установленных на устройстве, и системных приложений – в соответствии с выбором пользователя (Wi-Fi, сотовая сеть) и настраиваемыми правилами (по IP-адресам и/или портам, целым сетям, областям адресов).
- Мониторинг как текущего трафика, так и уже переданного – с получением информации об адресах/портах, к которым подключаются приложения, и о размере входящего и исходящего трафика.
- Подробные журналы.

Брандмауэр работает на Android 4.0 и выше.

Dr.Web для Blackberry

Функциональные возможности

- Быстрое/ полное сканирование файловой системы, а также проверка сканером отдельных файлов и папок по запросу пользователя, проверка карты памяти, проверка архивов. Проверка файловой системы в режиме реального времени монитором SpIDer Guard при попытке сохранения файлов в памяти устройства и при установке программ.
- Защита SD-карты от инфицирования файлами автозапуска и Exploit.Cpllnk, представляющими опасность для Windows-устройств
- Экономия трафика благодаря малому размеру обновлений вирусных баз, что особенно важно для пользователей лимитных тарифов мобильной связи.
- Перемещение обнаруженных угроз в карантин с возможностью восстановления файлов оттуда.

Дата актуализации 20.11.2015

- Минимальное влияние на скорость работы операционной системы.
- Бережное расходование ресурсов аккумулятора.
- Подробная статистика обнаруженных угроз, работы антивируса, а также журнала регистрации событий.
- Диагностика устройства на предмет наличия в нем уязвимостей. Помощь устранении проблем безопасности и уязвимостей устройства.

«Dr.Web Универсальный» (для клиентов АСЦ)

Комплексная защита ПК и ноутбуков для клиентов Авторизованных сервисных центров Dr.Web.

Электронные лицензии продукта «Dr.Web Универсальный» поставляются только Авторизованными сервисными центрами Dr.Web.

«Dr.Web Универсальный» обеспечивает защиту 1 ПК и 1 мобильного устройства в течение 1 года.

Состав лицензии:

- Dr.Web Security Space
- Антивирус Dr.Web для OS X
- Антивирус Dr.Web для Linux
- Dr.Web Mobile Security Suite
- Dr.Web для Android OS
- Dr.Web для Symbian OS
- Dr.Web для Windows Mobile

Подробнее об Авторизованных центрах Dr.Web – http://partners.drweb.com/service

Дата актуализации 20.11.2015

Dr.Web Enterprise Security Suite. Продукты для бизнеса

НОВАЯ X ВЕРСИЯ

Dr.Web Enterprise Security Suite – это группа продуктов Dr.Web, включающая элементы защиты всех узлов корпоративной сети и единый центр управления для большинства из них.

Продукты объединены в 5 групп по типу защищаемых объектов. При наличии у клиента определенных требований это значительно облегчает поиск нужного продукта.

Продукт	Программные продукты
Dr.Web Desktop Security Suite Защита рабочих станций, клиентов терминальных серверов, клиентов виртуальных серверов и клиентов встроенных систем	Dr.Web для Windows
	Dr.Web для Linux
	Dr.Web для OS X
	Dr.Web для MS DOS*
	Dr.Web для OS/2*
Dr.Web Server Security Suite Защита файловых серверов и серверов приложений (в том числе виртуальных и терминальных)	Dr.Web для серверов Windows
	Dr.Web для серверов UNIX
	Dr.Web для серверов Novell NetWare
	Dr.Web для серверов OS X Server
Dr.Web Mail Security Suite Защита почты	Dr.Web для почтовых серверов и шлюзов UNIX
	Dr.Web для MS Exchange
	Dr.Web для IBM Lotus Domino для Windows
	Dr.Web для IBM Lotus Domino для Linux
	Dr.Web для почтовых серверов Kerio для Windows
	Dr.Web для почтовых серверов Kerio для Linux
	Dr.Web для почтовых серверов Kerio для OS X
Dr.Web Gateway Security Suite Защита шлюзов	Dr.Web для интернет-шлюзов UNIX
	Dr.Web для интернет-шлюзов Kerio
	Dr.Web для MIMEsweeper*
	Dr.Web для Qbik WinGate*
	Dr.Web для Microsoft ISA Server и Forefront TMG*
Dr.Web Mobile Security Suite Защита мобильных устройств	Dr.Web для Windows Mobile
	Dr.Web для Symbian OS*
	Dr.Web для Android

* Централизованное управление пока не реализовано.

Дата актуализации 20.11.2015

Алгоритм выбора нужного продукта

1. Что вам необходимо защитить?	2. Под управлением какой ОС/на какой платформе работают защищаемые устройства?*	3. Вам нужен только антивирус или комплексная защита?	4. Вам нужна криптографическая защита информации?	5. Сколько объектов необходимо защитить?	6. На какой срок нужна лицензия?	7. Является ли требуемая лицензия первичной покупкой, продлением, дозакупкой, дозакупкой и продлением, полагается ли клиенту льгота?
Определяем продукт	Определяем ОС/платформу	Определяем базовую лицензию	Определяем дополнительные компоненты	Определяем количество лицензий	Определяем срок лицензии	Определяем тип лицензии и возможные скидки
	■ Windows 8/7/Vista/XP/2000 SP4 + Rollup 1 (32- и 64-битные системы)	■ Комплексная защита ■ Антивирус	■ Центр управления ■ Криптограф	1....	12, 24 или 36 месяцев	
	■ OS X ■ Linux ■ MS DOS ■ OS/2	■ Антивирус	■ Центр управления			
Файловые серверы (Dr.Web Server Security Suite)	■ Windows ■ Novell NetWare ■ OS X Server ■ UNIX	■ Антивирус	■ Центр управления	1...		
Почтовый трафик (Dr.Web Mail Security Suite)	■ UNIX ■ MS Exchange ■ Lotus Domino ■ Kerio	■ Антивирус	■ Антиспам ■ SMTP Proxy ■ Центр управления	■ Неограниченное количество пользователей ■ Серверы – с числом защищаемых пользователей не более 3 000		
Интернет-трафик (Dr.Web Gateway Security Suite)	■ Интернет-шлюзы Kerio ■ Интернет-шлюзы UNIX	■ Антивирус	■ Центр управления	■ Неограниченное количество пользователей		
	■ Qbik WinGate ■ MIMEsweeper ■ Microsoft ISA Server и Forefront TMG		■ Антиспам	■ Серверы – с числом защищаемых пользователей не более 3 000		
Мобильные устройства (Dr.Web Mobile Security Suite)	■ Windows Mobile ■ Android	■ Комплексная защита	■ Центр управления	■ Неограниченное количество мобильных устройств		
	■ Symbian OS					
Теперь у вас есть все необходимые данные о лицензии для расчета ее стоимости.						

* Этот шаг важен только при выборе защиты для рабочих станций, так как от используемой ОС зависит набор доступных дополнительных компонентов (см. «Лицензирование продуктов»).

Дата актуализации 20.11.2015

Центр управления Dr.Web

Централизованное управление защитой всех узлов корпоративной сети.

Ключевые функции

Централизованное управление всеми компонентами защиты, отслеживание состояния всех защищенных узлов, настройка автоматической реакции на вирусные инциденты.

Преимущества

- Низкозатратное управление системой защиты корпоративной сети из любой точки мира с одного рабочего места (через Веб-администратор), где бы оно ни находилось, даже вне корпоративной сети.
- Минимальная совокупная стоимость по сравнению с конкурирующими программами благодаря возможности развертывания сети под Windows- и UNIX-серверами, простоте установки и надежности защиты.
- Система защиты может быть развернута практически в любой корпоративной сети, вне зависимости от ее размера и особенностей – общего количества сотрудников и филиалов, топологии, наличия или отсутствия сервера Active Directory.
- Возможность развертывания агентов на рабочих станциях удобным для администратора способом – через политики Active Directory, стартовые скрипты, механизмы удаленной установки. Установка возможна, даже если узел сети является закрытым и недоступным для антивирусного сервера.
- Возможность реализации индивидуальных для конкретного предприятия и отдельных групп сотрудников политик безопасности.
- Автоматизация работы за счет интеграции с системой Windows NAP.
- Исключительная масштабируемость для сетей любого размера и сложности. Масштабирование обеспечивается за счет возможности использования иерархии взаимодействующих антивирусных серверов Центра управления и отдельного SQL-сервера для хранения данных, а также наличия комплексной структуры взаимодействия между ними и защищаемыми узлами сети.
- Безопасная передача данных между компонентами системы за счет возможности шифрования.
- Минимальный сетевой трафик. Компрессию данных между клиентом и сервером обеспечивает специально разработанный протокол обмена информацией.
- Прозрачность работы – журнал аудита действий администраторов позволяет отслеживать все шаги по установке и настройке системы. Все ее компоненты могут вести файлы отчетов с настраиваемым уровнем детализации.
- Удобная система оповещения администратора о проблемах, возникающих в антивирусной сети.
- Возможность назначения отдельных администраторов для различных групп, что позволяет использовать Центр управления как в компаниях с повышенными требованиями к безопасности, так и в многофилиальных организациях.
- Возможности настройки политик безопасности для любых типов пользователей, включая «мобильных», и для любых станций – даже отсутствующих в данный момент в сети – позволяют обеспечить актуальность защиты в любой момент времени.
- Гарантия невозможности самостоятельного изменения пользователями настроек защиты.
- Возможность защиты сетей, не имеющих доступа в Интернет.
- Возможность использования большинства существующих баз данных, как внутренних, так и внешних. При этом в качестве последних могут выступать Oracle, PostgreSQL, Microsoft SQL Server, любая СУБД с поддержкой SQL-92 через ODBC.

Дата актуализации 20.11.2015

- Возможность самостоятельного написания обработчиков событий на любом скриптовом языке, что дает прямой доступ к внутренним интерфейсам Центра управления.
- Возможность отката обновления – даже если процесс обновления вызвал ошибку, узел сети не останется без защиты.
- Открытость – с помощью этого комплекса системный администратор может устанавливать и синхронизировать дополнительные продукты сторонних производителей, что также снижает затраты на построение систем информационной безопасности.
- Наглядность системы контроля состояния защиты, непревзойденный по эффективности и удобству поиск станций сети.
- Возможности выбора списка обновляемых компонентов продукта и контроля перехода на новые версии позволяют администраторам устанавливать только необходимые и проверенные в их сети обновления.

Сервис онлайн-тестирования **Dr.Web LiveDemo**

http://download.drweb.com/live_demo/?lng=ru

Дата актуализации 20.11.2015

Dr.Web Desktop Security Suite

Защита рабочих станций, клиентов терминальных серверов, клиентов виртуальных серверов и клиентов встроенных систем.

- Dr.Web для Windows v.6 — сертифицирован ФСТЭК России
- Dr.Web для Linux v.6 — сертифицирован ФСТЭК России
- Dr.Web для OS X
- Консольные сканеры Dr.Web для Windows, MS DOS, OS/2

Поддерживаемые ОС

Dr.Web для Windows	Dr.Web для Linux	Dr.Web для OS X	Консольные сканеры Dr.Web
Windows 2012/8/7/2008/ Vista/2003/XP SP 2 (32- и 64-битные системы)	Дистрибутивы GNU/Linux, работающие на платформе Intel x86/amd64 на основе ядра 2.6.37 (и выше) и использующие библиотеку glibc версии 2.13 (и выше)	OS X 10.7 и выше	Windows, MS DOS, OS/2

Лицензирование Dr.Web Desktop Security Suite

Виды лицензий

По числу защищаемых рабочих станций, клиентов, подключающихся к терминальному или виртуальному серверу, или клиентов встроенных систем (от 5).

Программные продукты Dr.Web Desktop Security Suite можно приобрести отдельно или в составе группы Dr.Web Enterprise Security Suite. В последнем случае дополнительно лицензируются Центр управления Dr.Web Enterprise Security Suite (кроме консольных сканеров Dr.Web) и криптограф (только для Dr.Web для Windows).

Варианты лицензий

	Windows 8/7/Vista	Windows 8/7/Vista/ XP SP2/2000 SP4 + Rollup 1	Linux	OS X	MS DOS, OS/2
Базовая лицензия	■ Антивирус ■ Комплексная защита	Антивирус			
Компоненты защиты базовой лицензии	■ Антивирус ■ Антишпион ■ Антируткит ■ Антиспам ■ Веб-антивирус ■ Офисный контроль ■ Брандмауэр	■ Антивирус ■ Антишпион ■ Антируткит ■ Брандмауэр	■ Антивирус ■ Антишпион	■ Антивирус ■ Антишпион ■ Антируткит	■ Антивирус ■ Антишпион ■ Антируткит
Дополнительные компоненты					
Центр управления	+	+	+	+	–
Криптограф	+	+	–	–	–

Также продукты Dr.Web Desktop Security Suite (кроме консольных сканеров) доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

Информация о программных продуктах Dr.Web для Windows, OS X, Linux и консольных сканерах находится в разделе Dr.Web Home Security Suite. Продукты для дома. Информация о продукте Dr.Web Security Space соответствует лицензии Комплексная защита.

