Dr.WEB

Enterprise Security Suite

Управление станциями под macOS

Dr.Web Enterprise Security Suite. Управление станциями под macOS
Версия 13.0
Руководство администратора
06.06.2025

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 2, корп. 12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «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

1. Введение 5

1.1. Назначение документа 5

1.2. Условные обозначения и сокращения 6

2. Dr.Web Enterprise Security Suite 7

2.1. О продукте 7

2.2. Защита станций сети 8

3. Dr.Web Desktop Security Suite (macOS) и Dr.Web Server Security Suite (macOS) 10

3.1. Компоненты 10

3.2. Настройка 11

3.2.1. Сканер 12

3.2.2. SpIDer Guard 14

3.2.3. SpIDer Gate 17

4. Режим централизованной защиты 21

5. Шифрование и сжатие трафика 25

6. Работа в Мобильном режиме 27

7. Техническая поддержка 28

1. Введение

1.1. Назначение документа

В этом руководстве описывается централизованное управление настройками продуктов Dr.Web Desktop Security Suite (macOS) и Dr.Web Server Security Suite (macOS) (далее каждый из них — Dr.Web). Руководство входит в пакет документации антивирусной сети, который описывает реализацию комплексной антивирусной защиты компьютеров и мобильных устройств компании с помощью Dr.Web Enterprise Security Suite.

Этот документ предназначен 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

- В **Руководстве пользователя Dr.Web Desktop Security Suite (macOS)** и **Руководстве пользователя Dr.Web Server Security Suite (macOS)** содержится информация о настройке антивирусного ПО непосредственно на станции.
- В документации администратора антивирусной сети Dr.Web Enterprise Security Suite (включает **Руководство администратора**, **Руководство по установке** и **Приложения**) содержится основная информация по установке и настройке антивирусной сети, а также работе с Центром управления Dr.Web.

Последние версии указанных выше руководств размещены 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.
	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>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`/Volumes/Macintosh HD/`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте используются следующие сокращения:

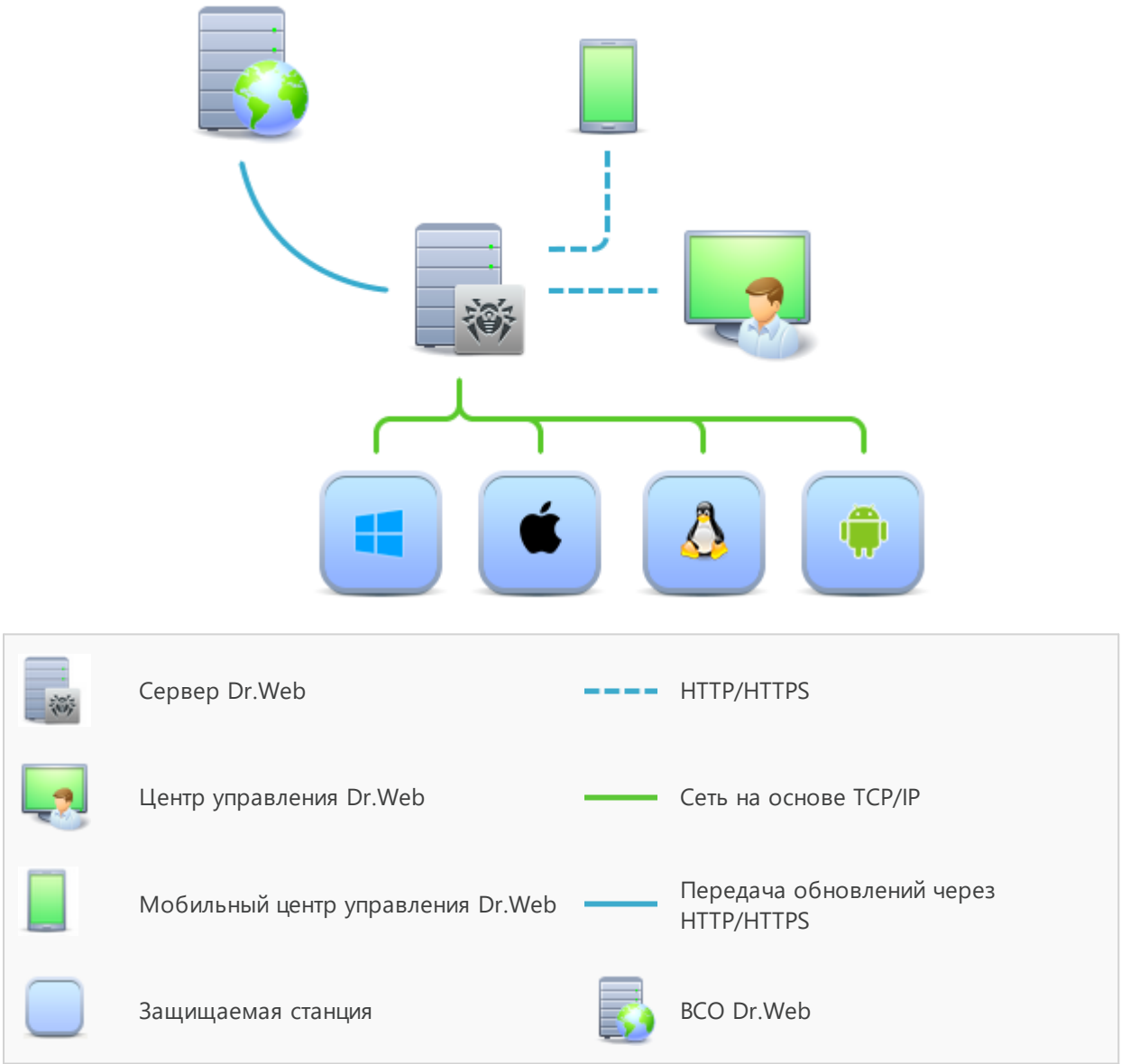
- ВСО Dr.Web — Всемирная Система Обновлений Dr.Web;
- ОС — операционная система;
- ЛВС — локальная вычислительная сеть.

