



Dr.WEB

Enterprise Security Suite

Управление Dr.Web для Linux



© «Доктор Веб», 2021. Все права защищены

Настоящий документ носит информационный и справочный характер в отношении указанного в нем программного обеспечения семейства Dr.Web. Настоящий документ не является основанием для исчерпывающих выводов о наличии или отсутствии в программном обеспечении семейства Dr.Web каких-либо функциональных и/или технических параметров и не может быть использован при определении соответствия программного обеспечения семейства Dr.Web каким-либо требованиям, техническим заданиям и/или параметрам, а также иным документам третьих лиц.

Материалы, приведенные в данном документе, являются собственностью ООО «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, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «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 ООО «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 Dr.Web для Linux

Версия 11.0.2

Руководство администратора

26.05.2021

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Россия, Москва, 3-я улица Ямского поля, вл.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

Глава 1. Введение	5
1.1. Назначение документа	5
1.2. Условные обозначения и сокращения	6
Глава 2. Dr.Web Enterprise Security Suite	7
2.1. О продукте	7
2.2. Защита станций сети	8
Глава 3. Dr.Web для Linux	10
3.1. Компоненты Dr.Web для Linux	11
3.2. Настройка Dr.Web для Linux	13
3.2.1. Настройки Сканера для рабочих станций	14
3.2.2. Настройки SplDer Guard	16
3.2.3. Настройки SplDer Gate	19
3.2.4. Настройки Агента Dr.Web для UNIX	21
3.2.5. Настройки File Checker	23
3.2.6. Настройки Scanning Engine	24
3.2.7. Настройки Dr.Web ConfigD	25
Приложение А. Техническая поддержка	27



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 Linux и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- **Руководство пользователя** антивирусного решения Dr.Web для Linux 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 веб-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.
<i>Антивирусная сеть</i>	Новый термин или акцент на термине в описаниях.
<code><IP-address></code>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
<code>/home/user</code>	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:

- HTTP — протокол передачи гипертекста (HyperText Transfer Protocol),
- HTTPS — защищенный протокол передачи гипертекста (Hypertext Transfer Protocol Secure),
- IP — протокол Интернета (Internet Protocol),
- LKM — модуль ядра Linux (Linux Kernel Module),
- TCP — протокол управления передачи (Transmission Control Protocol),
- URL — единообразный локатор ресурса (Uniform Resource Locator),
- ВСО — Всемирная Система Обновлений Dr.Web,
- ЛВС — Локальная Вычислительная Сеть,
- ОС — Операционная Система,
- ПО — Программное Обеспечение.