Дата актуализации 20.11.2015

Dr.Web Server Security Suite

Защита файловых серверов и серверов приложений (в том числе терминальных серверов)

- Dr.Web для серверов Windows — сертифицирован ФСТЭК России
- Dr.Web для OS X Server
- Dr.Web для серверов Novell NetWare
- Dr.Web для серверов UNIX (Samba) — сертифицирован ФСТЭК России

Поддерживаемые ОС

Dr.Web для серверов Windows	Dr.Web для серверов UNIX	Dr.Web для серверов Novell NetWare	Dr.Web для OS X Server
Microsoft Windows Server 2000* / 2003 (x32 и x64*) / 2008 / 2012 (x64)	■ Linux с версией ядра 2.4.x и выше ■ FreeBSD версии 6.x и выше для платформы Intel x86 ■ Solaris версии 10 для платформы Intel x86	Novell NetWare версии 4.11–6.5	OS X Server 10.7 и выше

Программные продукты Dr.Web Server Security Suite можно приобрести отдельно или в составе группы Dr.Web Enterprise Security Suite. В последнем случае дополнительно лицензируется Центр управления Dr.Web Enterprise Security Suite.

	Dr.Web для серверов Windows	Dr.Web для серверов Novell NetWare	Dr.Web для серверов UNIX	Dr.Web для OS X Server
Базовая лицензия	Антивирус			
Дополнительные компоненты				
Центр управления	+	+	+	+

Также все продукты Dr.Web Server Security Suite доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

* Поддерживаются только для версии 7.0.

Дата актуализации 20.11.2015

Dr.Web для серверов Windows

Антивирусная защита файловых и терминальных серверов под управлением Windows, включая серверы приложений

Преимущества

- Возможность использования в организациях, требующих повышенного уровня безопасности – продукт полностью отвечает требованиям российского законодательства и обладает сертификатами соответствия ФСТЭК и ФСБ.
- Высокая производительность и стабильность работы.
- Высокая скорость сканирования при минимальной нагрузке на операционную систему, что позволяет Dr.Web идеально функционировать на серверах практически любой конфигурации.
- Бесперебойная работа антивируса в автоматическом режиме.
- Гибкое распределение нагрузки на файловую систему сервера благодаря уникальной технологии отложенной проверки файлов, открываемых «на чтение».
- Гибкая клиентоориентированная система настройки – выбор объектов проверки, действий с обнаруженными вирусами или подозрительными файлами.
- Простота установки и администрирования.
- Полноценная защита сразу после установки (с настройками по умолчанию).
- Прозрачность – подробные файлы отчета с необходимой администратору степенью детализации.

Ключевые функции

- Проверка томов сервера по заранее заданному расписанию или запросу администратора.
- Сканирования на «лету» – непосредственно при записи или открытии файлов на сервере с рабочих станций.
- Многопоточная поверка.
- Автоматическое отключение от сервера станции – источника вирусной угрозы.
- Мгновенное оповещение администратора, других пользователей и групп о вирусных инцидентах – по электронной почте либо путем отправки уведомлений на мобильный телефон или пейджер.
- Изоляция инфицированных файлов в карантине.
- Лечение, восстановление и/или удаление файлов из карантина.
- Ведение журнала действий антивируса.
- Автоматические обновления вирусных баз.
- Бережное потребление ресурсов системы и учет мощности аппаратного обеспечения.
- Dr.Web Cloud – мгновенная реакция на новейшие угрозы*.
- Превентивная защита – надежная защита от еще неизвестных угроз путем запрета модификации критических объектов Windows и контроля небезопасных действий*.

Системные требования

- Процессор: поддерживающий систему команд i686 и старше.
- Операционная система: Microsoft Windows Server 2000**/2003 (x32 и x64**)/2008/2012 (x64)

Оперативная память: 512 МБ и больше.

Описание: http://products.drweb.com/fileserver/win

* Доступно для операционных систем Windows Server 2008 и выше.
** Поддерживаются только для версии 7.0.

Дата актуализации 20.11.2015

Dr.Web для OS X Server

Антивирусная защита рабочих станций под управлением серверных версий OS X

Ключевые функции

- Проверка объектов автозапуска, сменных носителей информации, сетевых и логических дисков, почтовых форматов, файлов и каталогов, включая упакованные и находящиеся в архивах.
- Быстрое, полное и выборочное сканирование.
- Антивирусная проверка вручную, автоматически или по заранее составленному расписанию.
- Защита настроек монитора SpIDer Guard® паролем от несанкционированного изменения.
- Применение действий для зараженных, подозрительных объектов и объектов другого типа, включая лечение, перемещение в карантин и удаление, в том числе в случае если выбранное ранее действие оказалось невозможным.
- Исключение из проверки путей и файлов по запросу пользователя.
- Обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками.
- Регистрация времени события, объекта проверки и типа воздействия на него.
- Загрузка обновлений автоматически (по расписанию) или по требованию.
- Автоматическое оповещение (в том числе с помощью звуковых уведомлений) о вирусных событиях.
- Изоляция зараженных файлов в карантине с возможностью задания времени хранения объектов в карантине и его максимального размера.
- Лечение, восстановление или удаление перемещенных в карантин объектов.
- Ведение подробного отчета о работе.
- Доступность модулей в виде утилит командной строки, с возможностью их встраивания в используемые для обслуживания системы Apple Scripts.

Преимущества

- Удобный центр управления.
- Высокая скорость сканирования.
- Возможность создания собственных профилей сканирования.
- Надежная защита в режиме реального времени.
- Минимальная нагрузка на защищаемую систему.
- Малый расход трафика при обновлениях.
- Разнообразные настройки.
- Простота управления.
- Стильный и удобный интерфейс.

Системные требования

- OS X Server 10.7 или выше.
- Процессор Intel.
- Оперативная память — в соответствии с требованиями ОС.
- Доступ к сети Интернет: для регистрации и получения обновлений.

Описание: http://products.drweb.com/fileserver/mac

Дата актуализации 20.11.2015

Dr.Web для серверов Novell NetWare

Антивирусная защита файловых хранилищ

Ключевые функции

- Проверка томов сервера по расписанию или запросу администратора.
- Проверка «на лету» всех файлов, проходящих через сервер.
- Многопоточная проверка.
- Возможность регулировки степени загрузки процессора, что позволяет задавать приоритетность процесса сканирования в системе.
- Автоматическое отключение от сервера станции – источника вирусной угрозы.
- Протоколирование проверки; управление детализацией протокола.
- Уведомления об обнаружении инфицированных объектов.
- Лечение, удаление или перемещение инфицированных объектов в карантин.
- Администрирование антивируса при помощи консоли сервера или удаленной консоли.
- Ведение статистики сканирования и журнала действий антивируса.
- Автоматические обновления вирусных баз.

Преимущества

- Широчайший спектр поддерживаемых версий Novell NetWare – от 4.11 до 6.5.
- Поддержка пространства имен NetWare.
- Высокая скорость сканирования огромных массивов данных при минимальной нагрузке на операционную систему.
- Простота установки.
- Гибкая клиентоориентированная система настройки параметров проверки и действий с обнаруженными вредоносными объектами.

Системные требования

- Novell NetWare версии 4.11-6.5 с установленными дополнениями из Minimum patch list.

Описание: http://products.drweb.com/fileserver/novell

Дата актуализации 20.11.2015

Dr.Web для серверов UNIX

Антивирусная защита файловых серверов Unix

Преимущества

- Высокая производительность и стабильность работы.
- Высокая скорость сканирования при минимальной нагрузке на операционную систему, что позволяет Dr.Web идеально функционировать на серверах практически любой конфигурации.
- Гибкая клиентоориентированная система настройки – выбор объектов проверки, действий с обнаруженными вирусами или подозрительными файлами.
- Отличная совместимость – не конфликтует с известными межсетевыми экранами и файловыми мониторами.
- Поддержка систем мониторинга (Cacti, Zabbix, Munin, Nagios и т. д.).
- Удобство администрирования, простота установки и настройки.

Ключевые функции

- Проверка томов сервера по заранее заданному расписанию или запросу администратора.
- Улучшено! Сканирование на «лету» – непосредственно при записи или открытии файлов на сервере с рабочих станций.
- Многопоточная проверка.
- Автоматическое отключение от сервера станции – источника вирусной угрозы.
- Мгновенное оповещение администратора, других пользователей и групп о вирусных инцидентах – по электронной почте либо путем отправки уведомлений на мобильный телефон или пейджер.
- Улучшено! Изоляция инфицированных файлов в карантине.
- Лечение, восстановление и/или удаление файлов из карантина.
- Ведение журнала действий антивируса.
- Автоматические обновления вирусных баз.

Системные требования

- Samba 3.0 и выше.

Поддерживаемые ОС

- GNU/Linux (на основе ядра с версией не ниже 2.6.37 и использующая библиотеку glibc версии 2.13 и выше).
- FreeBSD.
- Solaris – только для платформ Intel x86/amd64.
- Используемые операционные системы должны использовать сервер Samba версии не ниже 3.0, а также механизм аутентификации PAM.
- В случае использования 64-битной версии операционной системы должна быть включена поддержка исполнения 32-битных приложений.
- Место на жестком диске:
  Не менее 1 ГБ.
- Работоспособность комплекса была протестирована на дистрибутивах:
  Debian (7.8, 8), Fedora (20, 21), Ubuntu (12.04, 14.04, 14.10, 15.04), CentOS (5.11, 6.6, 7.1), Red Hat Enterprise Linux (5.11, 6.6, 7.1), SUSE Linux Enterprise Server (11 SP3, 12), FreeBSD (9.3, 10.1), Solaris (10 u11).

Описание: http://products.drweb.com/fileserver/unix

Дата актуализации 20.11.2015

Dr.Web Mail Security Suite

Защита почты

- Dr.Web для почтовых серверов UNIX — сертифицирован ФСТЭК России
- Dr.Web для MS Exchange — сертифицирован ФСТЭК России
- Dr.Web для IBM Lotus Domino (Windows, Linux)
- Dr.Web для почтовых серверов Kerio (Windows, Linux)

Поддерживаемые ОС

Продукт Dr.Web	Windows	Linux	FreeBSD	Solaris
		для платформы Intel x86		
Dr.Web для почтовых серверов UNIX		с версией ядра 2.4.x и выше	версии 6.x и выше	версии 10
Dr.Web для MS Exchange	Server 2000 / 2003 / 2008			
Dr.Web для IBM Lotus Domino	Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 (32- и 64-битные версии)	Red Hat Enterprise Linux (RHEL) 4 и 5 версии, Novell SuSE Linux Enterprise Server (SLES) 9 и 10 версии (только 32-битные)		
Dr.Web для почтовых серверов Kerio	Server 2000 / 2003 / 2008 XP / Vista / 7	Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0 и 11.1; CentOS Linux 5.2 и 5.3; Debian 5.0; Ubuntu 8.04 LTS		

Лицензирование Dr.Web Mail Security Suite

Виды лицензий

- По числу защищаемых пользователей (от 5).
- Посерверная лицензия – для проверки неограниченного объема корреспонденции на одном сервере, с числом защищаемых пользователей не более 3 000.

Программные продукты Dr.Web для защиты почты можно приобрести отдельно или в составе комплекса Dr.Web Enterprise Security Suite. В последнем случае дополнительно лицензируются Центр управления Dr.Web Enterprise Security Suite, Антиспам и SMTP proxy.

Совместное использование продуктов для защиты почты и дополнительного компонента SMTP proxy не только существенно повышает общую безопасность сети, но и снижает нагрузку на внутренние почтовые серверы и рабочие станции.

