

Управление станциями под macOS



© «Доктор Веб», 2019. Все права защищены

Материалы, приведенные в данном документе, являются собственностью «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

Товарные знаки

Dr.Web, SpIDer Mail, SpIDer Guard, Curelt!, CureNet!, AV-Desk, КАТАNA и логотип Dr.WEB являются зарегистрированными товарными знаками «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

Ограничение ответственности

Ни при каких обстоятельствах «Доктор Веб» и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

Dr.Web Enterprise Security Suite. Управление станциями под macOS Версия 12.0 Руководство администратора 01.04.2019

«Доктор Веб», Центральный офис в России 125040 Россия, Москва 3-я улица Ямского поля, вл.2, корп.12A Сайт: <u>https://www.drweb.com/</u>

cam. <u>https://www.arweb.com/</u>

Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах Вы можете найти на официальном сайте компании.

«Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности.

«Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!



Содержание

Глава 1. Введение	5
1.1. Назначение документа	5
1.2. Условные обозначения и сокращения	6
Глава 2. Dr.Web Enterprise Security Suite	
2.1. О продукте	
2.2. Защита станций сети	8
Глава 3. Dr.Web для macOS	10
3.1. Компоненты Dr.Web для macOS	10
3.2. Настройка Dr.Web для macOS	11
3.2.1. Сканер	12
3.2.2. SpIDer Guard	13
3.2.3. SpIDer Gate	15
Техническая поддержка	19



Глава 1. Введение

1.1. Назначение документа

Руководство описывает централизованное управление настройками антивирусного решения Dr.Web для macOS. Руководство администратора входит в пакет документации антивирусной сети, который описывает реализацию комплексной антивирусной защиты компьютеров и мобильных устройств компании с помощью Dr.Web Enterprise Security Suite.

Руководство предназначено для администратора антивирусной сети — сотрудника организации, которому поручено руководство антивирусной защитой рабочих станций и серверов корпоративной сети.

В руководстве приведена информация о централизованной настройке антивирусного ПО рабочих станций под управлением macOS. Администратор антивирусной сети управляет настройками через Центр управления Dr.Web.

Дополнительная информация

- Руководство пользователя Dr.Web для macOS содержит информацию о настройке антивирусного ПО непосредственно на станции.
- Документация администратора антивирусной сети Dr.Web Enterprise Security Suite (включает Руководство администратора, Руководство по установке и Приложения) содержит основную информацию по установке и настройке антивирусной сети, а также работе с Центром управления Dr.Web.

Последнюю версию руководств см. на сайте «Доктор Веб».



1.2. Условные обозначения и сокращения

Условные обозначения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
(!)	Важное замечание или указание.
\triangle	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<ip-address></ip-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
/Volumes/Macinto sh HD/	Наименования файлов и каталогов, фрагменты программного кода.
<u>Приложение А</u>	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте используются следующие сокращения:

- BCO Dr.Web Всемирная Система Обновлений Dr.Web,
- ОС операционная система,
- ПО программное обеспечение,
- ЛВС локальная вычислительная сеть.



Глава 2. Dr.Web Enterprise Security Suite

2.1. О продукте

Dr.Web Enterprise Security Suite предназначен для организации и управления единой и надежной комплексной антивирусной защитой как внутренней сети компании, включая мобильные устройства, так и домашних компьютеров сотрудников.

Совокупность компьютеров и мобильных устройств, на которых установлены взаимодействующие компоненты Dr.Web Enterprise Security Suite, представляет собой единую *антивирусную сеть*.



Логическая структура антивирусной сети



Антивирусная сеть Dr.Web Enterprise Security Suite имеет архитектуру клиент-сервер. Ее компоненты устанавливаются на компьютеры и мобильные устройства пользователей и администраторов, а также на компьютеры, выполняющие функции серверов ЛВС. Компоненты антивирусной сети обмениваются информацией, используя сетевые протоколы TCP/IP. Антивирусное ПО на защищаемые станции возможно устанавливать (и впоследствии управлять ими) как через ЛВС, так и через Интернет.

2.2. Защита станций сети

Каждый компьютер с установленным антивирусным пакетом, в соответствии с его функциями в антивирусной сети, является отдельной *рабочей станцией*. Защита рабочих станций осуществляется антивирусными пакетами Dr.Web для соответствующих операционных систем.