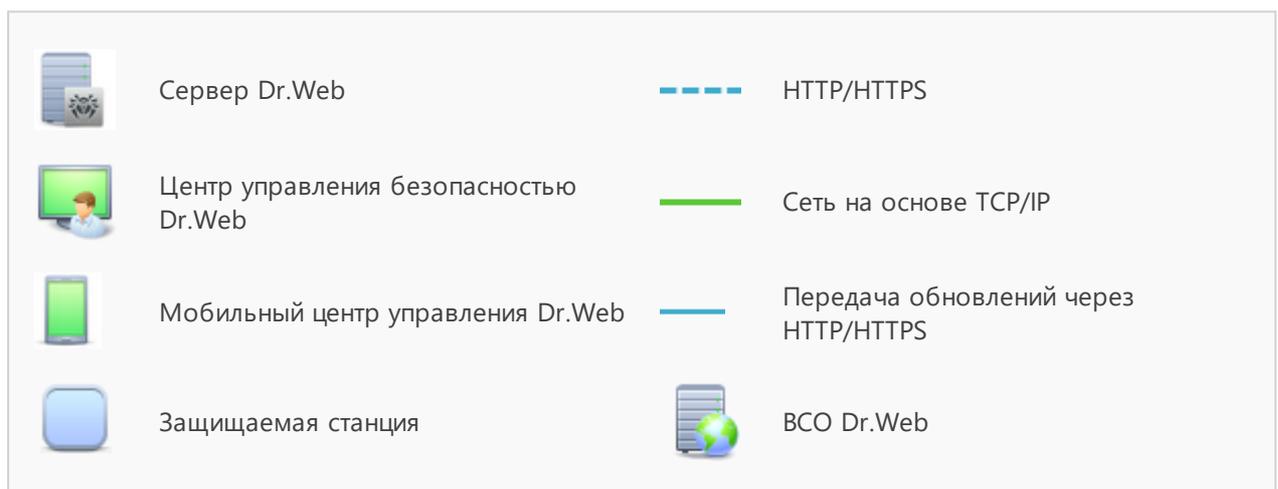
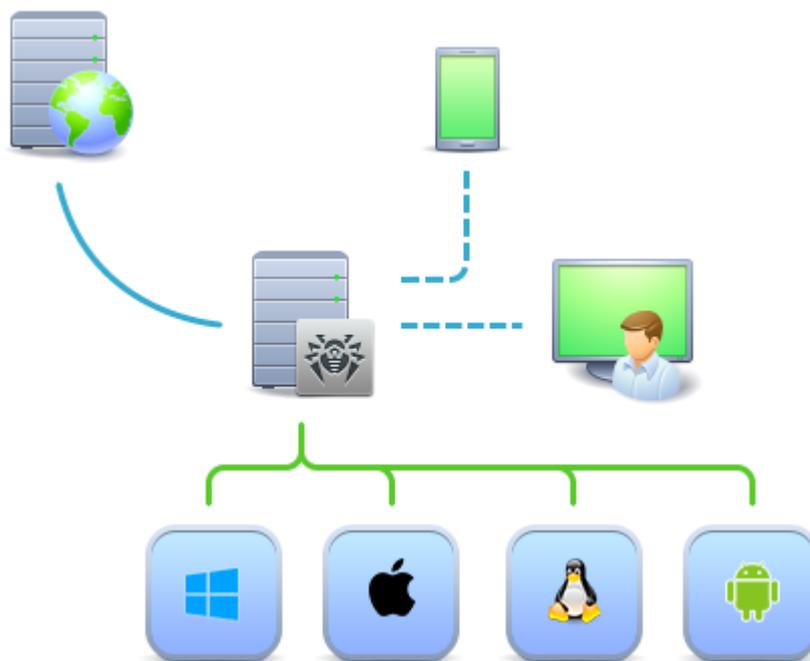


Глава 2. Dr.Web Enterprise Security Suite

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 осуществляется на компьютере пользователя непосредственно. Может производиться 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 антивирусного пакета на рабочих станциях при помощи Центра управления безопасностью.

При этом администратор может как запретить, так и оставить возможность пользователю самостоятельно изменять настройки антивирусного пакета 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. (в зависимости от функциональных возможностей антивирусного пакета, установленного на станции).

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, антивирусный пакет 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 BCO Dr.Web.



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



Глава 3. Dr.Web для Linux

В настоящем документе рассматриваются аспекты настройки компонентов, входящих в продукт Dr.Web для Linux, предназначенный для работы в ОС **GNU/Linux**. Руководство адресовано лицу, отвечающему за антивирусную безопасность и настройку сетей, называемому в данном руководстве «Администратором».

Основные функции продукта Dr.Web для Linux:

1. **Поиск и обезвреживание угроз.** Обнаруживаются и обезвреживаются как непосредственно вредоносные программы всех возможных типов (различные вирусы, включая вирусы, инфицирующие почтовые файлы и загрузочные записи дисков, троянские программы, почтовые черви и т. п.), так и нежелательные программы (рекламные программы, программы-шутки, программы автоматического дозвола).

Для обнаружения вредоносных и нежелательных программ используются:

- *Сигнатурный анализ.* Метод проверки, позволяющий обнаружить уже известные угрозы, информация о которых содержится в вирусных базах;
- *Эвристический анализ.* Набор методов проверки, позволяющих обнаруживать угрозы, которые еще неизвестны.
- *Обращение к сервису Dr.Web Cloud,* собирающему свежую информацию об актуальных угрозах, рассылаемую различными антивирусными продуктами Dr.Web.