Дата актуализации 20.11.2015

Варианты лицензий

	Dr.Web для MS Exchange	Dr.Web для IBM Lotus Domino	Dr.Web для почтовых серверов UNIX	Dr.Web для почтовых серверов Kerio
Базовая лицензия	Антивирус			
Дополнительные компоненты				
Антиспам	+	+	+	
SMTP proxy	+	+	+	+
Центр управления	+	+	+	+

Также продукты Dr.Web для защиты почты доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

Дата актуализации 20.11.2015

Dr.Web для почтовых серверов и шлюзов UNIX

Антивирусная и антиспам-защита почтового трафика, проходящего через серверы под управлением UNIX (Linux/FreeBSD/Solaris(x86))

Ключевые функции

- Фильтрация почтовых сообщений на вирусы и спам.
- Разбор почтовых сообщений и анализ всех их компонентов.
- Корректная обработка большинства известных типов архивов, в том числе многотомных и самораспаковывающихся (SFX).
- Белые и черные списки.
- Настраиваемые уведомления.
- Ведение статистики, учитывающей все аспекты работы системы.
- Защита работы собственных модулей от сбоев.

Соответствие требованиям российского законодательства

Dr.Web для почтовых серверов UNIX обладает сертификатами соответствия ФСТЭК и ФСБ. Это позволяет использовать продукт в организациях, требующих повышенного уровня безопасности, в том числе в составе подсистемы антивирусной защиты информационных систем персональных данных (ИСПДн) класса К1. Возможность архивации всех почтовых сообщений позволяет также применять продукт в составе информационных систем кредитных учреждений.

Возможность гибкой настройки под потребности пользователей

Для настройки **Dr.Web для почтовых серверов UNIX** можно применять правила. Это значительно повышает гибкость продукта и выгодно отличает его от конкурирующих аналогов, для настройки которых применяются статические параметры конфигурационного файла. Фильтрация и изменение сообщений происходят в зависимости от имеющихся политик. При этом администратор может задавать отдельные правила обработки не только для различных пользователей и групп, но и фактически для каждого письма. Благодаря этому продукт способен отвечать любым корпоративным требованиям к уровню информационной безопасности, что особенно важно в условиях вступления в силу закона о защите персональных данных.

Нетребовательность к квалификации администратора

Несмотря на богатство функциональных возможностей, **Dr.Web для почтовых серверов UNIX** не требует длительной настройки перед введением в строй. Кроме того, он поставляется не только в виде программного продукта, но и в составе программно-аппаратного комплекса Dr.Web Office Shield – сервера, спроектированного для работы по принципу «поставил и забыл».

Высокая скорость отклика

Технология многопоточной проверки обеспечивает высокую скорость отклика системы. Проверка сообщений в каждом случае производится «на лету», параллельно с обработкой ранее принятых файлов. Это позволяет конечным пользователям получать корреспонденцию практически мгновенно.

Дата актуализации 20.11.2015

Дополнительные преимущества антиспама Dr.Web:

- не требует обучения и начинает эффективно работать с момента установки – в отличие от антиспамов, построенных на использовании алгоритма Байеса (Panda, Kaspersky);
- вынесение вердикта спам/не спам не зависит от языка сообщения;
- позволяет задавать различные действия для разных категорий спама;
- использует собственные черные и белые списки, что делает невозможным компрометацию компаний через злонамеренное внесение их в списки нежелательных адресов;
- допускает рекордно малое количество ложных срабатываний;
- нуждается в обновлении не чаще одного раза в сутки – уникальные технологии распознавания нежелательной почты на основе нескольких тысяч правил избавляют от необходимости скачивать частые и громоздкие обновления.

Защита конфиденциальной информации

Продукт позволяет восстанавливать сообщения, случайно удаленные пользователями из своих почтовых ящиков, а также проводить расследования, связанные с утечкой информации. Этому способствует управление карантином как через веб-интерфейс, так и через специальную утилиту, а также возможность архивации всех проходящих сообщений.

Удобство администрирования

Возможность использования веб-интерфейса для настройки и управления продуктом позволяет с легкостью осуществлять администрирование защиты из любой точки мира.

Открытость

Dr.Web для почтовых серверов UNIX может интегрироваться в решения других производителей. Кроме того, благодаря открытому API в него можно добавить новые функциональные возможности.

Возможность подключения неограниченного количества плагинов

Dr.Web для почтовых серверов UNIX позволяет неограниченно наращивать функциональность, причем любой разработанный плагин работает сразу со всеми поддерживаемыми MTA.
Реализованные плагины:

- **Dr.Web** – плагин антивирусной проверки почты средствами антивирусного движка Dr.Web;
- **vaderetro** – плагин, фильтрующий почту на спам через собственную библиотеку Vade Retro;
- **headersfilter** – плагин, фильтрующий сообщения по заголовкам.

Поддерживаемые ОС

- Дистрибутивы Linux, имеющие версию ядра 2.4.x и выше.
- FreeBSD версии 6.x и выше (для платформы Intel x86 и amd64).
- Solaris версии 10 (для платформы Intel x86 и amd64).

Дата актуализации 20.11.2015

Dr.Web SMTP proxy

Модуль **Dr.Web SMTP proxy** – компонент продукта **Dr.Web для почтовых серверов UNIX** – может быть установлен как в демилитаризованной зоне (DMZ), так и внутри почтовой системы. Благодаря тому, что сервер проверки почтовых сообщений может быть вынесен в демилитаризованную зону, а почтовый сервер изолирован от Интернета, даже в случае взлома сервера злоумышленник не получит доступа к важной для компании информации. Решение реализует полную проверку почтовой корреспонденции по протоколам SMTP/LMTP.

Использование Dr.Web SMTP proxy:

- существенно повышает общую безопасность сети;
- дает возможность значительно улучшить качество фильтрации за счет отсутствия ограничений, накладываемых почтовыми серверами;
- снижает нагрузки на внутренние почтовые серверы и рабочие станции;
- повышает стабильность работы системы проверки почты в целом.

Преимущества

Защита от атак спамеров – с помощью **Dr.Web SMTP proxy** администратор получает возможность ограничивать параметры SMTP-сессии и тем самым определить признаки спамерской атаки.

Проверка подлинности IP-адреса – **Dr.Web SMTP proxy** позволяет организовать проверку подлинности IP-адреса и защитить компанию от спама, замаскированного под недостоверным IP-адресом отправителя.

Защита от атак хакеров – **Dr.Web SMTP proxy** позволяет эффективно противостоять как «пассивным» атакам (типа PLAIN, LOGIN и т. д.), так и активным атакам без перебора по словарю.

Защита от спам–ловушек – **Dr.Web SMTP proxy** позволяет проводить проверку получателя на спам-ловушку.

Защита от некорректно сформированных писем – **Dr.Web SMTP proxy** позволяет блокировать письма с пустыми полями отправителя, но, в то же время, корректно обрабатывать письма от почтовых клиентов, которые неверно формируют письма.

Экономия интернет–трафика – использование **Dr.Web SMTP proxy** позволяет экономить интернет–трафик и блокировать отправку вложений огромного размера сотрудниками компаний.

Ограничение Open Relays серверов – если в компании имеется производственная необходимость организовать такой сервер, с помощью **Dr.Web SMTP proxy** администратор может ограничить список доменов, на которые разрешена пересылка писем.

Описание: http://new-download.drweb.com/maild

Дата актуализации 20.11.2015

Dr.Web для MS Exchange

Антивирусная и антиспам-проверка трафика, передаваемого через почтовые серверы MS Exchange 2000/2003/2007/2010

Преимущества

- Возможность использования в организациях, требующих повышенного уровня безопасности, – продукт полностью отвечает требованиям российского законодательства и обладает сертификатами соответствия ФСТЭК и ФСБ.
- Большие возможности по установке и тонкой настройке в зависимости от потребностей компании.
- Высокая скорость сканирования при минимальной нагрузке на операционную систему, что позволяет Dr.Web идеально функционировать на серверах практически любой конфигурации.
- Наличие поддержки концепции серверных ролей и транспортных агентов для MS Exchange Server 2007/2010 – проверка писем на предмет наличия вирусов и спама может выполняться как на транспортном уровне, так и на уровне поддержки антивирусного интерфейса VSAPI. Это позволяет обеспечить оптимальный уровень защиты организации.
- Встроенный антиспам, не требующий обучения (действует с момента установки), который существенно снижает нагрузку на сервер и увеличивает производительность труда сотрудников компании.
- Возможность фильтрации по черным и белым спискам, что позволяет как исключать из проверки определенные адреса, так и увеличивать ее эффективность.
- Новая возможность для гибкого конфигурирования параметров защиты приложения через браузер в удобном для пользователя режиме при помощи веб-консоли администратора.
- Возможность фильтрации по типам файлов, что позволяет компании уменьшить объем трафика.
- Наличие механизма группирования, что позволяет задавать различные параметры для разных групп сотрудников, а следовательно – существенно сокращает введение системы антивирусной защиты в строй и упрощает сопровождение продукта.
- Гибкое конфигурирование параметров защиты приложения через браузер в удобном для пользователя режиме при помощи веб-консоли администратора.
- Высокая производительность и стабильность работы благодаря функции многопоточной проверки.
- Уникальные технологии обнаружения неизвестных (новейших) упаковщиков и вредоносных объектов.
- Полностью автоматизированный запуск приложения (при старте системы).
- Удобная система обновлений при помощи штатного планировщика Windows.
- Исчерпывающая документация на русском языке.

Ключевые функции

- Антивирусная и антиспам-проверка почтовых сообщений, в том числе вложенных файлов, «на лету».
- Антивирусный мониторинг сообщений в почтовых ящиках пользователей, а также файлов в папках общего доступа.
- Антивирусная проверка транзитного почтового потока, проходящего через сервер MS Exchange.
- Лечение инфицированных файлов.
- Группирование пользователей при помощи Active Directory.
- Поддержка концепции серверных ролей и транспортных агентов для MS Exchange Server 2007/2010.
- Сканирование с применением заданных параметров: выбор максимального размера и типов проверяемых объектов, действий (в том числе и для файлов, не поддающихся проверке), а также способов обработки инфицированных объектов.

Дата актуализации 20.11.2015

- Детектирование вредоносных объектов в многократно заархивированных файлах.
- Применение различных действий в зависимости от вида спама, включая перемещение в карантин и добавление префикса к теме письма.
- В случае необходимости – добавление произвольных текстов к отсылаемым письмам.
- Изоляция инфицированных и подозрительных файлов в карантине.
- Уведомление администратора или других пользователей о вирусных инцидентах.
- Ведение статистики работы комплекса.
- Автоматические обновления.

Системные требования

При использовании Microsoft Exchange Server 2000/2003:

- Процессор Pentium 133 МГц (рекомендуется 733 МГц).
- ОЗУ: 256 МБ (рекомендуется 512 МБ).
- Свободное дисковое пространство: 20 МБ для установки; 50 МБ для журнала событий.
- Microsoft® Windows® 2000 Server или Advanced Server с установленным SP4; Microsoft® Windows Server® 2003 (версия Standard, Enterprise или Datacenter) с установленным SP1 или выше.

При использовании Microsoft Exchange Server 2007/2010:

- Процессор Intel с архитектурой x64 и поддержкой технологии Intel 64 или AMD с поддержкой платформы AMD64.
- ОЗУ: 2 ГБ.
- Свободное дисковое пространство: 20 МБ для установки; 50 МБ для журнала событий.
- Microsoft® Windows Server® 2003 R2 x64 с установленным SP2; Microsoft® Windows Server® 2008 x64.

Описание: http://products.drweb.com/mailserver/exchange

Дата актуализации 20.11.2015

Dr.Web для IBM Lotus Domino

Антивирусная и антиспам-защита платформы IBM Lotus Domino под управлением Windows и Linux

Преимущества

Минимальная совокупная стоимость

Dr.Web для IBM Lotus Domino работает не только на отдельно стоящих серверах, но и на partitions-серверах и кластерах Lotus Domino. Копии антивирусов на разных разделах действуют в памяти компьютера автономно, используя общие базы и исполняемые файлы. В этом случае лицензировать необходимо только одну копию, что существенно снижает затраты на антивирусную защиту.

Ready for IBM Lotus software

Dr.Web для IBM Lotus Domino внесен в каталог решений IBM Lotus Business Solutions Catalog и имеет знак Ready for IBM Lotus software. Этот знак подтверждает совместимость продукта с системой Lotus Domino и свидетельствует о выполнении всех требований на соответствие IBM.

Высокая скорость сканирования

Организация системы Dr.Web для IBM Lotus Domino, особая реализация метода проверки и возможность гибко управлять этим процессом позволили добиться высокой скорости сканирования при малом потреблении системных ресурсов.