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 Dr.Web 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 отключится от антивирусной сети, на станции будет использоваться локальная копия настроек. Компоненты антивирусной защиты продолжат работу, пока не истечет срок действия лицензионного ключа станции, расположенного на Сервере Dr.Web. При этом ПО обновляться не будет. Если для станции разрешена работа в Мобильном режиме, при потере связи с Сервером Dr.Web вирусные базы будут обновляться напрямую с серверов ВСО Dr.Web.

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

3. Dr.Web Desktop Security Suite (macOS) и Dr.Web Server Security Suite (macOS)

Dr.Web Desktop Security Suite (macOS) и Dr.Web Server Security Suite (macOS) (далее каждый из них — Dr.Web) защищают 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 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

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

Сканер Dr.Web, Dr.Web Agent Сканер

Проверка станции 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 станции. 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 станции. Ограничение доступа к нерекомендуемым сайтам, известным источникам распространения вирусов и страницам, которые содержат материалы, нарушающие законодательство об авторских правах.

Брандмауэр (управляется со станции)

Защита станции от несанкционированного доступа извне и предотвращение утечки важных данных. Контроль подключения приложений к интернету и передачи данных по сети, а также блокировка подозрительных соединений.

3.2. Настройка

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
   - SpIDer Guard для рабочих станций/SpIDer Guard для серверов
   - SpIDer Gate для рабочих станций/SpIDer 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.

     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.

Скопировать 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 Dr.Web.

> 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 максимальный период времени, который отводится на проверку одного файла. Значение по умолчанию: 0 (время проверки 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.

- **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.

Действия Сканера над обнаруженными вредоносными объектами

Тип объекта	Действие				
	Лечить, перемещать в карантин неизлечимые	Лечить, удалять неизлечимые	Переместить в карантин	Удалить	Игнорировать
Вредоносные	+/*	+	+	+	
Подозрительные			+/*	+	+
Рекламные программы			+/*	+	+
Программы дозвона			+/*	+	+

Тип объекта	Действие				
	Лечить, перемещать в карантин неизлечимые	Лечить, удалять неизлечимые	Переместить в карантин	Удалить	Игнорировать
Программы-шутки			+	+	+/*
Потенциально опасные			+	+	+/*
Программы взлома			+	+	+/*

Условные обозначения

+	допустимое действие
+/*	действие, установленное по умолчанию

Исключаемые пути

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

3.2.2. SplDer Guard

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

Настройки SplDer Guard для компьютеров под управлением macOS задаются в разделе **SplDer Guard для рабочих станций**, для компьютеров под управлением macOS Server — в разделе **SplDer 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 максимальный период времени, который отводится на проверку одного файла. Допустимые значения: от 1 секунды (1s) до 1 часа (1h). Значение по умолчанию: 30 секунд (30s).