В локальной сети компьютер с установленным антивирусным пакетом может быть как рабочей станцией или мобильным устройством, так и сервером локальной сети в зависимости от его функций.

Антивирусные пакеты устанавливаются на станциях и подключаются к Серверу Dr.Web. Каждая станция входит в состав одной или нескольких групп, зарегистрированных на этом Сервере. Информация между станцией и Сервером передается по протоколу TCP/IP версии 4 или 6, который используется в локальной сети.

Установка

Администратор или пользователь устанавливает антивирусный пакет для macOS непосредственно на станцию. Подробное описание установки антивирусных пакетов на рабочие станции см. в **Руководстве по установке Dr.Web Enterprise Security Suite**.

Управление

При поддержке связи с Сервером Dr.Web администратору доступны следующие функции антивирусного пакета на станции:

• Централизованная настройка Dr.Web на рабочих станциях при помощи Центра управления.

При этом администратор может как запретить, так и разрешить пользователю самостоятельно изменять настройки на станции.

- Настройка расписания антивирусных проверок и других заданий, выполняемых на станции.
- Получение статистики антивирусной проверки и прочей информации о работе компонентов защиты и о состоянии станции.
- Запуск и останов антивирусной проверки и т. п.



Обновление

Сервер Dr.Web загружает обновления и распространяет их на подключенные к нему станции. Это позволяет автоматически устанавливать, поддерживать и регулировать защиту от угроз независимо от квалификации пользователей рабочих станций.

Если рабочая станция временно отключена от антивирусной сети, на станции используется локальная копия настроек. Компоненты антивирусной защиты продолжают работать (пока не истечет срок действия пользовательской лицензии). При этом обновление ПО не производится. Если для станции разрешено функционирование в Мобильном режиме, при потере связи с Сервером вирусные базы обновляются напрямую с серверов ВСО.



Принцип работы в Мобильном режиме описан в **Руководстве администратора** Dr.Web Enterprise Security Suite.



Глава 3. Dr.Web для macOS

Dr.Web для macOS защищает компьютеры под управлением macOS и macOS Server от угроз любого типа: вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и всех возможных типов вредоносных объектов из любых внешних источников.

Dr.Web для macOS состоит из нескольких компонентов защиты, которые отвечают за соответствующий функционал антивируса. В состав всех компонентов входят антивирусное ядро и вирусные базы. Компоненты продукта постоянно обновляются, а вирусные базы, списки нежелательных сайтов и правила фильтрации спама в почте регулярно дополняются новыми сигнатурами угроз.

Постоянное обновление помогает защищать устройства, приложения и данные пользователей от самых последних угроз. Для дополнительной защиты от неизвестного вредоносного программного обеспечения используются методы эвристического анализа, реализованные в антивирусном ядре.

3.1. Компоненты Dr.Web для macOS

Защиту станций под управлением macOS/macOS Server осуществляют следующие компоненты:

Сканер Dr.Web, Dr.Web Agent Сканер

Проверка Мас по запросу пользователя, а также согласно расписанию. Запуск удаленной антивирусной проверки станций из Центра управления.

SpIDer Guard

Постоянная проверка файловой системы в режиме реального времени. Контроль всех программ и процессов, запущенных на Мас. Проверка новых файлов на жестких дисках и файлов, которые пользователь открывает на сменных носителях.

SpIDer Gate

Проверка всех подключений к сайтам по протоколу HTTP. Обезвреживание угроз и блокировка передачи объектов, которые могут угрожать безопасности Мас. Ограничение доступа к нерекомендуемым сайтам, известным источникам распространения вирусов и страницам, которые содержат материалы, нарушающие законодательство об авторских правах.

Карантин

Изоляция обнаруженных вредоносных и подозрительных объектов в специальной папке.



Описание работы с Карантином через Центр управления приведено в Руководстве администратора Dr.Web Enterprise Security Suite.

