

# Dr.Web Gateway Security Suite

Для интернет-шлюзов Unix

<https://антивирус.пф>

<https://www.drweb.ru>

- Антивирусная проверка HTTP- и FTP-трафика, проходящего через корпоративный интернет-шлюз — прокси-сервер
- Защита от ВПО внутренних устройств компании, не имеющих установленного антивируса
- В Реестре отечественного ПО
- Сертифицирован ФСТЭК России, ФСБ России, Минобороны России
- Обеспечивает выполнение требований норм регуляторов в части антивирусной защиты ИСПДн до 1 уровня защищенности включительно, ГИС до 1 класса защищенности включительно, систем обработки сведений, содержащих гостайну, объектов КИИ вплоть до высшей категории
- Совместимость с российскими ОС МСВС, Альт Линукс, Astra Linux, ROSA, Ред ОС и др.



## Интернет является основным источником атак на компьютеры и устройства компании

От бесперебойного функционирования компьютеров и самых различных устройств, их «свободы» от вирусов зависят многие бизнес-процессы компании.

Пропуск в локальную сеть вредоносной программы позволяет злоумышленнику атаковать всё, что подключено к локальной сети, — от обычных компьютеров и серверов до офисной техники.

Установка антивируса Dr.Web на шлюз сети Интернет компании не позволит злоумышленнику модифицировать передающуюся через него информацию.

### Решаемые Dr.Web для интернет-шлюзов Unix задачи

- **Обнаружение неизвестных в момент атаки угроз**  
Надежная защита от всех вредоносных программ — в том числе еще не попавших на анализ в антивирусную лабораторию «Доктор Веб».
- **Полная проверка веб-трафика** — в том числе защищенных соединений. Чистый трафик от ваших партнеров и клиентов. Взлом домена или перехват трафика злоумышленниками не даст им возможности послать вам вирус.
- **Ограничение доступа к потенциально опасным ресурсам сети Интернет** с помощью тематических баз, а также черных и белых списков.
- **Непосредственная защита самого сервера** от атак злоумышленников, включая периодическую проверку объектов файловой системы.
- **Удаленная проверка систем, установка антивируса на которые невозможна.**

Использование Dr.Web для интернет-шлюзов Unix значительно снижает затраты предприятия и повышает надежность бизнес-процессов.

- **Поддержка систем мониторинга**  
Dr.Web для интернет-шлюзов Unix может быть интегрирован с любыми системами мониторинга — от локально расположенных в сети компании и до систем центров ГосСОПКА.
- **Распределенная проверка**  
Защищаемые данные могут передаваться на проверку на удаленные серверы или различные узлы кластерных систем.
- **Защита от ранее неизвестных вредоносных программ**  
Все загружаемые файлы и документы проверяются с использованием технологии обнаружения неизвестных вредоносных объектов новейших типов, в том числе скрытых неизвестными упаковщиками.
- **Минимальная совокупная стоимость**  
Dr.Web работает не только на отдельно стоящих серверах, но и на кластерах. В случае кластерного решения лицензировать необходимо только одну копию, что существенно снижает затраты на антивирусную защиту.
- **Защита от угроз нулевого дня**  
Обеспечивается с помощью Облака Dr.Web и алгоритмов на основе машинного обучения.
- **Защита объектов операционной системы, на которой установлен Dr.Web для интернет-шлюзов Unix**  
Периодическая проверка сервера производится встроенным антивирусным сканером.

- **Локальное облако**  
Возможности Dr.Web для интернет-шлюзов UNIX позволяют компонентам решения обмениваться обновлениями, результатами проверки файлов, передавать друг другу на проверку файлы, а также предоставлять услуги сканирующего ядра.
- **Возможность проверки удаленных устройств**  
Dr.Web для интернет-шлюзов UNIX позволяет выполнить удаленную проверку не только обычных компьютеров, но и устройств Интернета вещей — роутеров, ТВ-приставок.
- **Высокая скорость сканирования и актуальность в любой момент времени**  
Компактные вирусные базы и технология несигнатурного поиска неизвестных вирусов Origins Tracing™ и развитый эвристический анализ позволяют обнаружить любые, даже неизвестные вредоносные программы в момент атаки злоумышленников.
- **Простота установки и гибкость настроек**, автоматизированное и легко контролируемое развертывание Dr.Web, возможности гибкого конфигурирования через консоль администратора.
- **Удобство администрирования**  
Администратор сети может управлять защитой с помощью веб-интерфейса, утилит командной строки, контролировать работу защиты из внешних систем.
- **Отдельные настройки для различных защищаемых областей и гибкий выбор типов проверки.**
- **Ограничение данных, передаваемых через интернет-шлюз, а также ограничение доступа к шлюзу со стороны отдельных компьютеров.**
- **Встроенный компонент Dr.Web Firewall для Linux**  
Защита сервера от взлома.
- **Возможность работы при 500 МБ свободной оперативной памяти.**

