Dr.WEB

Enterprise Security Suite

Управление станциями под macOS

Dr.Web Enterprise Security Suite. Управление станциями под macOS
Версия 11.0.1
Руководство администратора
12.09.2018

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: https://www.drweb.com/

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

1.1. Назначение документа

Данное руководство является частью пакета документации администратора антивирусной сети, описывающей детали реализации комплексной антивирусной защиты компьютеров и мобильных устройств компании с помощью Dr.Web Enterprise Security Suite.

Руководство адресовано администратору антивирусной сети – сотруднику организации, которому поручено руководство антивирусной защитой рабочих станций и серверов этой сети.

В руководстве приведена информация о централизованной настройке антивирусного ПО рабочих станций, осуществляемой администратором антивирусной сети через Центр управления безопасностью Dr.Web. Руководство описывает настройки антивирусного решения Dr.Web для macOS и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- **Руководство пользователя** антивирусного решения Dr.Web для macOS содержит информацию о настройке антивирусного ПО, осуществляемой 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 и, в частности, по работе с Центром управления безопасностью Dr.Web.

Перед прочтением документов убедитесь, что это последняя версия руководств. Руководства постоянно обновляются, и последнюю их версию можно найти на официальном сайте компании «Доктор Веб» https://download.drweb.com/doc/.

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.
`C:\Windows\`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте Руководства будут употребляться без расшифровки следующие сокращения:

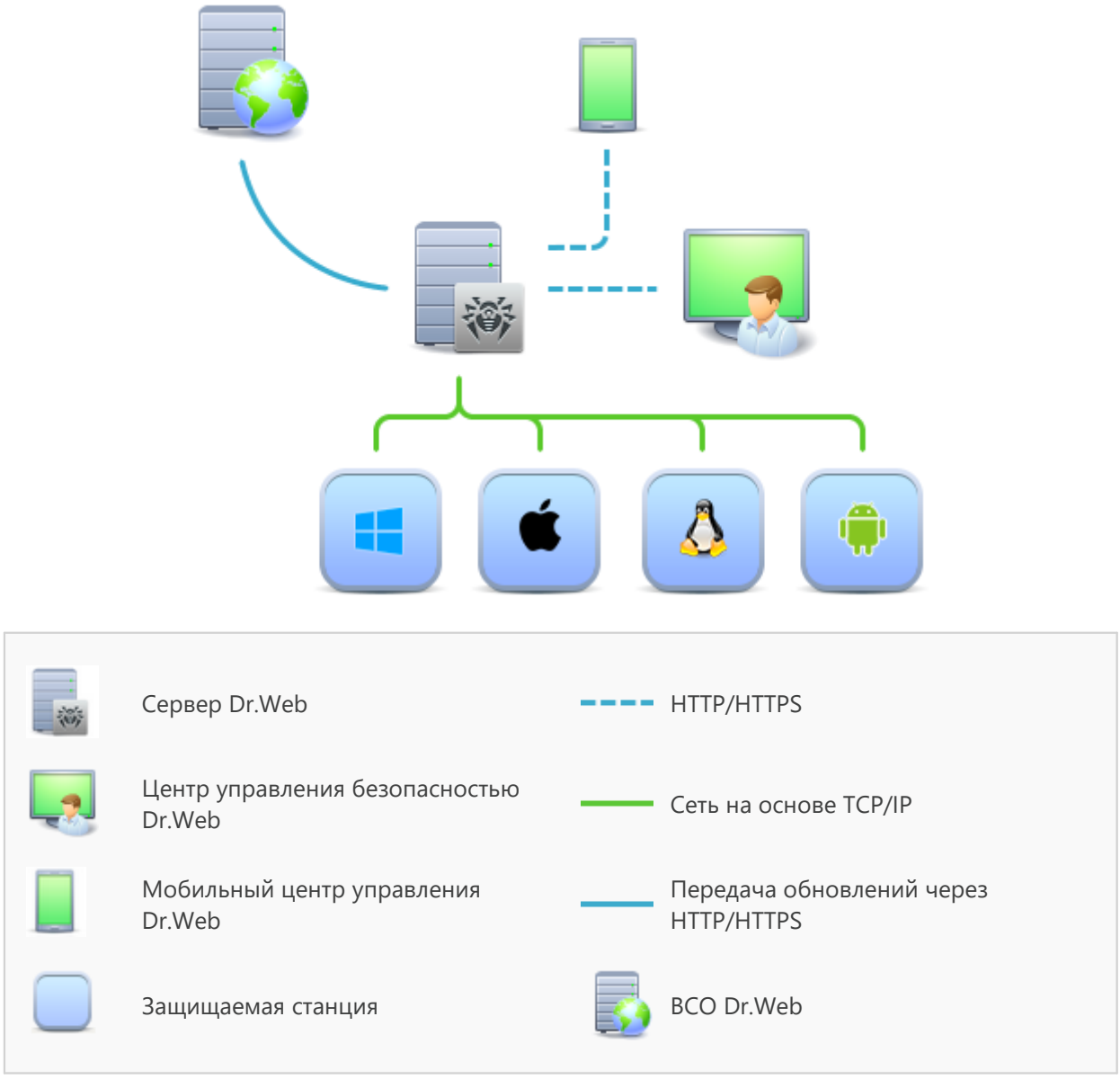
- ВСО Dr.Web – Всемирная Система Обновлений Dr.Web,
- ОС – Операционная Система,
- ПО – Программное Обеспечение.