3.2. Настройка Dr.Web для macOS

Чтобы просмотреть или изменить настройки компонентов защиты на рабочей станции

- 1. Выберите пункт Антивирусная сеть главного меню Центра управления.
- 2. В открывшемся окне в иерархическом списке нажмите на название станции под macOS/macOS Server или группы, содержащей такие станции.
- 3. В открывшемся управляющем меню в разделе **Конфигурация**, в подразделе **macOS** выберите необходимый компонент защиты:
 - Сканер для рабочих станций/Сканер для серверов
 - SplDer Guard для рабочих станций/SplDer Guard для серверов
 - SplDer Gate для рабочих станций/SplDer Gate для серверов

Откроется окно настроек компонента.

4. Внесите необходимые изменения в настройки компонентов.

Обратите внимание, управление настройками компонентов через Центр управления отличается от управления настройками непосредственно на станции:

 для управления отдельными параметрами используйте кнопки, расположенные справа от соответствующих настроек:

Установить в начальное значение — восстановить последнее сохраненное значение параметра.

К Сбросить в значение по умолчанию — установить для параметра значение по умолчанию.

• для управления совокупностью всех параметров раздела используйте кнопки на панели инструментов:

Установить все параметры в начальные значения — восстановить последние сохраненные значения всех параметров раздела.

Установить все параметры в значения по умолчанию — установить для всех параметров раздела значения по умолчанию.

Распространить эти настройки на другой объект — скопировать настройки из раздела в настройки другой станции, группы или нескольких групп и станций.

Установить наследование настроек от родительской группы — удалить персональные настройки станций и установить наследование настроек раздела от первичной группы.

Копировать настройки из родительской группы и установить их в качестве персональных — скопировать настройки раздела из первичной группы и задать их



для выбранных станций. Наследование при этом не устанавливается, и настройки станции считаются персональными.

Экспортировать настройки из данного раздела в файл — сохранить все настройки из раздела в файл специального формата.

Импортировать настройки в данный раздел из файла — заменить все настройки в разделе настройками из файла специального формата.

5. Нажмите кнопку Сохранить.

Настройки будут переданы на станции. Если станции были отключены в момент внесения изменений, настройки будут переданы в момент подключения станций к Серверу.



Администратор может запретить пользователю редактировать настройки на станции (см. раздел Права пользователей станции в Руководстве администратора Dr.Web Enterprise Security Suite). При этом редактировать настройки сможет только сам администратор через Центр управления.

3.2.1. Сканер

Сканер Dr.Web осуществляет быструю или полную проверку объектов файловой системы или проверяет только критические файлы и папки.

Настройки Сканера Dr.Web для компьютеров под управлением macOS задаются в разделе **Сканер для рабочих станций**, для компьютеров под управлением macOS Server — в разделе **Сканер для серверов**.

Общие

- Включите опцию Проверять архивы, чтобы использовать проверку файлов в архивах.
- Включите опцию **Проверять почтовые файлы**, чтобы использовать проверку файлов почты.
- В поле **Время проверки одного файла** укажите максимальное время проверки одного файла. Значение 0 указывает, что время проверки одного файла не ограничено.



Включение проверки архивов и почтовых файлов, а также увеличение максимального времени проверки одного файла могут привести к замедлению работы системы и увеличить общее время проверки.

Действия

В этом разделе настроек вы можете настроить действия, которые Dr.Web должен применять к угрозам, обнаруженным Сканером. Действия задаются отдельно для каждого



типа вредоносных и подозрительных объектов. Состав доступных действий при этом зависит от типа объектов.

Возможные действия

• Лечить, перемещать в карантин неизлечимые. Восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин.

Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).

• Лечить, удалять неизлечимые. Восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален.

Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).

- Перемещать в карантин. Поместить обнаруженную угрозу в специальную папку, изолированную от остальной системы.
- Удалять. Удалить объект, представляющий угрозу.

Наиболее эффективный способ устранения компьютерных угроз любых типов.

• Игнорировать. Пропустить объект без выполнения каких-либо действий и не выводить оповещения.



Предустановленные настройки являются оптимальными для большинства случаев, не изменяйте их без необходимости.

Исключаемые пути

В этом разделе укажите пути к файлам и папкам, которые будут исключены из проверки Сканером Dr.Web.

3.2.2. SpIDer Guard

Монитор файловой системы SplDer Guard в режиме реального времени проверяет все файлы, к которым обращаются пользователи, и контролирует программы и процессы, запущенные на Мас.