Обратите внимание, что эвристический анализатор может ложно реагировать на программное обеспечение, не являющегося вредоносным. Поэтому объекты, содержащие обнаруженные им угрозы, получают специальный статус «подозрительные». Рекомендуется помещать такие файлы в карантин, а также передавать на анализ в антивирусную лабораторию «Доктор Веб».

Проверка файловой системы может запускаться как вручную, по запросу пользователя, так и автоматически — в соответствии с заданным расписанием. Имеется возможность как полной проверки всех объектов файловой системы, доступных пользователю, так и выборочной проверки только указанных объектов (отдельных каталогов или файлов). Кроме того, доступна возможность отдельной проверки загрузочных записей томов и исполняемых файлов, из которых запущены процессы, активные в системе в данный момент. В последнем случае при обнаружении угрозы выполняется не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него.

2. **Мониторинг обращений к файлам.** Отслеживаются обращения к файлам с данными и попытки запуска исполняемых файлов. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках инфицирования ими компьютера.
3. **Мониторинг доступа к сети Интернет.** Отслеживаются попытки обращения к серверам в сети Интернет (веб-серверам, почтовым серверам, файловым серверам)



для блокировки доступа пользователя к веб-сайтам, отмеченным как нежелательные для посещения, а также для предотвращения получения и отправки сообщений электронной почты, содержащих инфицированные файлы, нежелательные ссылки или классифицированных как спам. Проверка сообщений электронной почты и файлов, загружаемых по сети, на наличие в них вирусов и других угроз, производится «на лету». Для определения нежелательных ссылок используются как поставляемая вместе с Dr.Web для Linux автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, так и черные и белые списки, ведущиеся пользователем вручную. Дополнительно продукт обращается к сервису Dr.Web Cloud для проверки, не отмечен ли веб-сайт, к которому пытается обратиться пользователь, как вредоносный, другими антивирусными продуктами Dr.Web.

4. **Надежная изоляция инфицированных или подозрительных объектов** в специальном хранилище — карантине, чтобы они не могли нанести ущерба системе. При перемещении объектов в карантин они специальным образом переименовываются, и могут быть восстановлены в исходное место (в случае необходимости) только по команде пользователя.

3.1. Компоненты Dr.Web для Linux

Для защиты рабочих станций под управлением ОС **GNU/Linux** предоставляются следующие антивирусные компоненты:

Основные

Сканер для рабочих станций

Выполняет проверку объектов файловой системы (файлы, каталоги и загрузочные записи) и активных процессов на наличие угроз по требованию пользователя или по заданному расписанию.



В качестве Сканера для рабочих станций подразумевается версия Сканера, работающая в графической среде ОС. В состав Dr.Web для Linux входит также Консольный сканер, позволяющий запускать проверки из командной строки. Центр управления не управляет работой Консольного сканера.

SpIDer Guard

Компонент, работающий в резидентном режиме и отслеживающий операции с файлами (такие как создание, открытие, закрытие и запуск файла). Проверяет содержимое новых и изменившихся файлов, а также исполняемых файлов в момент запуска программ.

SpIDer Gate

Компонент, работающий в резидентном режиме и отслеживающий все сетевые соединения.



- Проверяет наличие URL в базах категорий веб-ресурсов и черных списках пользователя; блокирует доступ к веб-сайтам, если ведущие к ним URL зарегистрированы в черном списке пользователя или категориях, отмеченных как нежелательные для посещения.
- Блокирует отправку и прием сообщений электронной почты, если они содержат вредоносные объекты или нежелательные ссылки.
- Выполняет проверку файлов, загружаемых из сети Интернет (с серверов, доступ к которым был разрешен), и блокирует их загрузку, если они содержат угрозы.

Дополнительно, при наличии соответствующего разрешения от пользователя, посылает запрашиваемые им URL на проверку в сервис Dr.Web Cloud.

Консольный сканер (управляется только на станции)

Используется для запуска из командной строки ОС проверки объектов файловой системы, активных процессов, а также удаленной проверки узлов сети на наличие угроз.

Вспомогательные

Агент Dr.Web для UNIX

Вспомогательный компонент. Используется для взаимодействия Dr.Web для Linux, установленного на станции, с Dr.Web Enterprise Security Suite.