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 SplDer 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.

Действия SplDer Guard над обнаруженными вредоносными объектами

Тип объекта	Действие				
	Лечить, перемещать в карантин неизлечимые	**Лечить, удалять неизлечимые**	**Переместить в карантин**	**Удалить**	**Игнорировать**
Вредоносные	+/*	+	+	+	
Подозрительные			+/*	+	+
Рекламные программы			+/*	+	+
Программы дозвона			+/*	+	+
Программы-шутки			+	+	+/*
Потенциально опасные			+	+	+/*
Программы взлома			+	+	+/*

Условные обозначения

+	допустимое действие
+/*	действие, установленное по умолчанию

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 SpIDer Guard.

3.2.3. SplDer Gate

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

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

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

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

Общие

- Используйте опцию **Включить SplDer 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 максимальный период времени, который отводится на проверку одного файла. Допустимые значения: от 1 секунды (1s) до 1 часа (1h). Значение по умолчанию: 30 секунд (30s).

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 SplDer 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 интернет-ресурсов, 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.
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: адрес `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 SplDer 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 SplDer Gate.
- **Path** — сообщения журнала SplDer Gate сохраняются в отдельный заданный файл. В случае выбора этого метода укажите путь к файлу в поле **Файл журнала**.

4. Режим централизованной защиты

Настройки и компоненты

Настройки и работа компонентов Dr.Web на станции могут быть удаленно изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг провайдера. С Сервера Dr.Web, который выступает в роли сервера централизованной защиты, могут контролироваться:

- Обновление вирусных баз. Обновления загружаются на рабочую станцию с Сервера Dr.Web автоматически. Если соединения с Сервером Dr.Web нет, то станция переходит в Мобильный режим и обновления начинают загружаться через интернет с серверов ВСО Dr.Web.

  Станция сможет перейти в Мобильный режим, только если этот режим для нее разрешен в Центре управления (**Антивирусная сеть** → **Права** → **macOS** → **Общие** → **Запуск в мобильном режиме**). В противном случае вирусные базы на станции не будут обновляться, пока соединение с Сервером Dr.Web не восстановится.

- Постоянная защита файловой системы.
- Проверка веб-трафика.
- Проверка Mac на вирусы. Администратор антивирусной сети может запустить удаленную проверку рабочей станции с сервера вручную или согласно расписанию.

Подключение станции к Серверу Dr.Web

Каждый компьютер под управлением macOS с установленным Dr.Web является отдельной станцией. Существует два способа подключения станции к антивирусной сети:

- С имеющимися учетными данными: если станция уже создана на Сервере Dr.Web и для нее заданы идентификатор и пароль.
- В качестве новой станции («новичка»): идентификатор и пароль для станции будут созданы при подключении ее к Серверу Dr.Web. Станцию, создаваемую в качестве новой, требуется авторизовать на Сервере Dr.Web. Это делается вручную или автоматически в зависимости от настроек доступа, установленных на Сервере Dr.Web.

  Dr.Web версии 12.5 и более поздних совместим только с Сервером Dr.Web Enterprise Security Suite версии 11.0 и более поздних.

  Инструкции по созданию учетной записи станции и настройке политики подключения станций приведены в **Руководстве администратора Dr.Web Enterprise Security Suite**.

Подключение с имеющимися учетными данными

Существует несколько вариантов подключения станции к Серверу Dr.Web. Выбор варианта зависит от наличия на станции установленного Dr.Web.

Dr.Web на станции еще не установлен

Установите Dr.Web на станции и подключите станцию к Серверу Dr.Web с помощью инсталляционного пакета (с расширением `.run`), содержащего параметры подключения. Для установки следуйте инструкциям, приведенным в **Руководстве пользователя Dr.Web Desktop Security Suite (macOS)** и **Руководстве пользователя Dr.Web Server Security Suite (macOS)** (раздел «Режим централизованной защиты > Автоматическое подключение > Чтобы установить Dr.Web с помощью файла .run»).