Простота установки и гибкость настроек

Предусмотрено автоматизированное и легко контролируемое развертывание Dr.Web для IBM Lotus Domino. Программа поддерживает административные скрипты и имеет подробную документацию. Удобство управления комплексом обеспечивается благодаря возможности гибкого конфигурирования через консоль администратора. Средства «тонкой» настройки алгоритмов действий антивируса по результатам проверки позволяют отсылать уведомления об обнаруженных вирусах отправителю, получателям и администраторам системы, сохранять заголовки полученных почтовых сообщений и вложения к ним и т. д.

Удобство администрирования

Механизмы группирования и управление группами значительно упрощают администрирование антивирусной защиты.

Ключевые функции

- Проверка и фильтрация почтовых сообщений и всех их компонентов на вирусы, спам и нежелательные сообщения «на лету» или по заданию администратора.
- Фильтрация почты на спам, в том числе по черным и белым спискам адресов.
- Проверка документов в заданных nsf-базах на наличие вирусов.
- Проверка объектов по требованию при помощи функции ручного запуска и остановки задач сканера.
- Разбор почтовых сообщений с выделением всех компонентов письма для последующего анализа.
- Лечение инфицированных почтовых сообщений и вложенных в них файлов.
- Детектирование вредоносных объектов в многократно заархивированных файлах.
- Использование механизма обнаружения вредоносных программ, скрытых неизвестными упаковщиками.
- Использование дополнительной технологии обнаружения неизвестных вредоносных объектов, которая увеличивает вероятность обнаружения вирусов новейших типов.
- Хранение инфицированных и подозрительных объектов в карантине (доступ к перемещенным в карантин объектам осуществляется через клиент Lotus Notes).
- Уведомления о результатах проверки при помощи шаблонов, описанных в системе, что позволяет адресатам, администраторам и другим лицам получать информацию в максимально удобном виде.
- Ведение статистики работы системы.
- Защита работы собственных модулей от сбоев.
- Автоматические обновления.

Дата актуализации 20.11.2015

Поддерживаемые ОС

Версия для Windows

- Операционная система: Windows Server 2000/2003/2008/2008R2/2012/2012 R2 (32- и 64-битные версии).
- Lotus Domino версии R6.0 и выше (32- и 64-битные версии).
- Процессор Intel Pentium 133 и выше.
- RAM 128 MB (рекомендуется 512 MB).
- Свободное дисковое пространство: 128 MB.

Версия для Linux

- Операционная система: Red Hat Enterprise Linux (RHEL) 4 и 5 версии, Novell SuSE Linux Enterprise Server (SLES) 9 и 10 версии (только 32-битные).
- Lotus Domino версии 7.x или 8.x.
- Lotus Notes 6.5 (или более поздний) для Windows.
- Процессор Intel Pentium 133 и выше.
- RAM 64 MB (рекомендуется 128 MB).
- Свободное дисковое пространство: 90 MB.

Описание: http://products.drweb.com/lotus

Dr.Web для почтовых серверов Kerio

Антивирусная проверка вложений всех почтовых сообщений, передаваемых по протоколам SMTP/POP3

Преимущества

- Прекрасная совместимость с почтовыми серверами Kerio, подтвержденная тестированиями Kerio Technologies.
- Возможность работы в режиме централизованной защиты при помощи Центра управления Dr.Web Enterprise Security Suite.
- Dr.Web – единственный на сегодняшний день российский антивирусный плагин для почтовых серверов Kerio, что особенно важно при поставке продукта государственным предприятиям.
- Локализованная поддержка пользователей, в России – на русском языке.
- Минимальное время доставки сообщений и повышенная надежность продукта за счет использования технологии многопоточной проверки.
- Щадящие системные требования и отсутствие нагрузки на локальную сеть.
- Гибкая клиентоориентированная система настройки: выбор объектов проверки и действий с обнаруженными вирусами или подозрительными файлами.
- Возможность выбора действий для файлов, не поддающихся проверке.
- Удобное управление из консоли администрирования почтового сервера Kerio.

Ключевые функции

- Проверка файловых вложений всех входящих и исходящих электронных сообщений.

Системные требования

Версия для Windows

- Место на жестком диске: не менее 350 МБ
- Операционная система: Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (32- и 64-битные версии)
- Почтовый сервер: Kerio MailServer 6.2 или выше, Kerio Connect 7.0.0 или выше.

Версия для Linux

- Место на жестком диске: не менее 290 МБ
- Операционная система: Red Hat 9.0; Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0 и 11.1; CentOS Linux 5.2 и 5.3; Debian 5.0; Ubuntu 8.04 LTS.
- Почтовый сервер: Kerio MailServer 6.2 или выше, Kerio Connect 7.0.0 или выше.

Версия для OS X

- Место на жестком диске: не менее 55 МБ
- Операционная система: OS X 10.7 и выше.
- Почтовый сервер: Kerio MailServer 6.2 или выше, Kerio Connect 7.0.0 или выше.

Описание: http://products.drweb.com/mailserver/kerio

Дата актуализации 20.11.2015

Dr.Web Gateway Security Suite

Защита почтовых и интернет–шлюзов

- Dr.Web для интернет-шлюзов UNIX — сертифицирован ФСТЭК России
- Dr.Web для интернет-шлюзов Kerio
- Dr.Web для MIMEswepper
- Dr.Web для Qbik WinGate
- Dr.Web для Microsoft ISA Server и Forefront TMG

Поддерживаемые ОС

	Windows	Linux	FreeBSD	Solaris
		для платформы Intel x86		
Dr.Web для интернет–шлюзов UNIX		с версией ядра 2.4.x и выше	версии 6.x и выше	версии 10
Dr.Web для интернет–шлюзов Kerio	2000 / XP / 2003 / 2008 / 7			
Dr.Web для MIMEsweeper	2000 Server SP4 или выше/Server 2003 или выше			
Dr.Web для Qbik WinGate	Vista / Server 2008 / Server 2003 / XP / 2000 (32- и 64-бит-ные системы)			
Dr.Web для Microsoft ISA Server и Forefront TMG	**При использовании Microsoft ISA Server:** ■ Microsoft® Windows Server® 2003 x86 с Service Pack 1 (SP1); ■ Microsoft® Windows Server® 2003 R2 x86 **При использовании Microsoft Forefront TMG:** ■ Microsoft® Windows Server® 2008 SP2 ■ Microsoft® Windows Server® 2008 R2			

Дата актуализации 20.11.2015

Лицензирование Dr.Web Gateway Security Suite

Виды лицензий

- По числу защищаемых пользователей (от 5).
- Посерверная лицензия – для проверки неограниченного объема трафика на одном сервере, с числом защищаемых пользователей не более 3 000.

Программные продукты Dr.Web для защиты шлюзов можно приобрести отдельно или в составе комплекса Dr.Web Enterprise Security Suite. В последнем случае дополнительно лицензируются Центр управления Dr.Web Enterprise Security Suite (для интернет-шлюзов Kerio и UNIX) и Антиспам (кроме интернет-шлюзов UNIX и Kerio).

Варианты лицензий

	Dr.Web для интернет-шлюзов UNIX	**Dr.Web для интернет-шлюзов Kerio**	**Dr.Web для MIME-sweeper**	**Dr.Web для Qbik WinGate**	**Dr.Web для Microsoft ISA Server и Forefront TMG**
Базовая лицензия	Антивирус				
Дополнительные компоненты					
Антиспам			+	+	+
Центр управления	+	+			

Также продукты Dr.Web для защиты шлюзов доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

Дата актуализации 20.11.2015

Dr.Web для интернет-шлюзов UNIX

Антивирусная проверка HTTP- и FTP-трафика, проходящего через корпоративный интернет-шлюз – прокси-сервер

Ключевые функции

- Антивирусная проверка FTP- и HTTP-трафика.
- Централизованное управление через Веб-администратор Центра управления Dr.Web Enterprise Security Suite.
- Фильтрация доступа по MIME-типу и размеру файлов или по названию хоста.
- Регулирование доступа к веб-ресурсам.
- Оптимизация проверки трафика за счет использования технологии Preview.
- Работа как с протоколом IPv4, так и с протоколом следующего поколения IPv6.
- Проверка и применение различных действий в зависимости от типов проверяемых файлов.
- Изоляция зараженных объектов в карантине.
- Предоставление отчетности в удобном виде.
- Обработка нескольких запросов в ходе одного соединения.
- Защита от несанкционированного доступа.
- Мониторинг и автоматическое восстановление работы системы.
- Оповещение пользователя о попытках загрузки вредоносной страницы или об обнаружении вируса.

Преимущества

- Широкие возможности по организации комплексной защиты от угроз, таящихся во входящем веб-трафике.
- Доставка только безопасного контента внутрь защищаемой сети.
- Эффективная фильтрация трафика на уровне ICAP-сервера – практически без замедления скорости доставки контента.
- Значительное снижение затрат на использование сети Интернет.
- Эффективное противодействие проникновению вредоносных программ любого типа.
- Высокая масштабируемость – способность обрабатывать гигантские массивы информации в режиме реального времени.
- Способность обрабатывать гигантские массивы информации в режиме реального времени.
- Отличная совместимость – интеграция с любым программным обеспечением, поддерживающим ICAP-протокол, со всеми известными межсетевыми экранами.
- Поддержка практически всех используемых в настоящее время операционных систем на базе UNIX.
- Нетребовательность к системным ресурсам – продукт идеально функционирует на интернет-шлюзах практически любой конфигурации.
- Гибкость и удобство администрирования – продукт позволяет реализовать те схемы защиты, которые соответствуют политике безопасности компании.

Поддерживаемые ОС

- Linux с версией ядра 2.4.x и выше.
- FreeBSD версии 6.x и выше (для платформы Intel x86).
- Solaris версии 10 (для платформы Intel x86).

Любые прокси-серверы, полноценно поддерживающие протокол ICAP, в частности:

- Squid не ниже 3.0.
- SafeSquid не ниже 3.0.

Описание: http://products.drweb.com/gateway/unix

Дата актуализации 20.11.2015

Dr.Web для интернет-шлюзов Kerio

Антивирусная проверка трафика, передаваемого по протоколам HTTP, FTP, SMTP и POP3, а также посредством веб-сервиса Kerio Clientless SSL VPN

Dr.Web для интернет-шлюзов Kerio – антивирусный плагин, который подключается к межсетевому экрану Kerio. Он инсталлируется на тот же компьютер, где установлен, Kerio, и используется последним в качестве внешнего антивирусного программного обеспечения.

Преимущества

- Детектирование вредоносных объектов, передаваемых по протоколам HTTP, FTP, SMTP и POP3, а также посредством веб-сервиса Kerio Clientless SSL VPN.
- Надежная защита доступа в Интернет как для частных пользователей, так и для компаний любого размера и рода деятельности.
- Возможность работы в режиме централизованной защиты при помощи Центра управления Dr.Web Enterprise Security Suite.
- Удобство администрирования – возможность получать сообщения обо всех вирусных инцидентах как через почтовые уведомления, так и через СМС.
- Минимальное время доставки сообщений за счет многопоточной проверки.

Ключевые функции

- Детектирование вредоносных объектов, передаваемых по протоколам HTTP, FTP, SMTP и POP3, а также посредством веб-сервиса Kerio Clientless SSL VPN.
- Детектирование инфицированных вложений в электронных письмах до их обработки почтовым сервером.
- Формирование списка проверяемых протоколов обмена данными.
- Просмотр информации о работе программы через веб-консоль.
- Сканирование с возможностью настройки параметров: выбор максимального размера, типов проверяемых объектов, способов обработки инфицированных файлов.
- Применение действий к обнаруженным угрозам согласно настройкам Kerio.
- Включение/отключение детектирования вредоносных программ (по их типам).
- Регистрация ошибок и происходящих событий в журнале регистрации событий (Event Log) и текстовом журнале.
- Рассылка почтовых уведомлений о различных событиях выбранным пользователям.
- Автоматические обновления вирусных баз.

Системные требования

Версия для Windows

- Не менее 350 МБ свободного дискового пространства.
- Операционная система Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (32- и 64-битные версии).
- Межсетевой экран Kerio WinRoute Firewall 6.2 или выше, Kerio Control 7.0.0 или выше.

Версия для Kerio Control VMware Virtual Appliance и Kerio Control Software Appliance

- Не менее 290 МБ свободного дискового пространства.
- Операционная система Kerio Control VMware Virtual Appliance или Kerio Control Software Appliance.
- Межсетевой экран Kerio Control 8.x или выше.