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

Защита рабочих станций осуществляется антивирусными пакетами Dr.Web, разработанными для соответствующих операционных систем.

Защищаемый компьютер с установленным антивирусным пакетом, в соответствии с его функциями в антивирусной сети, именуется *рабочей станцией* антивирусной сети. Необходимо помнить, что по своим функциям в локальной сети такой компьютер может быть как рабочей станцией или мобильным устройством, так и сервером локальной сети.

Антивирусные пакеты устанавливаются на защищаемых станциях и подключаются к Серверу Dr.Web. Каждая станция входит в состав одной или нескольких групп, зарегистрированных на этом Сервере. Передача информации между станцией и Сервером осуществляется по протоколу, используемому в локальной сети (TCP/IP версии 4 или 6).

Установка

Локальная установка антивирусного пакета для macOS осуществляется на станции непосредственно. Может производится как администратором, так и пользователем.

Подробное описание процедур установки антивирусных пакетов на рабочие станции приведено в **Руководстве по установке** Dr.Web Enterprise Security Suite.

Управление

При поддержке связи с Сервером Dr.Web администратору доступны следующие функции, реализуемые антивирусным пакетом на станции:

- Централизованная настройка Антивируса на рабочих станциях при помощи Центра управления.

  При этом администратор может как запретить, так и оставить возможность пользователю самостоятельно изменять настройки Антивируса на станции.
- Настройка расписания антивирусных проверок и других заданий, выполняемых на станции.

- Получение статистики сканирования и прочей информации о работе антивирусных компонентов и о состоянии станции.
- Запуск и останов антивирусного сканирования и т.п.

Обновление

Сервер Dr.Web загружает обновления и распространяет их на подключенные к нему станции. Таким образом автоматически устанавливается, поддерживается и регулируется оптимальная стратегия защиты от угроз независимо от уровня квалификации пользователей рабочих станций.

В случае временного отключения рабочей станции от антивирусной сети, Антивирус на станции использует локальную копию настроек, антивирусная защита на рабочей станции сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии), но обновление ПО не производится. Если для станции разрешено функционирование в Мобильном режиме, при потере связи с Сервером будет доступно обновление вирусных баз непосредственно 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 надежно защищает компьютеры под управлением macOS и macOS Server от вирусов и прочих типов угроз.