Настройки SpIDer Guard для компьютеров под управлением macOS задаются в разделе **SpIDer Guard для рабочих станций**, для компьютеров под управлением macOS Server — в разделе **SpIDer Guard для серверов**.



Общие

- Включите опцию **Использовать эвристический анализ**, чтобы использовать эвристический анализатор для поиска неизвестных угроз.
- Используйте опцию Включить SplDer Guard для macOS (для серверов Включить SplDer Guard для серверов macOS), чтобы включить постоянную антивирусную защиту файловой системы.
- В поле **Время проверки одного файла** укажите максимальное время проверки одного файла. Значение 0 указывает, что время проверки одного файла не ограничено.



Увеличение максимального времени проверки одного файла может привести к замедлению работы системы и увеличить общее время проверки.

Действия

В этом разделе настроек вы можете настроить действия, которые Dr.Web должен применять к угрозам, обнаруженным SpIDer Guard. Действия задаются отдельно для каждого типа вредоносных и подозрительных объектов. Состав доступных действий при этом зависит от типа объектов.

Возможные действия

• Лечить, перемещать в карантин неизлечимые. Восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин.

Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).

• Лечить, удалять неизлечимые. Восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален.

Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).

- Перемещать в карантин. Поместить обнаруженную угрозу в специальную папку, изолированную от остальной системы.
- Удалять. Удалить объект, представляющий угрозу.

Наиболее эффективный способ устранения компьютерных угроз любых типов.

• Игнорировать. Пропустить объект без выполнения каких-либо действий и не выводить оповещения.





Предустановленные настройки являются оптимальными для большинства случаев, не изменяйте их без необходимости.

Контейнеры

В этом разделе вы можете указать максимальный уровень вложенности составных объектов. Если уровень вложенности будет превышать установленное значение, составные объекты будут пропущены при проверке. Если установлено значение 0, вложенные объекты проверяться не будут.

В поле **Максимальный коэффициент сжатия архива** укажите максимальную степень сжатия объекта (отношение размеров сжатого объекта и исходного). Если степень сжатия проверяемого объекта будет превышать установленное значение, объект будет пропущен при проверке.

Исключаемые пути

В этом разделе укажите пути к файлам и папкам, которые будут исключены из проверки SplDer Guard.

3.2.3. SplDer Gate

Интернет-монитор SplDer Gate проверяет входящий HTTP-трафик и блокирует передачу объектов, которые могут угрожать безопасности Mac.

SpIDer Gate ограничивает доступ к нерекомендуемым сайтам, известным источникам распространения вирусов и страницам, которые содержат материалы, нарушающие законодательство об авторских правах.

SpIDer Gate также позволяет ограничить доступ пользователей к различным категориям интернет-ресурсов, например, сайтов, посвященных азартным играм, оружию, наркотикам и т. п.

Настройки SpIDer Gate для компьютеров под управлением macOS задаются в разделе **SpIDer Gate для рабочих станций**, для компьютеров под управлением macOS Server — в разделе **SpIDer Gate для серверов**.

Общие

- Используйте опцию Включить SpiDer Gate, чтобы включить проверку HTTP-трафика.
- Включите опцию **Использовать эвристический анализ**, чтобы использовать эвристический анализатор для поиска неизвестных угроз.



• В поле **Время проверки одного файла** укажите максимальное время проверки одного файла. Значение 0 указывает, что время проверки одного файла не ограничено.



Увеличение максимального времени проверки одного файла может привести к замедлению работы системы и увеличить общее время проверки.

Действия

- Включите опцию **Проверять получаемые файлы**, чтобы включить проверку файлов, загружаемых по сети, на наличие вирусов и других угроз.
- В списках **Блокировать файлы** и **Блокировать дополнительно** выберите типы небезопасных получаемых объектов, которые будут блокироваться компонентом SpIDer Gate.