Описание: http://products.drweb.com/gateway/kerio

Дата актуализации 20.11.2015

Dr.Web для MIMEsweeper

Антивирусная и антиспам-защита почтового трафика, проходящего через серверы контентной фильтрации ClearSwift MIMEsweeper

Преимущества

Простота установки и настройки

Встроенные в Dr.Web для MIMEsweeper средства конфигурации – мастера создания сценариев – позволяют автоматизированно создавать наиболее современные сценарии проверки сообщений (тип 1 по классификации ClearSwift).

Совместимость с DEP

Dr.Web для MIMEsweeper поддерживает технологию предотвращения выполнения данных (Data Execution Prevention, DEP), которая позволяет дополнительно проверять память и предотвращать запуск кода. Благодаря этому пользователям не нужно менять режим работы DEP – вредоносные программы не смогут воспользоваться механизмом обработки исключений Windows.

Гибкие настройки

При обнаружении инфицированного объекта плагин пытается вылечить его или сразу удаляет, если опция лечения не выбрана. Если к почтовому сообщению прикреплено несколько файлов или архивов, плагин обезвреживает только зараженные вложения. При обнаружении вируса в теле письма контентный фильтр перемещает письмо в карантин. «Чистые» письма, файлы и архивы передаются получателю без изменений. Вредоносные письма, которые плагин Dr.Web не может нейтрализовать, помечаются и по умолчанию перемещаются в карантин.

Ключевые функции

- Проверка почтовых сообщений и их вложений, включая архивы, до их обработки почтовым сервером.
- Лечение инфицированных объектов.
- Изоляция инфицированных и подозрительных файлов в карантине.
- Фильтрация почты на спам, в том числе с использованием черных и белых списков.
- Ведение статистики работы комплекса.
- Автоматические обновления.

Системные требования

- ОС Windows 2000 Server с пакетом обновления 4 (SP4) или выше, или Windows Server 2003 или более поздняя версия.
- Почтовый контентный фильтр ClearSwift MIMEsweeper™ for SMTP 5.2 или более поздняя версия.

Описание: http://products.drweb.com/mimesweeper

Дата актуализации 20.11.2015

Dr.Web для Qbik WinGate

Антивирусная и антиспам-проверка трафика, передаваемого по протоколам HTTP/POP3/FTP прокси-сервера и SMTP-сервера Qbik WinGate

Ключевые функции

- Антивирусная и антиспам-проверка почтовых сообщений, передаваемых по протоколам SMTP и POP3, включая проверку вложенных файлов.
- Антивирусная проверка файлов и данных, передаваемых по протоколам HTTP и FTP.
- Лечение инфицированных файлов, передаваемых по протоколу HTTP.
- Журнал регистрации событий.
- Собственная панель управления и менеджер карантина.
- Автоматические обновления вирусных баз.

Преимущества

- Dr.Web для Qbik WinGate – единственный на сегодняшний день полностью русифицированный плагин для Qbik WinGate.
- Только Dr.Web для Qbik WinGate имеет как документацию, так и техническую поддержку непосредственно от производителя.
- В отличие от конкурирующих аналогов, продукт компании «Доктор Веб» имеет возможность антиспам-фильтрации. Эффективный и компактный модуль антиспама не требует обучения, позволяет задавать различные действия для каждой из трех предусмотренных программой категорий спама, а также создавать черный и белый списки электронных адресов.
- Наличие не имеющей аналогов у других производителей дополнительной технологии обнаружения неизвестных вредоносных объектов (Origins Tracing), в том числе в архивах с неизвестным форматом.

Описание: http://products.drweb.com/gateway/qbik

Dr.Web для Microsoft ISA Server и Forefront TMG

Антивирусная и антиспам-проверка трафика, передаваемого через серверы Microsoft ISA Server и Forefront TMG

Преимущества

- Проверка любых объектов за минимальное время за счет использования технологий динамического анализа потребностей иных серверных сервисов в ресурсах и мгновенное автоматическое переключение между задачами.
- Использование возможностей новейших платформ для ускорения скорости проверки.
- Возможность работы на серверах любой конфигурации – в том числе с малым количеством оперативной памяти.
- Защита как реальных, так и виртуальных серверов.
- Встроенный антиспам, не требующий обучения (действует с момента установки), обеспечивающий снижение нагрузки на сервер и увеличение производительности труда сотрудников компании.
- Блокировка доступа к различным интернет-ресурсам и возможность фильтрации по типам файлов, что позволяет компании исключить проникновение вирусов с заведомо вредоносных ресурсов и уменьшить объем трафика.
- Уникальные технологии обнаружения неизвестных (новейших) упаковщиков и вредоносных объектов.

Дата актуализации 20.11.2015

- Большие возможности по установке и тонкой настройке в зависимости от потребностей компании.
- Исчерпывающая документация на русском языке.

Ключевые функции

- Антивирусная и антиспам-проверка всего проходящего трафика, в том числе вложенных файлов.
- Возможность проверки проходящих файлов «на лету» с возможностью обнаружения вредоносных объектов в многократно заархивированных файлах.
- Лечение инфицированных файлов.
- Применение различных действий в зависимости от вида спама.
- Добавление сопроводительного текста к почтовым сообщениям, которые содержали угрозы безопасности.
- Блокирование доступа к инфицированным данным для всех пользователей локальных сетей.
- Ограничение доступа пользователей к интернет-ресурсам с помощью Офисного контроля.
- Изоляция инфицированных и подозрительных файлов в карантине.
- Уведомление администратора о вирусных инцидентах.
- Ведение статистики работы комплекса.
- Автоматические обновления.

Требования к ОС и программному обеспечению

При использовании Microsoft ISA Server:

Процессор Pentium III 733 МГц и выше.

ОЗУ: 1 ГБ и больше.

Свободное дисковое пространство: 300 МБ для установки. Дополнительный необходимый размер свободного дискового пространства требуется для временного хранения данных на этапе антивирусной проверки.

ОС: Microsoft® Windows Server® 2003 x86 с Service Pack 1 (SP1), Microsoft® Windows Server® 2003 R2 x86.

Прокси-сервер: Microsoft® ISA Server 2004, Microsoft® ISA Server 2006.

При использовании Microsoft Forefront TMG:

Процессор Pentium III 1.86 ГГц и выше.

ОЗУ: 2 ГБ и больше.

Свободное дисковое пространство: 300 МБ для установки. Дополнительный необходимый размер свободного дискового пространства требуется для временного хранения данных на этапе антивирусной проверки.

ОС: Microsoft® Windows Server® 2008 SP2, Microsoft® Windows Server® 2008 R2.

Прокси-сервер: Microsoft® Forefront® TMG 2010.

Описание: http://products.drweb.com/gateway/isa

Дата актуализации 20.11.2015

Dr.Web Mobile Security Suite

Защита мобильных устройств

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

	Dr.Web для Android	Dr.Web для Symbian OS	Dr.Web для Windows Mobile
Компоненты защиты	Комплексная защита*	Антивирус + Антиспам	Антивирус + Антиспам
Централизованное управление в составе Dr.Web Enterprise Security Suite	+	–	+
Поддерживаемые ОС	Android OS 4.0 – 5.0. Брандмауэр работает на Android 4.0 и выше	S60, Symbian 9 и выше	Windows Mobile 2003/2003 SE/5.0/6.0/6.1/6.5
Ключевые функции			
Проверка «на лету»	+	+	+
Проверка файлов, поступающих через GPRS/ Infrared/Bluetooth/Wi–Fi/USB-соединения или во время синхронизации с ПК	+	+	+
Два типа проверки: полная и выборочная	+	+	+
Возможность включения/ выключения постоянной проверки карты памяти	+	–	+
Сканирование по требованию всей файловой системы или отдельных файлов и папок	+	+	+
Проверка файлов в архивах ZIP, SIS, CAB, RAR	+	+	+
Черные и белые списки входящих телефонных звонков и СМС–сообщений	+	+	+
Удаление инфицированных файлов	+	+	+
Перемещение подозрительных файлов в карантин	+	+	+
Восстановление файлов из карантина	+	+	+

Дата актуализации 20.11.2015

Обновления через Интернет: ■ по протоколу HTTP с использованием встроенного модуля GPRS; ■ через Infrared/Bluetooth/Wi–Fi/USB-соединение; ■ путем синхронизации ПК, имеющего доступ к сети Интернет, через соединение ActiveSync	+	+	+
Детальные отчеты о сканировании системы	+	+	+
Удаленное управление мобильным устройством в случае его утери или кражи — с помощью «Антивора»			+
CloudChecker — проверка из «облака» ссылок, открываемых в браузере.	+		
Разблокировка от троянцев-вымогателей — нет аналогов у конкурентов.	+		

* В состав лицензии входят такие компоненты защиты: антивирус, антиспам, антивор, родительский контроль.

Лицензирование Dr.Web Mobile Security Suite

Dr.Web для защиты мобильных устройств лицензируется по числу защищаемых мобильных устройств.

Варианты лицензий

Dr.Web для Windows Mobile	Dr.Web для Symbian OS	Dr.Web для Android
■ Антивирус + Антиспам + Центр управления	■ Антивирус + Антиспам	■ Комплексная защита + Центр управления

Также продукты Dr.Web для мобильных устройств доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

Специальное предложение

Бесплатная лицензия на Dr.Web Mobile Security Suite предоставляется зарегистрированным пользователям Dr.Web Security Space и Антивирус Dr.Web.

Описание: http://products.drweb.com/mobile/biz

Дата актуализации 20.11.2015

Dr.Web Retail Security Suite. Продукты для розницы

Dr.Web Security Space

Антивирус Dr.Web
2 ПК/1 год

Dr.Web Бастион
2 ПК/1 год

Комплект «Малый бизнес»
5 ПК/1 сервер/1 год

Бонусы

- Лицензия на Dr.Web Mobile Security для защиты мобильных устройств под управлением Android OS, Symbian OS, Windows Mobile. Число защищаемых устройств равняется числу защищаемых ПК.
- Лицензия на лечащую утилиту **Dr.Web CureIt!**

«Dr.Web Универсальный» (для клиентов АСЦ)

Медиапакет «Dr.Web Универсальный» поставляется только Авторизованными сервисными центрами Dr.Web и доступен клиентам АСЦ по специальной цене.

Продукт обеспечивает защиту 1 ПК и 1 мобильного устройства в течение 1 года.

Состав лицензии:

- Dr.Web Security Space
- Антивирус Dr.Web для OS X
- Антивирус Dr.Web для Linux
- Dr.Web Mobile Security
- Dr.Web для Android OS
- Dr.Web для Symbian OS
- Dr.Web для Windows Mobile

Комплект поставки

- Фирменный конверт
- Лицензионный сертификат
- Диск с дистрибутивом

Бонусы

- Dr.Web Mobile Security
- Dr.Web CureIt!

Подробнее об Авторизованных центрах Dr.Web
http://partners.drweb.com/service

Памятка продавца розничных продуктов
https://st.drweb.com/static/new-www/files/booklets/pamyatka_site_a5/Pamyatka_ru.pdf

Дата актуализации 20.11.2015

Комплекты Dr.Web

В состав комплектов включены продукты Dr.Web для защиты всех типов объектов.

ВАЖНО! На комплект не распространяются никакие скидки, в том числе на продление. Чтобы продолжить пользоваться комплектом, необходимо приобрести новую лицензию за полную стоимость. Предоставляется скидка на продление при переходе с комплекта на отдельные продукты Dr.Web.

Комплект Dr.Web «Универсальный»

Доступная комплексная защита enterprise-класса для предприятий малого и среднего масштаба

Небольшие компании зачастую не имеют возможности выделить значительные средства на комплексную информационную защиту. Именно на них рассчитан комплект Dr.Web «Универсальный» – экономичное предложение для организаций с числом ПК от 5 до 50.

Комплект «Dr.Web Универсальный + Криптограф» поставляется с лицензиями на Atlansys Bastion Pro*.

Продукты	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mail Security Suite	Dr.Web Gateway Security Suite	Dr.Web Mobile Security Suite
Защищаемые объекты	Рабочие станции	Серверы	Пользователи почты	Пользователи почтовых и интернет-шлюзов	Мобильные устройства
Лицензия	Комплексная защита	Антивирус	Антивирус + Антиспам	Антивирус	Антивирус
Комплектация	От 5 до 50	1	Равняется количеству станций	Равняется количеству станций (от 25)	Равняется количеству станций

Комплекты Dr.Web: http://products.drweb.com/bundles/universal

* Разработчик Atlansys Bastion Pro – компания «Программные системы Атлансис» (www.atlansys.ru).