Основные компоненты программы (*антивирусное ядро* и *вирусные базы*) являются не только крайне эффективными и нетребовательными к ресурсам, но и кросс-платформенными, что позволяет специалистам «Доктор Веб» создавать надежные антивирусные решения для различных операционных систем (ОС). Компоненты Dr.Web для macOS постоянно обновляются, а вирусные базы дополняются новыми сигнатурами, что обеспечивает защиту на наиболее современном уровне. Для дополнительной защиты от неизвестных вирусов используется эвристический анализатор.

3.1. Компоненты Dr.Web для macOS

Для защиты станций под macOS/macOS Server предоставляются следующие антивирусные компоненты:

Сканер Dr.Web, Dr.Web Agent Сканер

Сканирование компьютера по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления.

SpIDer Guard

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

SpIDer Gate

Проверка всех обращений к сайтам по протоколу HTTP. Нейтрализация угроз в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокировка доступа к подозрительным или некорректным ресурсам.

Карантин

Изоляция вредоносных и подозрительных объектов в специальном каталоге.

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 антивирусных компонентов 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 требуемый компонент:
   - 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
4. Откроется окно настроек антивирусного компонента.

   Управление настройками антивирусных компонентов через Центр управления имеет некоторые отличия от управления настройками непосредственно через соответствующие компоненты антивируса на станции:

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

     Установить в начальное значение – восстановить значение, которое параметр имел до редактирования (последнее сохраненное значение).

     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 значения, которые все параметры данного раздела имели до текущего редактирования (последние сохраненные значения).

     Установить все параметры в значения по умолчанию – установить для всех параметров данного раздела значения, заданные по умолчанию.

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

     Установить наследование настроек от первичной группы – удалить персональные настройки станций и установить наследование настроек данного раздела от первичной группы.

     Скопировать настройки из первичной группы и установить их в качестве персональных – скопировать настройки данного 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 данного раздела в файл специального формата.

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

5. После внесении каких-либо изменений в настройки при помощи Центра управления, для принятия этих изменений, 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 файловой системы или проверку только критических файлов и папок.

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

- Установите флаг **Проверять архивы**, чтобы включить проверку файлов в архивах.
- Установите флаг **Проверять почтовые файлы**, включить проверку содержимого почтовых файлов.
- В поле **Время проверки одного файла** укажите максимальное время проверки одного файла. Значение 0 указывает, что время проверки одного файла неограничено.

> 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 выберите действия, которые будут применяться к угрозам, обнаруженным Сканером Dr.Web, в зависимости от их типа:

- **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.

- **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.
- **Перемещать в карантин**. Обнаруженная угроза помещается в специальную папку, изолированную от остальной системы.
- **Удалять**. Наиболее эффективный способ устранения компьютерных угроз любых типов. Применение данного действия подразумевает полное удаление объекта, представляющего угрозу.
- **Игнорировать**. К объекту не применяется никакое действие, оповещение об обнаруженном объекте не появляется.

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

SpIDer Guard осуществляет постоянное сканирование файловой системы в режиме реального времени, проверяет файлы при изменении и сохранении, тем самым обеспечивая защиту системы от угроз безопасности.

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

- Установите флаг **Использовать эвристический анализ**, чтобы использовать эвристический анализатор для поиска неизвестных угроз.
- Установите/снимите флаг **Включить SpIDer Guard для macOS** (для серверов – **Включить SpIDer Guard для серверов macOS**), чтобы включить/отключить компонент SpIDer Guard.
- В поле **Время проверки одного файла** укажите максимальное время проверки одного файла. Значение 0 указывает, что время проверки одного файла неограничено.

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

Действия

В этом разделе выберите действия, которые будут применяться к угрозам, обнаруженным SpIDer Guard, в зависимости от их типа:

- **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.
- **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.
- **Перемещать в карантин**. Обнаруженная угроза помещается в специальную папку, изолированную от остальной системы.
- **Удалять**. Наиболее эффективный способ устранения компьютерных угроз любых типов. Применение данного действия подразумевает полное удаление объекта, представляющего угрозу.
- **Игнорировать**. К объекту не применяется никакое действие, оповещение об обнаруженном объекте не появляется.