Чтобы скачать инсталляционный пакет

1. Перейдите в раздел **Администрирование** главного меню Центра управления, затем в управляющем меню слева выберите **Общая конфигурация репозитория**.
2. Перейдите на вкладку **Инсталляционные пакеты Dr.Web → Корпоративные продукты Dr.Web**.
3. Установите флаг для **Dr.Web Desktop Security Suite (macOS)** и нажмите **Сохранить**.
4. Обновите репозиторий через раздел **Состояние репозитория** в управляющем меню.
5. Перейдите в раздел **Антивирусная сеть** главного меню Центра управления.
6. Выберите группу или станцию, для которой нужно скачать инсталляционный пакет (файл с расширением `.run`).
7. Справа напротив параметра **Инсталяционный пакет** нажмите ссылку для macOS и скачайте файл.

Dr.Web на станции установлен, но не подключен, и нужно подключить станцию, не вводя параметры подключения вручную

Если Dr.Web на станции уже установлен, но работает в автономном режиме (без указания параметров подключения), подключите его к Серверу Dr.Web с помощью конфигурационного файла `install.cfg`, содержащего параметры подключения. Для установки следуйте инструкциям, приведенным в **Руководстве пользователя Dr.Web Desktop Security Suite (macOS)** и **Руководстве пользователя Dr.Web Server Security Suite (macOS)** (раздел «Режим централизованной защиты > Автоматическое подключение > Чтобы подключить станцию с помощью конфигурационного файла»).

Чтобы скачать конфигурационный файл

1. Перейдите в раздел **Антивирусная сеть** главного меню Центра управления.
2. Выберите станцию, для которой нужно скачать конфигурационный файл.
3. Справа напротив параметра **Конфигурационный файл** нажмите ссылку для macOS & Android & Linux и скачайте файл.

Dr.Web на станции установлен, но не подключен, и нужно подключить станцию, введя параметры подключения вручную

Вы можете вручную настроить параметры подключения станции с установленным Dr.Web к Серверу Dr.Web. Для этого вам понадобится сертификат. Чтобы настроить параметры подключения на станции, следуйте инструкциям, приведенным в **Руководстве пользователя Dr.Web Desktop Security Suite (macOS)** и **Руководстве пользователя Dr.Web Server Security Suite (macOS)** (раздел «Режим централизованной защиты > Автоматическое подключение > Чтобы настроить параметры подключения к серверу вручную»).

Чтобы скачать сертификат

1. Выберите пункт **Администрирование** главного меню Центра управления, затем в управляющем меню слева выберите раздел **Ключи шифрования**.
2. Справа установите флаг для нужного объекта и нажмите **Экспортировать**.

Подключение в качестве новой станции («новичка»)

Если учетные данные станции на Сервере Dr.Web еще не создавались, пользователь может подключить свою станцию как новую самостоятельно. Для этого отправьте пользователю сертификат, а также адрес и порт подключения к Серверу Dr.Web. Вы также можете подключить станцию пользователя в качестве «новичка» самостоятельно, следуя инструкциям, приведенным в **Руководстве пользователя Dr.Web Desktop Security Suite (macOS)** и **Руководстве пользователя Dr.Web Server Security Suite (macOS)** (раздел «Режим централизованной защиты > Подключение в качестве «новичка»).

Чтобы скачать сертификат

1. Выберите пункт **Администрирование** главного меню Центра управления, затем в управляющем меню слева выберите раздел **Ключи шифрования**.
2. Справа установите флаг для нужного объекта и нажмите **Экспортировать**.

Автономный режим

Пользователь может отключить режим централизованной защиты и восстановить автономную работу Dr.Web. При этом восстанавливаются все настройки программы, заданные до перехода в централизованный режим, или настройки по умолчанию. Также возобновляется доступ ко всем компонентам Dr.Web.

5. Шифрование и сжатие трафика

Режим шифрования используется для обеспечения безопасности данных, передаваемых по небезопасному каналу, и позволяет избежать возможного разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищаемые станции.