Комплект Dr.Web для школ

Защищаемые объекты	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mobile Security Suite
Лицензия	Комплексная защита + ЦУ	Антивирус	
Комплектация	10 – 200	1 – 8	10 – 200

Дата актуализации 20.11.2015

Утилиты

Лечащие утилиты Dr.Web предназначены для диагностики и экстренного лечения в случае необходимости. Они не обеспечивают постоянной защиты компьютера.

Dr.Web CureNet!

Централизованное лечение локальных сетей любого масштаба, в том числе с установленным антивирусом другого производителя

Потенциальные пользователи	Малые, средние, крупные и очень крупные предприятия, в локальных сетях которых установлен антивирус другого производителя.
Решаемые задачи	■ Удаленное централизованное лечение рабочих станций и серверов Windows. ■ Проверка качества антивирусной защиты другого производителя.
Особенности утилиты	■ Не требует деинсталляции антивируса другого производителя перед проверкой и лечением. ■ Не требует наличия сервера или установки дополнительного ПО. ■ Может использоваться в сетях, полностью изолированных от Интернета. ■ Мастер Dr.Web CureNet! можно запустить с любого внешнего носителя, в том числе с USB.
Описание продукта	http://curenet.drweb.com/
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) ■ Windows Server
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.
Лицензирование	Срок лицензий на Dr.Web CureNet! составляет 1, 2 или 3 года, количество проверяемых станций – от 5
Демоверсия	Без функции лечения.

Дата актуализации 20.11.2015

Dr.Web CureIt!

Экстренное лечение ПК и серверов под управлением Windows, в том числе с установленным антивирусом другого производителя

Потенциальные пользователи	Малые и средние предприятия, на компьютерах и серверах которых установлен антивирус другого производителя.
Решаемые задачи	■ Экстренное лечение рабочих станций и серверов Windows. ■ Проверка качества антивирусной защиты другого производителя.
Особенности утилиты	■ Не требует установки, не конфликтует ни с одним антивирусом, а значит, на время сканирования не требуется отключать установленный антивирус другого производителя. ■ Повышенная самозащита и усиленный режим для эффективного противодействия блокировщикам Windows. ■ Обновления один или несколько раз в час. ■ Утилиту можно запустить с любого внешнего носителя, в том числе с USB.
Описание продукта	http://free.drweb.com/cureit
Поддерживаемые ОС	MS Windows 8/7/Vista/2012/2008 (32- и 64-битные системы), XP/2003 (32-битные системы)
Лицензирование	Утилита лицензируется по количеству станций, на 1, 2 и 3 года использования.
Особенности лицензирования	Утилита бесплатна для лечения собственного домашнего ПК.
Демоверсия	Отсутствует.

Дата актуализации 20.11.2015

Программно-аппаратные комплексы Dr.Web Office Shield

Высокопроизводительные и отказоустойчивые серверы для комплексной централизованной защиты рабочих станций и файловых серверов Windows, а также почтового и интернет-трафика.

Преимущества

- Экономичная защита корпоративной сети решением enterprise-класса.
- Возможность использования решения в условиях отсутствия высококвалифицированных специалистов («поставил и забыл»).
- Снижение потерь рабочего времени, простоев оборудования и персонала благодаря уменьшению количества вирусных инцидентов и высокой устойчивости устройства к внешним атакам.
- Существенное сокращение расходов на интернет-трафик и возможность контроля деятельности сотрудников в сети Интернет.
- Экономия рабочего времени системного администратора за счет простоты управления.

Dr.Web Office Shield можно использовать 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 Интернета), предназначенного для обеспечения защиты почтового и интернет-трафика от вирусов, различных вредоносных объектов и спама. Использование Dr.Web Office Shield в качестве шлюза значительно снижает затраты компаний на безопасность доступа к сети и позволяет существенно экономить интернет-трафик;
- внутреннего сервера локальной сети, обеспечивающего централизованную защиту рабочих станций и файловых серверов Windows.

Dr.Web Office Shield можно установить в действующую сеть или использовать в качестве основы для создания новой сети – это важная особенность программно-аппаратного комплекса. Наличие сервисов DHCP и DNS позволит провести эту работу с минимальными усилиями.

В состав Dr.Web Office Shield входят:

- Dr.Web Enterprise Suite;
- Dr.Web для интернет-шлюзов UNIX;
- Dr.Web Mail Gateway;
- Корпоративный межсетевой экран;
- VPN-сервер;
- Сервер DHCP&DNS;
- Точка доступа Wi-Fi.

Дата актуализации 20.11.2015

Виды поставки

NEO

Защищаемые объекты

- почтовый трафик;
- интернет-трафик.

Рекомендуемое количество пользователей: от 10 до 150.

Защищаемые объекты

- рабочие станции Windows;
- файловые серверы Windows;
- почтовый трафик;
- интернет-трафик.

Рекомендуемое количество пользователей: от 10 до 50.

TWISTER

Защищаемые объекты

- рабочие станции Windows;
- файловые серверы Windows;
- почтовый трафик;
- интернет-трафик.

Рекомендуемое количество пользователей: от 50 до 250.

Защищаемые объекты

- почтовый трафик;
- интернет-трафик.

Рекомендуемое количество пользователей: от 50 до 250.

Лицензирование

- Безлимитная лицензия.
- Лицензия по количеству защищаемых объектов: рабочих станций, пользователей почты и шлюзов.
- Применяются все действующие на момент покупки скидки, предусмотренные для продуктов Dr.Web (кроме случая с безлимитной лицензией).

Условия лицензирования безлимитной лицензии

Корпус NEO	Корпус TWISTER
■ Центр управления ■ Dr.Web Desktop Security Suite, Комплексная защита (50 ПК) ■ Dr.Web Server Security Suite (5 серверов) ■ Dr.Web Mail Security Suite, Антивирус+Антиспам + SMTP proxy(50 пользователей) ■ Dr.Web Gateway Security Suite, Антивирус (50 пользователей)	■ Центр управления ■ Dr.Web Desktop Security Suite, Комплексная защита (250 ПК) ■ Dr.Web Server Security Suite (25 серверов) ■ Dr.Web Mail Security Suite, Антивирус+Антиспам + SMTP proxy (250 пользователей) ■ Dr.Web Gateway Security Suite, Антивирус (250 пользователей)

Дата актуализации 20.11.2015

- Лицензия является условно безлимитной, так как ее параметры ограничены параметрами аппаратной части устройств.
- Лицензия предназначена только для новых покупателей.
- Лицензия поставляется только при условии одновременной покупки корпуса устройства.
- На стоимость этой лицензии не распространяются скидки на продление, скидки для образовательных и медицинских учреждений.
- Безлимитная лицензия предоставляется только на 1 год.
- Продление безлимитной лицензий производится по количеству необходимых клиенту защищаемых объектов.
- Дозакупка к безлимитной лицензии не производится.

Обучающий курс **DWCERT-010-1 Dr.Web Office Shield**
https://pa.drweb.com/training/courses/sales

Dr.Web LiveDemo

Сервис удаленного онлайн-тестирования **Dr.Web LiveDemo** позволяет еще до приобретения программно-аппаратного комплекса испытать выбранную конфигурацию в виртуальной локальной сети на сервере компании «Доктор Веб».

Сервис онлайн-тестирования **Dr.Web LiveDemo**
http://download.drweb.com/live_demo/?lng=ru

Дата актуализации 20.11.2015

Решения

Dr.Web Security Suite для UNIX Appliance

Модульная группа решений, предназначенных для интеграции с программно-аппаратными комплексами, построенными на базе операционных систем UNIX (Linux/FreeBSD/Solaris(x86)).

Решения выполняют функции корпоративного интернет-шлюза – прокси-сервера, используемого для организации доступа пользователей внутренней интранет-сети к ресурсам сети Интернет.

	Dr.Web Mail Security Suite для UNIX Appliance	Dr.Web Gateway Security Suite для UNIX Appliance
Ключевая функция	Фильтрация почтовых сообщений от вирусов и спама	Фильтрация HTTP- и FTP-трафика от вирусов
Варианты лицензий	Антивирус Антивирус + Антиспам	Антивирус

Виды лицензий

- По числу защищаемых пользователей (оно неограниченно).
- Посерверная лицензия – для проверки неограниченного объема корреспонденции/трафика на одном сервере, с числом защищаемых пользователей не более 3 000.

Лицензирование SDK

SDK распространяется бесплатно в составе продукта. Сторонние разработчики могут свободно разрабатывать и распространять плагины на основе SDK на некоммерческих условиях. Для коммерческого распространения необходимо пройти процесс сертификации.

Dr.Web ATM Shield

Централизованная антивирусная защита встроенных систем (банкоматов, терминалов, мультикиосков).

Потенциальные пользователи: банки (банкоматы), торговые сети (кассовые терминалы, мультикиоски), а также компании и организации, управляющие производственными процессами (заправочные станции, заводы и т. д.).

Описание: http://solutions.drweb.com/atm_shield

Преимущества

- Легкая интеграция в сети банкоматов и кассовых устройств и, как следствие, существенное сокращение времени на их обслуживание;
- возможность работы на компьютерах на основе слабой аппаратной платформы (512 МБ), работающих в течение длительного времени без возможности перезагрузок – в режиме 24/7;
- централизованное управление всеми компонентами антивирусной защиты встроенных систем;
- наличие в составе решения компонентов, позволяющих обеспечить защиту как от неизвестных вредоносных программ, еще не поступивших на анализ в антивирусную лабораторию, так и от несанкционированных действий обсуживающего персонала;
- легкая масштабируемость, обеспечивающая возможность использования в сетях с неограниченным числом узлов (за счет иерархической структуры антивирусной сети);
- работа в сетях, основанных на стеке TCP/IP, IPX, NetBIOS;

Дата актуализации 20.11.2015

- возможность выбора типа СУБД сервера защиты;
- минимальный сетевой трафик, основанный на специально разработанном протоколе обмена информацией, поддерживающем компрессию данных между клиентом и сервером;
- возможность шифрования данных при обмене между различными компонентами системы;
- мониторинг состояния всех защищенных узлов сети;
- централизованный сбор статистики о вирусных инцидентах;
- резервное копирование критических данных сервера защиты сети;
- прозрачность работы — журнал аудита действий администраторов позволяет отслеживать все действия по установке и настройке системы.

Внимание! В связи с тем, что применение антивирусных средств защиты во встроенных устройствах имеет ряд особенностей, настоятельно рекомендуйте клиентам перед использованием Dr.Web ATM Shield изучить руководство администратора (доступно в Мастере скачиваний после запроса демо) и пройти учебный курс по данному продукту.

Лицензирование

- По числу защищаемых встроенных устройств.
- Центр управления Dr.Web ATM Shield лицензируется бесплатно.

Демо

Для получения тестовой лицензии необходимо заполнить анкету на http://download.drweb.com/demoreq/atm_shield, указав количество защищаемых устройств, а также (желательно) используемую операционную систему.

Внимание! Если во встраиваемых устройствах клиента используются ОС типа Embedded (MS Windows Embedded 7, MS Windows Embedded 8 и т. д.), его необходимо предупредить о том, что такие ОС не являются полным аналогом обычных операционных систем — они собираются под каждый тип встраиваемого устройства, поэтому в них могут отсутствовать те или иные компоненты, потенциально необходимые для реализации антивирусной защиты. В связи с этим может потребоваться тестирование защищаемого устройства (в виде образа) отделом разработки или отделом развития компании «Доктор Веб», по итогам которого (в случае отсутствия таких компонентов) могут быть выработаны рекомендации по их доустановке.

Инструменты маркетинга для партнеров
https://pa.drweb.com/products/atm_shield

Дата актуализации 20.11.2015

Сервисы

Software as a service (SaaS) – широко распространенная за пределами России модель предоставления программного обеспечения в качестве услуги.

В российской антивирусной отрасли до 2007 года эта модель не использовалось. Это было связано с банальным отсутствием отечественных решений подобного класса. Все изменилось в мае 2007 года, когда российская компания «Доктор Веб» выпустила собственный интернет-сервис Dr.Web AV-Desk. На рынке ИТ-услуг России появился новый сегмент – сегмент услуг антивирусной защиты. Первой среди них стала услуга «Антивирус Dr.Web».