File Checker

Вспомогательный компонент. Используется Сканером для рабочих станций, Консольным сканером, SplDer Guard и SplDer Gate для проверки файлов и управления Карантином.

Scanning Engine

Вспомогательный компонент. Используется для антивирусной проверки и управления вирусными базами.

Dr.Web ConfigD

Вспомогательный компонент. Координирует работу всех компонентов Dr.Web для Linux.

Карантин

Используется Сканером для рабочих станций, Консольным сканером и SplDer Guard для изоляции вредоносных и подозрительных объектов.



Описание работы с Карантином через Центр управления приведено в **Руководстве администратора**.



В состав Dr.Web для Linux на станции могут входить также иные вспомогательные компоненты, не указанные в списке.

3.2. Настройка Dr.Web для Linux

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 ОС **Linux** или группы, содержащей такие станции.
3. В открывшемся управляющем меню в разделе **Конфигурация**, в подразделе **UNIX** выберите требуемый компонент.
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 внесения 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**). При этом редактировать настройки сможет только сам администратор через Центр управления.

3.2.1. Настройки Сканера для рабочих станций

В разделе **Сканер для рабочих станций** представлены следующие разделы настройки функционирования Dr.Web для Linux:

- **Общие** — общие настройки Сканера для рабочих станций.
- **Действия** — настройки действий при обнаружении угроз Сканером для рабочих станций.
- **Исключаемые пути** — настройки исключений в проверке файлов Сканером для рабочих станций.

3.2.1.1. Общие

В данном разделе вы можете управлять следующими параметрами Сканера для рабочих станций на защищаемой станции:

- **Время проверки одного файла** — определяет максимальный период времени, который отводится Сканеру для рабочих станций на проверку одного файла. Если указано 0, время проверки одного файла не ограничивается.

3.2.1.2. Действия

В данном разделе вы можете управлять параметрами, которые Сканер для рабочих станций будет применять при проверке файлов на защищаемой станции.

В качестве событий, на которые может реагировать Сканер для рабочих станций, доступны следующие:

- **Инфицированные** — в проверенном файле обнаружен известный вирус.
- **Подозрительные** — проверенный файл отмечен как *подозрительный*.
- **Рекламные программы** — в проверенном файле обнаружена рекламная программа.



- **Программы дозвола** — в проверенном файле обнаружена программа дозвола.
- **Программы-шутки** — в проверенном файле обнаружена программа-шутка.
- **Потенциально опасные** — в проверенном файле обнаружена потенциально-опасная программа.
- **Программы взлома** — в проверенном файле обнаружена программа взлома.

В качестве действий доступны следующие:

- *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 Карантин, изолированный от остальной системы.
- *Удалять* — наиболее эффективный способ устранения компьютерных угроз любых типов. Применение данного действия подразумевает полное удаление объекта, представляющего угрозу.
- *Сообщать* — выдать пользователю сообщение об обнаруженной угрозе.

Дополнительно доступны следующие параметры антивирусной защиты:

- **Автоматически применять действия к угрозам** — если флажок снят, то Сканер для рабочих станций будет только информировать пользователя об обнаруженной угрозе, предлагая ему выбрать требуемое действие из доступных.
- **Архивы** — управляет возможностью проверки содержимого архивов. Если флажок снят, архивы проверяются Сканером для рабочих станций как обычные файлы, без анализа их внутренней структуры.
- **Почтовые файлы** — управляет возможностью проверки содержимого почтовых файлов (сообщения электронной почты, почтовые ящики). Если флажок снят, почтовые файлы проверяются Сканером для рабочих станций как обычные файлы, без анализа их внутренней структуры.

3.2.1.3. Исключаемые пути

В данном разделе вы можете управлять списком путей к каталогам и файлам на защищаемой станции, которые будут пропускаться при проверке Сканером для рабочих станций объектов файловой системы.

Исключаемые пути указываются в поле **Исключаемые пути** (по одному пути на строку).



Для добавления нового пути в список нажмите кнопку . Для удаления некоторого пути из списка нажмите кнопку  в соответствующей строке списка.