Антивирусная сеть Dr.Web Enterprise Security Suite использует следующие криптографические средства:

- электронная цифровая подпись (ГОСТ Р 34.10-2001),
- асимметричное шифрование (VKO GOST R 34.10-2001 — RFC 4357),
- симметричное шифрование (ГОСТ 28147-89),
- криптографическая хеш-функция (ГОСТ Р 34.11-94).

Антивирусная сеть Dr.Web Enterprise Security Suite позволяет зашифровать трафик между Сервером Dr.Web и клиентами, к которым относятся:

- Агенты Dr.Web,
- инсталляторы Агентов Dr.Web,
- соседние Серверы Dr.Web,
- Прокси-серверы Dr.Web.

Ввиду того, что трафик между компонентами, в особенности между Серверами Dr.Web, может быть объемным, антивирусная сеть позволяет установить сжатие этого трафика. Настройка политики сжатия и совместимость таких настроек на разных клиентах аналогичны настройкам для шифрования.

Политика согласования настроек

Политика использования шифрования и сжатия настраивается отдельно на каждом из компонентов антивирусной сети, при этом настройки остальных компонентов должны быть согласованы с настройками Сервера Dr.Web.

При согласовании настроек шифрования и сжатия на Сервере Dr.Web и клиенте следует иметь ввиду, что ряд сочетаний настроек является недопустимым, и их выбор приведет к невозможности установки соединения между Сервером Dr.Web и клиентом.

В таблице 4-1 приведены сведения о том, при каких настройках соединение между Сервером Dr.Web и клиентом будет зашифрованным/сжатым (**+**), при каких — не зашифрованным/не сжатым (**–**), и о том, какие сочетания являются недопустимыми (**Ошибка**).

Таблица 4-1. Совместимость настроек политик шифрования и сжатия

Настройки клиента	Настройки Сервера Dr.Web		
	Да	**Возможно**	**Нет**
Да	+	+	Ошибка
Возможно	+	+	–
Нет	Ошибка	–	–

Использование шифрования трафика создает заметную вычислительную нагрузку на компьютеры с производительностью, близкой к минимально допустимой для установленных на них компонентов. В тех случаях, когда шифрование трафика не требуется для обеспечения дополнительной безопасности, можно отказаться от этого режима.

Для отключения режима шифрования следует последовательно переключать Сервер Dr.Web и компоненты сначала в режим **Возможно**, не допуская создания несовместимых пар клиент-Сервер Dr.Web.

Использование сжатия уменьшает трафик, но значительно увеличивает потребление оперативной памяти и вычислительную нагрузку на компьютеры, в большей степени, чем шифрование.

6. Работа в Мобильном режиме

Если рабочая станция пользователя долгое время не будет иметь связи с Сервером Dr.Web, для своевременного получения обновлений с серверов ВСО Dr.Web используется *Мобильный режим* работы Агента Dr.Web на станции.

Включение Мобильного режима в настройках Агента Dr.Web будет доступно при условии, что использование Мобильного режима разрешено в Центре управления в разделе **Антивирусная сеть** → **Права** → **macOS** → **Общие** → **Запуск в мобильном режиме**.

В Мобильном режиме Агент Dr.Web пытается подключиться к Серверу Dr.Web, делает три попытки и, если не удалось, выполняет HTTP-обновление с серверов ВСО Dr.Web. Попытки найти Сервер Dr.Web идут непрерывно с интервалом около минуты.

Во время функционирования Агента Dr.Web в Мобильном режиме связь Агента Dr.Web с Сервером Dr.Web прерывается. Все изменения, которые задаются на Сервере Dr.Web для такой станции, вступят в силу, как только Мобильный режим работы Агента Dr.Web будет отключен, и связь Агента Dr.Web с Сервером Dr.Web возобновится.

В мобильном режиме производится обновление только вирусных баз.

В Мобильном режиме функционирование Агента Dr.Web не ограничено по времени, однако обновление вирусных баз с ВСО Dr.Web осуществляется только до конца срока действия лицензионного ключа станции, информация о котором была сохранена Агентом Dr.Web при последнем подключении к Серверу Dr.Web (сам лицензионный ключ располагается на Сервере Dr.Web).

7. 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:

1. Ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/.
2. Прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/.
3. Посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

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

1. Заполните веб-форму в соответствующей секции раздела https://support.drweb.com/.
2. 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 https://company.drweb.com/contacts/offices/.