Интернет-сервис Dr.Web AV-Desk

Что такое Dr.Web AV–Desk?	Dr.Web AV-Desk – это интернет–сервис для предоставления комплекса онлайн-услуг по информационной защите ПК и серверов неограниченному числу клиентов – домашних и бизнес-пользователей. Dr.Web AV-Desk – это программное обеспечение, позволяющее централизованно управлять процессом предоставления услуги «Антивирус Dr.Web». Dr.Web AV-Desk – это VAD–модель бизнеса, с помощью которой можно привлечь новых клиентов и увеличить доходы.
Для кого предназначен сервис Dr.Web AV–Desk?	Для интернет-провайдеров и любых других компаний, работающих в сфере информационных технологий.
Для кого предназначена услуга «Антивирус Dr.Web»?	Для физических и юридических лиц – клиентов поставщиков услуги.
Какие услуги может оказывать провайдер, используя Dr.Web AV–Desk?	Услуги по информационной защите ПК клиентов от вирусов, спама и разного рода вредоносных программ. Они предоставляются в виде подписки на любой удобный для пользователя срок. За право использования защитных функций программного обеспечения (ПО) Dr.Web взимается абонентская плата.

Дата актуализации 20.11.2015

Функционал ПО Dr.Web AV–Desk	Программный комплекс для централизованного управления процессом предоставления услуг по информационной защите ПК клиентов поставщиков услуги.
Лицензирование Dr.Web AV–Desk	Сервис Dr.Web AV-Desk предоставляется поставщику услуги бесплатно. В свою очередь, услуга «Антивирус Dr.Web» лицензируется по количеству подписчиков, подключенных к сервису в отчетный период (месяц), с неистекшим сроком действия услуги.

Как это работает?

Поставщик услуги	**Клиенты услуги**
■ Организует подписку на услугу «Антивирус Dr.Web» через Центр управления подпиской. ■ Обеспечивает клиентов услуги актуальными обновлениями вирусных баз и программных модулей Dr.Web. ■ Оказывает техническую поддержку (опционально). ■ Отслеживает состояние антивирусной сети и собирает статистическую информацию о вирусных заражениях. ■ Предоставляет дополнительные услуги. ■ Взимает с клиентов плату за пользование услугой.	■ Оформляют подписку в Центре управления подпиской. ■ Производят установку ПО Dr.Web. ■ Самостоятельно управляют параметрами подписки. ■ Вносят абонентскую плату поставщику услуги.

Dr.Web AV-Desk – это мультивариантная модель бизнеса. Поставщиками услуги «Антивирус Dr.Web» могут стать интернет-провайдеры или любые другие компании, работающие в сфере информационных технологий.

	Реселлер услуги «Антивирус Dr.Web»	**Провайдер услуги «Антивирус Dr.Web»**	**Сервис-агрегатор Dr.Web AV-Desk**
Основной бизнес	Компания реализует подписку на услугу «Антивирус Dr.Web» конечным пользователям через интегрированный в свой сайт Центр управления подпиской.	Компания внедряет сервис Dr.Web AV-Desk и оказывает услугу «Антивирус Dr.Web» конечным пользователям.	Компания является владельцем серверных мощностей, на которых внедряет сервис Dr.Web AV-Desk, формирует собственную сеть реселлеров услуги и сублицензирует им Центры управления подпиской без права реализации услуги конечным пользователям.

Более подробная информация о Dr.Web AV-Desk и услуге «Антивирус Dr.Web» предоставляется партнерам по запросу.

Новый экзамен по курсу DWCERT-004 Dr.Web AV-Desk v.6
https://pa.drweb.com/training/engineers

Новый экзамен по курсу DWCERT-010-3 Услуга «Антивирус Dr.Web»
https://pa.drweb.com/training/courses/sales

Дата актуализации 20.11.2015

Скидочная политика

Скидочные коэффициенты применяются к цене лицензии на 1 год (согласно прайс-листу).

Если пользователь имеет право на несколько видов скидок, то они не суммируются, а предоставляется наибольшая из них (за исключением скидок для интернет-провайдеров).

Действие скидок распространяется только на прайсовые решения. Распространение действия скидок на запрайсовые решения необходимо согласовывать с менеджерами ООО «Доктор Веб».

Скидки за количество лицензируемых продуктов Dr.Web Enterprise Security Suite

Скидки за количество лицензируемых продуктов (типов лицензируемых объектов начисляются от суммы цен базовых лицензий и цен лицензий на дополнительные компоненты – отдельно для каждого продукта. Эти скидки применяются в калькуляторе автоматически.

Количество лицензируемых продуктов	Скидка
4	30%
3	25%
2	20%

Исключение: скидки не применяются для продукта Dr.Web Mobile Security Suite.

Ограничения

Скидки не применяются, если:

- количество серверов составляет менее 10% от количества станций, пользователей почты или шлюзов;
- количество пользователей почты или шлюзов меньше количества станций;
- количество пользователей шлюзов меньше количества пользователей почты и наоборот.

Таблица скидок

Тип клиента	Основание для скидки	Новая лицензия			Продление			Миграция*		
		1 год	2 года	3 года	1 год	2 года	3 года	1 год	2 года	3 года
Нельготные категории	Для скидки на продление – ключевой файл или серийный номер Dr.Web сроком не менее 3 месяцев на аналогичный продукт Dr.Web.	–	1,6	2,17	0,6	1,17	1,72	0,5	1	1,5
	Для скидки на миграцию – оригинал лицензии / ключевой файл / письмо-подтверждение о покупке электронной версии антивируса другого производителя.									
Учебные заведения, библиотеки, музеи и учреждения здравоохранения	Копия лицензии об образовательной деятельности / свидетельства о регистрации / лицензии Минздравсоцразвития РФ и заполненная анкета.	0,5	0,85	1,2	0,35	0,7	1,05			

Дата актуализации 20.11.2015

Условия продления

1. Продлить со скидкой можно как действующую, так и истекшую лицензию. Срока давности для продления лицензий Dr.Web не существует.
2. Продлить со скидкой можно лицензию на аналогичный продукт или решение Dr.Web. Срок действия такой лицензии должен составлять не менее 3 месяцев.
3. Скидка на продление предоставляется при условии приобретения лицензии на 1, 2 или 3 года на аналогичный продукт или решение Dr.Web.
4. Лицензия продления со скидкой предоставляется на число защищаемых объектов, не превышающее число защищаемых объектов, указанное в прежней (продлеваемой) лицензии.
5. Основанием для получения скидки на продление является ключевой файл или серийный номер Dr.Web, которые могут быть продлены только один раз.
6. Для получения скидки на продление пользователь должен предоставить продавцу серийный номер или ключевой файл (в том числе OEM).

«Переходи на зеленый!»

Программа льготной миграции на Dr.Web для пользователей антивирусов других производителей.

1. Данное специальное предложение распространяется только на продукты Dr.Web. Комплекты, утилиты, программно-аппаратные комплексы, сервисы и решения не участвуют в программе льготной миграции.
2. Скидка не предоставляется частным лицам. Ее могут получить только организации и компании и только один раз.
3. Скидка при переходе не предоставляется пользователям OEM-лицензий.
4. При переходе на годовую лицензию Dr.Web предоставляется скидка 50%. При переходе на двух- и трехгодичные лицензии для расчета стоимости применяется коэффициент 1 или 1,5 соответственно, который умножается на цену годовой лицензии Dr.Web.
5. Скидка при переходе с другого антивируса предоставляется только на аналогичный продукт семейства Dr.Web (по типу и числу защищаемых объектов).
6. Для получения скидки на переход пользователь должен предоставить оригинал лицензии, ключевой файл или письмо-подтверждение о покупке электронной версии антивируса другого производителя с регистрационной информацией.
7. Скидка предоставляется пользователям как действующих, так и истекших лицензий при условии, что с момента окончания срока действия лицензии до обращения к партнеру ООО «Доктор Веб» прошло не более 30 дней.
8. Если срок лицензии на антивирус другого производителя на момент оплаты лицензии перехода не истек, оставшееся время бесплатно добавляется к сроку новой лицензии.
9. Дальнейшее продление лицензий перехода производится с обычной скидкой на продление.
10. Скидки миграции не суммируются ни с какими другими скидками.

Дата актуализации 20.11.2015

Общие условия продаж

1. Партнеры обязаны продавать программы Dr.Web конечным пользователям строго в соответствии с комплектацией и согласно рекомендованным ценам, зафиксированным в прайс-листе.
2. Для всех продуктов Dr.Web стандартной комплектации в ценах прайс-листа стоимость обновлений программных модулей и вирусных баз, а также базовая техническая поддержка через веб-форму на странице http://support.drweb.com, включены в стоимость лицензии, отраженную в прайс-листе, на весь срок ее действия.
3. При заказе лицензий в фирменной коробке цена увеличивается на стоимость медиа-комплекта (кроме вкладки «Коробки –медиа–комплекты»).
4. Если покупателю требуется решение для защиты большего количества объектов, чем указано в прайс-листе, партнер обязан запросить у ООО «Доктор Веб» рекомендованные цены и предоставить через веб-форму по адресу https://pa.drweb.com/support/price1 следующие данные о покупателе:
   - название организации;
   - ее адрес;
   - e-mail;
   - телефон сотрудника технической службы клиента, ответственного за антивирусную защиту;
   - контактные данные службы технической поддержки партнера.

Все виды скидок при покупке таких решений предоставляются конечному пользователю только после получения рекомендаций от ООО «Доктор Веб».

5. Рекомендованные цены на решения, не указанные в прайс–листе, определяются лицензионным договором, который заключается ООО «Доктор Веб» непосредственно с поставщиком таких решений конечному пользователю.

Дата актуализации 20.11.2015

Дозакупка для Dr.Web Enterprise Security Suite

Общие правила

1. Дозакупка (или расширение) лицензии в течение срока ее действия может быть:
   - **качественной** – если к действующей лицензии добавляются новые компоненты защиты, а состав продуктов лицензии остается неизменным;
   - **количественной** – если производится увеличение количества защищаемых объектов в рамках продуктов текущей лицензии;
   - **продуктовой** – если к действующей лицензии добавляются новые продукты.

Также дозакупка может состоять из комбинации описанных выше типов.

2. Минимальный срок лицензии при дозакупке – 3 месяца, максимальный – 33 месяца.
3. Оставшееся время действия лицензии рассчитывается исходя из числа месяцев, оставшихся до истечения срока ранее приобретенной лицензии (при этом неполный месяц округляется до 1 месяца).
4. Дозакупка возможна только для лицензий с неистекшим сроком действия, до конца которого осталось не менее 3 месяцев, – в противном случае применяется дозакупка с продлением.
5. Тип лицензии в коде новой лицензии – C (дозакупка).
6. Активация лицензии дозакупки производится автоматически в момент ее генерации.
7. Предыдущая лицензия блокируется через сутки после регистрации лицензии дозакупки, и продлить ее невозможно. Для продления клиент должен предъявить дозакупленную лицензию.

Дозакупка с продлением

1. Дозакупка с продлением возможна как для еще действующих лицензий, так и для лицензий с уже истекшим сроком действия.
2. При дозакупке и продлении еще не истекшей лицензии сроки прежней (неистекшей) и новой лицензии (дозакупки с продлением) суммируются.
3. Тип лицензии в коде новой лицензии – D (дозакупка+продление).
4. Активация лицензии дозакупки производится автоматически в момент ее генерации.
5. Предыдущая (продлеваемая) лицензия блокируется через сутки после регистрации новой лицензии (дозакупки с продлением), и продлить ее невозможно. Для продления клиент должен предъявить дозакупленную лицензию.
6. При одновременном продлении и дозакупке стоимость ДОЗАКУПАЕМЫХ лицензий рассчитывается исходя из цены диапазона суммарного количества приобретаемых лицензий (продлеваемых + дозакупаемых). Стоимость ПРОДЛЕВАЕМЫХ лицензий рассчитывается исходя из цены диапазона суммарного количества ПРОДЛЕВАЕМЫХ лицензий.

Правила расчета стоимости дозакупаемых лицензий

I. Качественная дозакупка (добавление дополнительных компонентов к лицензии с сохранением количества защищаемых объектов и состава продуктов).

1. Если требуется расширение с Антивируса до Комплексной защиты для продукта Dr.Web Desktop Security Suite, применяется наценка 20% от стоимости лицензии на Антивирус, разделенная пропорционально на количество месяцев, оставшихся до конца срока действия лицензии.

Пример

Новая лицензия на Антивирус на 90 ПК стоила клиенту 52 123 руб. Спустя 2 месяца после начала ее действия клиент захотел перейти на Комплексную защиту.

52 123 руб.ч12 мес. × 0,2 (наценка 20%) × 10 мес. = 8 687, 16 руб. (доплата за переход на Комплексную защиту).