3.2.2. Настройки SplDer Guard



Монитор файловой системы SplDer Guard может использовать два режима работы:

- **FANOTIFY** — работа через системный механизм **fanotify** (поддерживается не всеми ОС семейства **GNU/Linux**)
- **LKM** — работа с использованием загружаемого модуля ядра **Linux** (может быть использован в любой ОС семейства **GNU/Linux** с ядром версии 2.6.x и новее)

По умолчанию монитор файловой системы автоматически выбирает подходящий режим работы, исходя из возможностей окружения. В случае если SplDer Guard не запускается, выполните на защищаемой станции сборку и установку загружаемого модуля ядра из поставляемых исходных кодов.

В разделе **SplDer Guard** представлены следующие разделы настройки функционирования Dr.Web для Linux:

- [Общие](#) — общие настройки SplDer Guard.
- [Действия](#) — настройки действий при обнаружении угроз SplDer Guard.
- [Контейнеры](#) — настройки проверки составных объектов (архивов, почтовых файлов и т. п.).
- [Пути проверки](#) — настройки исключений в проверке файлов.
- [Дополнительно](#) — дополнительные настройки SplDer Guard.

3.2.2.1. Общие

В данном разделе вы можете управлять следующими параметрами SplDer Guard на защищаемой станции:

- **Включить SplDer Guard для Linux** — управляет запуском SplDer Guard на защищаемой станции.
- **Использовать эвристический анализ** — управляет использованием SplDer Guard на защищаемой станции эвристического анализа при проверке файлов «на лету». Использование эвристического анализа замедляет проверку, но повышает ее надежность.
- **Время проверки одного файла** — определяет максимальный период времени, который отводится на проверку одного файла SplDer Guard на станции. Если указано 0, время проверки одного файла не ограничивается.



3.2.2.2. Действия

В данном разделе вы можете управлять параметрами антивирусной защиты, которые SpliDer Guard будет применять при проверке файлов.

В качестве событий, на которые может реагировать SpliDer Guard, доступны следующие:

- **Инфицированные** — в проверенном файле обнаружен известный вирус.
- **Подозрительные** — проверенный файл отмечен как *подозрительный*.
- **Рекламные программы** — в проверенном файле обнаружена рекламная программа.
- **Программы дозвона** — в проверенном файле обнаружена программа дозвона.
- **Программы-шутки** — в проверенном файле обнаружена программа-шутка.
- **Потенциально опасные** — в проверенном файле обнаружена потенциально опасная программа.
- **Программы взлома** — в проверенном файле обнаружена программа взлома.

В качестве действий доступны следующие:

- *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 Карантин, изолированный от остальной системы.
- *Удалять* — наиболее эффективный способ устранения компьютерных угроз любых типов. Применение данного действия подразумевает полное удаление объекта, представляющего угрозу.
- *Сообщать* — выдать пользователю сообщение об обнаруженной угрозе.

3.2.2.3. Контейнеры

В данном разделе вы можете управлять параметрами проверки SpliDer Guard составных файлов, таких, как архивы, почтовые файлы, упакованные объекты и прочие контейнеры (т. е. составные файлы, не отнесенные ни к одному из предыдущих типов).

Для каждого типа файла в соответствующем поле можно указать максимально допустимый уровень вложенности, ниже которого он не должен распаковываться при проверке SpliDer Guard. Например, чтобы проверять содержимое архивов, вложенных в



архивы, необходимо указать уровень вложенности для них не менее 2. Чтобы запретить проверку вложенных объектов, укажите уровень вложенности 0 для соответствующего типа контейнеров.

Помните, что увеличение допустимого уровня вложенности уменьшает скорость проверки.

Поле **Максимальный коэффициент сжатия архива** устанавливает максимальную допустимую степень сжатия проверяемых объектов (как отношение сжатого объема файла к несжатому). Если степень сжатия проверяемого объекта превысит указанную величину, он будет пропущен при проверке.

3.2.2.4. Пути проверки

В данном разделе вы можете управлять списками путей к каталогам и файлам на защищаемой станции, которые будут проверяться или пропускаться SplDer Guard при мониторинге файловой системы.

Исключаемые пути указываются в поле **Исключаемые пути** (по одному пути на строку). Файлы и каталоги, попавшие в список исключаемых путей, не контролируются монитором SplDer Guard.