**Для перехода на иные почтовые серверы или операционные системы смена или дозакупка лицензии не требуется!**

**Импортозамещение не доставит вам проблем.**

Лицензирование Dr.Web Mail Security Suite

Виды лицензий	Варианты лицензий
<ul style="list-style-type: none"><li>▪ По числу защищаемых серверов</li><li>▪ Посерверная лицензия (до 3000 пользователей)</li><li>▪ Безлимитная лицензия</li></ul>	<ul style="list-style-type: none"><li>▪ Антивирус</li></ul> Центр управления лицензируется бесплатно. <a href="#">Все условия лицензирования</a>

## Предпродажная поддержка

- Бесплатное тестирование продуктов Dr.Web — в сети заказчика или удаленно в виртуальной среде
- Развертывание, помощь при внедрении (по телефону или с выездом на территорию заказчика (только в Москве))
- Презентация, вебинар, семинар
- Помощь в написании или проверке написанного технического задания

## Техническая поддержка

- Круглосуточно — по телефону и через форму <https://support.drweb.ru>
- В России, на русском языке
- Бесплатные услуги поддержки и бесплатная расшифровка от троянцев-вымогателей для лицензий в прайсовом диапазоне
- Стоимость поддержки для запрайсовых и безлимитных лицензий оговаривается особо
- Платная VIP-поддержка

## Услуги и сервисы

### Dr.Web vxCube

- **Облачный интеллектуальный интерактивный анализатор подозрительных объектов на вредоносность**
- **Немедленное изготовление лечащей утилиты по результатам анализа**
- **Для специалистов по информационной безопасности и киберкриминалистов**

Незаменимым средством в ситуациях, когда вредоносный файл пробрался внутрь защищаемого антивирусом периметра или у вас появились обоснованные, на ваш взгляд, подозрения, что в сети завелся «чужой», является облачный интерактивный анализатор Dr.Web vxCube.

Dr.Web vxCube в течение одной минуты оценит вредоносность файла и изготовит лечащую утилиту для устранения последствий его работы. Проверка занимает от одной минуты! По результатам анализа предоставляется отчет. Его можно просмотреть в личном кабинете пользователя Dr.Web vxCube или скачать в виде архива.

Если объект однозначно представляет угрозу, пользователь немедленно получает специальную сборку лечащей утилиты Dr.Web CureIt! (если это входит в лицензию) для очищения системы от действий, произведенных проанализированным файлом.

Это дает возможность максимально быстро обезвредить новейшую угрозу, не дожидаясь обновлений используемого антивируса.

Благодаря универсальности утилиты Dr.Web CureIt!, способной работать без установки в любой системе, где используется другой антивирус (не Dr.Web), это будет особенно полезно компаниям, пока не использующим Dr.Web в качестве основного средства защиты.

Демодоступ: <https://download.drweb.ru/vxcube>

Подробнее о Dr.Web vxCube: <https://www.drweb.ru/vxcube>

## Антивирусные исследования

### Анализ вредоносных файлов специалистами антивирусной лаборатории «Доктор Веб»

Ни один автоматизированный сервис никогда не заменит опыт и знания вирусного аналитика. В случае если вердикт Dr.Web vxCube о проанализированном файле будет не однозначно вредоносный, но у вас останутся сомнения в этом решении, предлагаем воспользоваться услугами специалистов антивирусной лаборатории «Доктор Веб» с многолетним опытом вирусного анализа.

Услуги включают анализ вредоносных файлов любой сложности, по результатам которого выдается отчет, содержащий:

- описание алгоритмов работы вредоносного ПО и его модулей;
- категоризацию объектов: однозначно вредоносный, потенциально вредоносный (подозрительный), др.;
- анализ сетевого протокола и выявление командных серверов;
- влияние на зараженную систему и рекомендации к устранению заражения.

Заявки на антивирусные исследования принимаются по адресу: <https://support.drweb.ru>.

### Экспертиза вирусозависимых компьютерных инцидентов (ВКИ)

Если ваша компания пострадала от действия вредоносного ПО и требуется квалифицированная экспертиза вирусных аналитиков, воспользуйтесь услугами специального подразделения компании «Доктор Веб».

Об экспертизе ВКИ: <https://antifraud.drweb.ru/expertise>

Заявки на экспертизу: <https://support.drweb.ru/expertise>



© ООО «Доктор Веб», 2003–2019

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Тел.: +7 495 789-45-87 (многоканальный), факс: +7 495 789-45-97

<https://антивирус.пф> • <https://www.drweb.ru> • <https://free.drweb.ru> • <https://curenet.drweb.ru>