Итоговая стоимость лицензии для клиента – **60 810 руб.**

Дата актуализации 20.11.2015

2. Если требуется дозакупка **Криптографа** к Антивирусу или Комплексной защите для продукта Dr.Web Desktop Security Suite, применяется наценка 20% от стоимости ранее купленной лицензии, разделенная пропорционально на количество месяцев, оставшихся до конца срока действия лицензии.
3. Если требуется дозакупка **Антиспама** для продуктов Dr.Web Mail Security Suite или Dr.Web Gateway Security Suite, применяется наценка 40% от суммы, уплаченной за лицензию на Антивирус или Антивирус + SMTP proxy.

Пример

Клиент приобрел лицензию на Антивирус для защиты 90 пользователей почты за 41 616 руб. и спустя 2 месяца захотел дозакупить Антиспам.

41 616 руб. ч 12 мес. × 0,4 × 10 мес. = 13 872 руб. (доплата за дозакупку Антиспама).
Итоговая стоимость лицензии для клиента — **55 488 руб.**

4. Если требуется дозакупка **SMTP proxy**, применяется наценка 20% от стоимости лицензии на Антивирус или Антивирус + Антиспам.

Сводная таблица наценок при качественной дозакупке без увеличения количества защищаемых объектов

Продукт	Текущая лицензия	Новая лицензия	Наценка
Dr.Web Desktop Security Suite	Антивирус	Комплексная защита	20%
	Антивирус	+ Криптограф	
	Комплексная защита		
Dr.Web Mail Security Suite или Dr.Web Gateway Security Suite	Антивирус	+ Антиспам	40%
	Антивирус + SMTP proxy		
	Антивирус	+ SMTP proxy	20%
	Антивирус + Антиспам		

II. Количественная дозакупка (с увеличением количества защищаемых объектов)

Стоимость дозакупаемых лицензий рассчитывается по текущему прайс-листу из диапазона суммарного количества защищаемых объектов **без какой-либо скидки**.

III. Продуктовая дозакупка (расширение состава продуктов)

Стоимость дозакупаемых лицензий рассчитывается по текущему прайс-листу **без скидки за количество продуктов**.

Продукты для бизнеса, для которых дозакупка невозможна

- Коробочный продукт Dr.Web «Малый бизнес».
- Комплекты «Dr.Web Универсальный» и Dr.Web для школ.

Чтобы расширить лицензию на эти продукты, применяется переход на Dr.Web Enterprise Security Suite по правилам дозакупки с продлением.

Дата актуализации 20.11.2015

QRутой Dr.Web

Бесконтактный сервис продаж лицензий через СМС.

Чтобы купить лицензию через этот сервис, покупателю необходимо иметь мобильный телефон и достаточную сумму для покупки лицензии на счету у мобильного оператора. Через этот сервис продаются лицензии на Dr.Web Mobile Security и Dr.Web Универсальный.

Чтобы инициировать обработку заказа на лицензию, покупателю необходимо либо отсканировать QR-код, либо отправить СМС с нужным текстом на короткий номер 1121. В процессе покупки покупателю нужно отправить два СМС-сообщения. Комиссия за их отправку оплачивается покупателем. Сумма комиссии зависит от оператора покупателя и продукта Dr.Web.

Чтобы организовать продажи через этот сервис, необходимо разместить QR-коды — на веб-сайтах, плакатах, билбордах и POS-материалах (например, беджиках продавцов). Важное условие безопасности продаж в торговых точках — место с QR-кодом не должно быть доступно мошенникам для переклейки кода.

Для партнеров «Доктор Веб» разработан специальный сервис генерации QR-кодов с ID карточки партнера — это позволяет получать комиссию за каждую проданную лицензию.

Преимущества сервиса QRутой Dr.Web для партнеров

- готовая модель продаж без дополнительных затрат на внедрение;
- полное отсутствие издержек на логистику лицензий, складское хранение, поддержку ассортимента и место товара на полках;
- гарантированная комиссия не только за каждую новую продажу, но и за каждое продление такой лицензии;
- защита продлений проданных через сервис лицензий — партнер автоматически назначается реальным поставщиком в лидах (клиент закрепляется за партнером), создаваемых после активации каждой проданной лицензии, и впоследствии может работать с клиентом по продлению;
- онлайн-статистика продаж;
- продажа лицензий через сайт партнера без платежных инструментов.

Дата актуализации 20.11.2015

Коды продуктов, комплектов, утилит и программно-аппаратных комплексов Dr.Web

Правила формирования кодов

1. Код всегда состоит из 5 групп.
2. Каждая группа кода отделена от другой группы дефисом.
3. Код лицензии для категории «Продукты» формируется для каждого коммерческого продукта Dr.Web отдельно (см. раздел «Продуктовая линейка Dr.Web Security Suite»).
4. Коды программно-аппаратных комплексов Dr.Web Office Shield состоят из двух кодов:
   - кода аппаратного устройства,
   - кода лицензии.
5. Коды коробочных продуктов, скретч-карт и медиапакетов, а также коды аппаратной части ПАК Dr.Web Office Shield смотрите в прайс-листе — они фиксированные.
6. В коде лицензии «дозакупка» указываются 2 срока: общий срок дозакупаемой лицензии и – через двоеточие – оставшийся срок действия приложенного (действующего) ключа.
7. В коде лицензии «дозакупка + продление» указываются 2 срока: общий срок дозакупаемой и продлеваемой лицензии и – через двоеточие – оставшийся срок действия приложенного (продлеваемого) ключа.
8. В коде лицензии «дозакупка» указываются 2 количества защищаемых объектов: общее количество лицензий с учетом дозакупки и – через двоеточие – количество объектов действующей (приложенной лицензии).
9. В коде лицензии «дозакупка+продление» указываются 2 количества защищаемых объектов: общее количество лицензий с учетом дозакупки и продления и – через двоеточие – количество объектов действующей (продлеваемой лицензии).

Дата актуализации 20.11.2015

Сводная таблица символов кодов

1 группа			2 группа		3 группа	4 группа	5 группа	
Комплектация	**Продуктовая категория**	**Защищаемые объекты**	**Базовая лицензия**	**Дополнительные компоненты**	**Срок лицензии**	**Количество защищаемых объектов**	**Тип лицензии**	**Льгота**
L – экземпляр программы (продукт), загружаемый с веб-сайта	**B** – продукт для бизнеса **H** – продукт для дома	**G** – пользователи шлюза	**A** – Антивирус	**A** – Антиспам	**XXM** – где XX – число месяцев	Любое число	**A** – новая лицензия	**1 —** учебное заведение, учреждение здравоохранения, библиотека, музей
B – экземпляр программы в картонной коробке **A** – экземпляр программы в акционной упаковке	**X** – экземпляр программы, поставляемый в составе Dr.Web Office Shield	**M** – мобильные устройства	**B** – Комплексная защита	**C** – Центр управления	**XXXD** – где XXX –число дней	**UL** – unlimited (для безлимитной лицензии)	**B** – продление **C** – дозакупка	**2 — акция** **3 —** нет льготы
C – карточка со скретч-полосой	**Y** – утилита	**P** – пользователи почты	**K** – Katana	**K** – нет дополнительных компонентов			**D** – продление с дозакупкой	**4 —** миграция
D – экземпляр программы в DVD-упаковке	**Z** – комплект	**S** – серверы	* – лицензии для нескольких продуктов (применяется только для Комплектов)	**R** – Криптограф			**R** – Rescue Pack	**5 —** NFR лицензия для партнера
K – экземпляр программы в лицензионном пакете		**W** – рабочие станции		**S** – SMTP proxy			**F** – OEM-лицензия	**6 —** NFR-лицензия (демо) для клиента
M – экземпляр программы на фирменном диске (в том числе, OEM)		**Z** – все объекты					**G** – сервисная лицензия	**7 —** нужды маркетинга/обучения
N – экземпляр программы в сертифицированном медиапакете							**H** – без техподдержки	**8 —** благотворительность
P – экземпляр программы в медиапакете для OEM-лицензий							**V** – важный клиент	**9 —** разбивка одного ключа
Q – продажи через CMC								**10 —** объединение нескольких ключей
								11 — замена ключа

Дата актуализации 20.11.2015

Примеры

Примеры кодов лицензий для категории «Продукты»

1.	Заказчику – учебному заведению необходима защита 200 ПК с Центром управления, Комплексная защита + Брандмауэр, на 12 месяцев, электронная лицензия. Dr.Web приобретается впервые.	**LBW-BRC-12M-200-A1**
2.	У заказчика – учебного заведения имеется действующая лицензия для защиты 200 ПК с Центром управления, Комплексная защита + Брандмауэр , на 12 месяцев, электронная лицензия, до окончания действия которой осталось 6 месяцев. Ему необходимо докупить защиту для 10 станций.	**LBW-BRC-6M:6M-210:200-C1**
3.	У заказчика – учебного заведения имеется лицензия из примера 2, до окончания действия которой осталось 7 месяцев. Ему необходимо докупить защиту для 10 станций и одновременно продлить лицензию еще на 2 года.	**LBW-BRC-31M:7M-210:200-D1**

Примеры кодов лицензий для категории «Комплекты»

1.	Заказчику необходим комплект Dr.Web «Универсальный», защита 50 ПК с Центром управления, Комплексная защита, на 12 месяцев, электронная лицензия.	**LZZ-*CR-12M-50-A3**
2.	Заказчику необходим комплект Dr.Web «Универсальный», защита 50 ПК с Центром управления, Комплексная защита, на 12 месяцев, электронная лицензия.	**LZZ-*C-12M-50-A3**
3.	Заказчику – учебному заведению (школа) необходима защита для 100 ПК.	**LZZ-*C-12M-100-A1**

Примеры кодов лицензий для категории «Утилиты»

1.	Заказчику необходимо провести лечение 100 ПК в течение 10 дней. ПК объединены в корпоративную сеть.	**LYW-AC-10D-100-A3**
2.	Заказчику необходимо провести лечение 10 ПК в течение 30 дней. ПК не объединены в корпоративную сеть.	**LYW-AK-30D-10-A3**

Примеры кодов лицензий для категории «ПАК Dr.Web Office Shield»

Создается столько кодов, сколько лицензируется продуктов Dr.Web

1.	Заказчику – учебному заведению необходима защита 25 пользователей почты (AB+AC+SMTP proxy) и 50 пользователей интернет-шлюза.	**LXP-AASC-12M-25-A1** **LXG-AK-12M-50-A1**
2.	Заказчику необходима комплексная защита 150 ПК, 1 сервера Windows, 100 пользователей почты (только антивирус) и 50 пользователей интернет-шлюза.	**LXW-BC-12M-150-A3** **LXS-AC-12M-1-A3** **LXP-AC-12M-100-A3** **LXG-AC-12M-50-A3**
3.	Заказчик имеет лицензию из примера 2, до окончания действия которой осталось 7 месяцев. Ему необходимо докупить защиту еще для 20 ПК и продлить лицензию на 1 год.	**LXW-BC-19M:7M-170:150-D3** **LXS-AC-19M-1-B3** **LXP-AC-19M-100-B3** **LXG-AK-19M-50-B3**

Примеры кодов для OEM-продуктов

1.	Партнер закупает 500 OEM-карт в медиапакетах	**PHW-B-6M-1-F3**
2.	Партнер закупает 500 OEM-лицензий, поставляемых на дисках	**MHW-B-6M-1-F3**

Обучающее видео: https://pa.drweb.com/marketing/video

Дата актуализации 20.11.2015

Контакты

Россия

ООО «Доктор Веб»

Россия, 125124, 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 | www.freedrweb.com

Германия

Doctor 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, +7 (727) 323–62–31, +7 (727) 323–62–32
www.drweb.kz

Украина

Центр технической поддержки «Доктор Веб»

01601, Украина, г. Киев, ул. Пушкинская, 27, 5-й этаж, оф.6
Тел./факс: +38 (044) 238–24–35
www.drweb.ua

Франция

Doctor Web France

333 b Avenue de Colmar, 67100 Strasbourg
Телефон: +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

Китай

Doctor Web Software Company (Tianjin), Ltd.

300457, КНР, г. Тяньцзинь, Тяньцзинская зона экономического и технического развития, 4-й проспект, д. 80, Технопарк «Тяньда», Северный Софт-корпус, каб. 112.
天津市经济技术开发区第四大街80号软件大厦北楼112
Тел.: +86-022-59823480
Факс: +86-022-59823480
E-mail: D.Liu@drweb.com
www.drweb.com