Исключаемые процессы указываются в поле **Исключаемые процессы** (по одному на строку). Обращения к файлам, инициированные процессами (программами), включенными в этот список, не контролируются монитором SplDer Guard. Для каждого исключаемого процесса необходимо указать полный путь к его исполняемому файлу на защищаемой станции.

Пути, подлежащие проверке на защищаемой станции, указываются в поле **Проверяемые пути** (по одному пути на строку). Монитор SplDer Guard будет контролировать обращение только к тем файлам, которые находятся в проверяемых путях и не находятся в путях из списка **Исключаемые пути**.

Для добавления нового пути в нужный список нажмите кнопку  в соответствующей строке списка. Для удаления некоторого пути из списка нажмите кнопку  в соответствующей строке списка.

3.2.2.5. Дополнительно

В данном разделе вы можете управлять дополнительными настройками работы SplDer Guard на защищаемой станции.

Доступны следующие дополнительные настройки SplDer Guard:

- **Режим работы** — управляет способом работы SplDer Guard на защищаемой станции: через модуль ядра Linux (LKM), через службу **fanotify** или в режиме автоматического определения наиболее подходящего способа. Рекомендуется оставлять режим *AUTO*.



- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом SplDer Guard.
- **Метод ведения журнала** — управляет способом сохранения сообщений SplDer Guard в журнал. Возможные значения:
 - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
 - *Syslog* — используется системный сервис **syslog** для ведения журнала SplDer Guard. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от SplDer Guard.
 - *Path* — сообщения журнала от SplDer Guard сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

3.2.3. Настройки SplDer Gate

В разделе **SplDer Gate** представлены следующие разделы настройки функционирования Dr.Web для Linux:

- [Общие](#) — общие настройки SplDer Gate.
- [Действия](#) — настройки действий при обнаружении угроз SplDer Gate.
- [Веб-фильтр](#) — настройки проверки веб-трафика и контроль доступа к интернет-ресурсам компонентом SplDer Gate.
- [Контейнеры](#) — настройки проверки составных объектов (архивов, почтовых файлов и т. п.).
- [Дополнительно](#) — дополнительные настройки SplDer Gate.

3.2.3.1. Общие

В данном разделе вы можете управлять следующими параметрами SplDer Gate на защищаемой станции:

- **Включить SplDer Gate** — управляет запуском SplDer Gate на защищаемой станции.
- **Использовать эвристический анализ** — управляет использованием SplDer Gate на защищаемой станции эвристического анализа для поиска неизвестных угроз. Использование эвристического анализа замедляет проверку, но повышает ее надежность.
- **Время проверки одного файла** — определяет максимальный период времени, который отводится на проверку одного файла SplDer Guard на станции. Если указано 0, время проверки одного файла не ограничивается.



3.2.3.2. Действия

В данном разделе вы можете управлять следующими параметрами SpIDer Gate на защищаемой станции:

- Установите флаг **Проверять получаемые файлы**, чтобы включить проверку входящего интернет-трафика (в частности — файлов, загруженных из Интернет).
- В списках **Блокировать файлы** и **Блокировать дополнительно** выберите типы небезопасных получаемых объектов, которые будут блокироваться компонентом SpIDer Gate.

3.2.3.3. Веб-фильтр

В данном разделе вы можете управлять следующими параметрами SpIDer Gate на защищаемой станции:

- Установите флажок **Проверять URL**, чтобы включить блокировку интернет-ресурсов по категориям.
- Установите флажок **Блокировать nereкомендуемые сайты**, чтобы включить блокировку сайтов, на которых используются методы социальной инженерии для обмана посетителей.
- Установите флажок **Блокировать URL, добавленные по обращению правообладателя**, чтобы заблокировать доступ к сайтам в связи с обращениями правообладателей, 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 полный адрес его домена (например, `www.example.com`). Доступ ко всем ресурсам, расположенным на этом домене, будет определяться данной записью.
 - Чтобы настроить доступ к веб-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 веб-сайтам будет определяться данной записью.
 - Чтобы настроить доступ к веб-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`, SpIDer Gate будет определять доступ к веб-страницам таким как `example.com/test11`, `template.example.com/test22` и т. п.