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

Контейнеры

В этом разделе укажите максимальный уровень вложенности для проверяемых составных объектов. Если уровень вложенности будет превышать установленное значение, составные объекты будут пропускаться 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

Проверка веб-трафика и контроль доступа к интернет-ресурсам осуществляется при помощи компонента SplDer Gate. SplDer Gate проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих угрозы безопасности. Через протокол HTTP работают браузеры, менеджеры загрузки и многие другие приложения, обменивающиеся данными с веб-серверами, т.е. работающие с сетью Интернет.

SplDer Gate также позволяет контролировать доступ к интернет-ресурсам и тем самым оградить пользователей от нежелательных сайтов (например, сайтов, содержащих насилие, азартные игры, контент для взрослых 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

- Установите/снимите флаг **Включить SplDer Gate**, чтобы включить/отключить компонент SplDer Gate.
- Установите флаг **Использовать эвристический анализатор**, 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 неограничено.

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

Действия

- Установите/снимите флаг **Проверять получаемые файлы**, чтобы включить/отключить проверку входящего интернет-трафика.
- В списках **Блокировать файлы** и **Блокировать дополнительно** выберите типы небезопасных получаемых объектов, которые будут блокироваться компонентом SplDer Gate.

Веб-фильтр

- Установите/снимите флаг **Проверять URL**, чтобы включить/отключить блокировку интернет-ресурсов по категориям.
- Установите/снимите флаг **Блокировать нерекомендуемые сайты**, чтобы включить/отключить блокировку сайтов, на которых используются методы социальной инженерии для обмана посетителей.
- Установите/снимите флаг **Блокировать URL, добавленные по обращению правообладателя**, чтобы заблокировать/разрешить доступ к сайтам в связи с обращениями право-

обладателей, обнаруживших нарушения прав на интеллектуальную собственность в сети Интернет.

- В списке **Блокировать следующие категории сайтов** выберите категории интернет-ресурсов, доступ к которым необходимо заблокировать.
- В разделах **Белый список**/**Черный список** добавьте пути к сайтам, доступ к которым нужно разрешить/ограничить:
  - Чтобы добавить в список определенный сайт, введите его полный адрес (например, `www.example.com`). Доступ ко всем ресурсам, расположенным на этом сайте, будет определяться данной записью.
  - Чтобы настроить доступ к сайтам со схожими именами, введите общую часть их доменных имен. Пример: если вы введете текст `example`, то доступ к адресам `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru` и другим подобным сайтам будет определяться данной записью.
  - Чтобы настроить доступ к сайтам определенного домена, укажите имя домена с символом «**.**». В таком случае доступ ко всем ресурсам, находящиеся на этом домене, будет определяться данной записью. Если при указании домена используется символ прямого слэша «**/**», 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`, SplDer Gate будет определять доступ к страницам таким как `example.com/test11`, `template.example.com/test22` и т.п.

Контейнеры

В этом разделе укажите максимальный уровень вложенности для проверяемых составных объектов. Если уровень вложенности будет превышать установленное значение, составные объекты будут пропускаться 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

- **Исполняемый файл** – путь к исполняемому файлу SplDer Gate.
- **Уровень журнала** – определяет уровень подробности ведения журнала компонентом SplDer Gate.
- **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** – используется системный сервис `syslog`. В случае выбора этого метода необходимо также указать в выпадающем списке **Подсистема syslog** используемую **`syslog`** подсистему (метку) для сохранения сообщений от SplDer Gate.
- **Path** – сообщения журнала от SplDer Gate сохраняются в отдельный заданный файл. В случае выбора этого метода необходимо указать путь к файлу в поле **Файл журнала**.

Приложение А. 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 https://support.drweb.com/show_faq/;
- 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»:

- заполните веб-форму в соответствующей секции раздела https://support.drweb.com/;
- 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/.