Веб-фильтр

- Включите опцию **Проверять URL**, чтобы ограничить доступ к интернет-ресурсам по категориям.
- Включите опцию **Блокировать нерекомендуемые сайты**, чтобы ограничить доступ к сайтам с сомнительным содержимым, ресурсам, заподозренным в фишинге, краже паролей и т. п.
- Включите опцию Блокировать URL, добавленные по обращению правообладателя, чтобы ограничить доступ к сайтам, которые содержат материалы, нарушающие законодательство об авторских правах. Это различные «пиратские» сайты, каталоги файловых ссылок, файлообменные ресурсы и т. п.
- В списке Блокировать следующие категории сайтов выберите категории интернетресурсов, доступ к которым будет ограничен:

Категория	Описание
Сайты для взрослых	Сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. п.
Насилие	Сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. п.
Оружие	Сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. п.
Азартные игры	Сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. п.
Наркотики	Сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.



Категория	Описание
Нецензурная лексика	Сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.).
Чаты	Сайты для обмена сообщениями в режиме реального времени.
Терроризм	Сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.
Электронная почта	Сайты, предоставляющие возможность бесплатной регистрации почтового ящика.
Социальные сети	Социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств.

- В разделах **Белый список/Черный список** добавьте пути к сайтам, доступ к которым нужно разрешить/ограничить:
 - a) Чтобы добавить в список определенный сайт, введите его адрес (например, www.example.com). Доступ ко всем ресурсам, расположенным на этом сайте, будет определяться данной записью.
 - b) Чтобы настроить доступ к сайтам с похожими именами, введите в поле общую часть их доменных имен. Пример: если вы введете текст example, то доступ к example.com, example.test.com, test.com/example, test.example222.ru и другим похожим сайтам будет определяться данной записью.
 - c) Чтобы настроить доступ к сайтам на определенном домене, укажите имя домена с символом «.», например, .ru. В таком случае доступ ко всем ресурсам, находящимся на этом домене, будет определяться данной записью.

Если при указании домена используется символ «/», то та часть подстроки, что стоит слева от символа «/», будет считаться доменным именем, а части справа от символа — частью разрешенного на данном домене адреса. Пример: если вы введете текст example.com/test, то будут обрабатываться такие адреса как example.com/test11, template.example.com/test22 и т. п.

d) Чтобы добавить в исключения определенные сайты, введите определяющую их маску в поле ввода. Маски добавляются в формате: mask://...

Маска задает общую часть имени объекта, при этом:

- символ «*» заменяет любую, возможно пустую, последовательность символов;
- символ «?» заменяет любой, в том числе пустой, но только один символ.

Примеры

- mask://*.ru/ или .ru в исключения будут добавлены все сайты в домене .ru;
- mask://mail в исключения будут добавлены все сайты, в именах которых содержится слово "mail";



• mask://???.ru/ — будут открываться все сайты зоны .ru, имена которых состоят из трех или менее знаков.

Введенная строка при добавлении в список может быть преобразована к универсальному виду. Например: adpec http://www.example.com будет преобразован в запись www.example.com.

Контейнеры

В этом разделе вы можете указать максимальный уровень вложенности составных объектов. Если уровень вложенности будет превышать установленное значение, составные объекты будут пропущены при проверке. Если установлено значение 0, вложенные объекты проверяться не будут.

В поле **Максимальный коэффициент сжатия архива** укажите максимальную степень сжатия объекта (отношение размеров сжатого объекта и исходного). Если степень сжатия проверяемого объекта будет превышать установленное значение, объект будет пропущен при проверке.

Дополнительно

- Настройка **Уровень журнала** определяет уровень подробности ведения журнала компонентом SplDer Gate.
- Настройка **Метод ведения журнала** определяет способ ведения журнала компонентом SplDer Gate. Возможные значения:
 - Auto используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web.
 - Syslog сообщения журнала SpIDer Gate сохраняются с помощью системного сервиса syslog. В случае выбора этого метода укажите в выпадающем списке Подсистема syslog используемую syslog подсистему (метку) для сохранения сообщений от SpIDer Gate.
 - Path сообщения журнала SplDer Gate сохраняются в отдельный заданный файл. В случае выбора этого метода укажите путь к файлу в поле Файл журнала.



Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу <u>https://support.drweb.com/show_faq/;</u>
- посетите форумы компании «Доктор Веб» по адресу <u>https://forum.drweb.com/</u>.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Beб»:

- заполните веб-форму в соответствующей секции раздела <u>https://support.drweb.com/;</u>
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу <u>https://company.drweb.com/contacts/offices/</u>.