3.2.3.4. Контейнеры

В данном разделе вы можете управлять параметрами проверки SplDer Gate составных файлов, таких, как архивы, почтовые файлы, упакованные объекты и прочие контейнеры (т. е. составные файлы, не отнесенные ни к одному из предыдущих типов).

Для каждого типа файла в соответствующем поле можно указать максимально допустимый уровень вложенности, ниже которого он не должен распаковываться при проверке SplDer Gate. Например, чтобы проверять содержимое архивов, вложенных в архивы, необходимо указать уровень вложенности для них не менее 2. Чтобы запретить проверку вложенных объектов, укажите уровень вложенности 0 для соответствующего типа контейнеров.

Помните, что увеличение допустимого уровня вложенности уменьшает скорость проверки.

Поле **Максимальный коэффициент сжатия архива** устанавливает максимальную допустимую степень сжатия проверяемых объектов (как отношение сжатого объема файла к несжатому). Если степень сжатия проверяемого объекта превысит указанную величину, он будет пропущен при проверке.

3.2.3.5. Дополнительно

В данном разделе вы можете управлять дополнительными настройками работы SplDer Gate на защищаемой станции.

Доступны следующие дополнительные настройки SplDer Gate:

- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом SplDer Gate.
- **Метод ведения журнала** — управляет способом сохранения сообщений SplDer Gate в журнал. Возможные значения:
 - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
 - *Syslog* — используется системный сервис **syslog** для ведения журнала SplDer Gate. В случае выбора этого значения 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 файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

3.2.4. Настройки Агента Dr.Web для UNIX

В разделе **Агент Dr.Web** представлены следующие разделы настройки функционирования Dr.Web для Linux:



- [Общие](#) — настройки Агента Dr.Web для UNIX.
- [Конфигурация](#) — редактор настроек всех компонентов Dr.Web для Linux.

3.2.4.1. Общие

В данном разделе вы можете управлять настройками работы на защищаемой станции вспомогательного компонента Агент Dr.Web для UNIX. Доступны следующие настройки:

- **Периодичность отправки статистики** — определяет периодичность, с которой Агент Dr.Web для UNIX отправляет статистику на сервер.
- **Мобильный режим получения обновлений** — определяет режим использования мобильного режима получения обновлений. Возможные значения:
 - *Автоматически* — использовать мобильный режим, если он разрешен администратором на сервере Dr.Web Enterprise Security Suite (получать обновления с серверов BCO, используя локальный компонент обновления, работающий на станции, либо получать обновления от Dr.Web Enterprise Security Suite, в зависимости от того, какое соединение доступно и качество какого соединения лучше).
 - *Использовать* — использовать мобильный режим, если он разрешен администратором на сервере Dr.Web Enterprise Security Suite (получать обновления с серверов BCO, используя локальный компонент обновления, работающий на станции).
 - *Запретить* — не разрешать Dr.Web для Linux на станции получать обновления с серверов BCO в случае невозможности подключения к серверу Dr.Web Enterprise Security Suite.
- **Обрабатывать discovery-запросы** — установите флаг, чтобы разрешить агенту принимать discovery-запросы от сервера Dr.Web Enterprise Security Suite (используются для проверки структуры и состояния антивирусной сети).
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Агент Dr.Web для UNIX.
- **Метод ведения журнала** — управляет способом сохранения сообщений Агентом Dr.Web для UNIX в журнал. Возможные значения:
 - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
 - *Syslog* — используется системный сервис **syslog** для ведения журнала Агента Dr.Web для UNIX. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от Агента Dr.Web для UNIX.
 - *Path* — сообщения журнала от Агента Dr.Web для UNIX сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.



Как правило, для настроек этого компонента по умолчанию заданы оптимальные значения, изменять которые не рекомендуется без необходимости.

3.2.4.2. Конфигурация

В данном разделе вы можете задавать (в формате ini-файла конфигурации) настройки для любого из компонентов Dr.Web для Linux, установленного на станции.

Для этого внесите необходимые изменения в поле **Конфигурационный файл drweb.ini**.

Обратите внимание, что:

- В редакторе настроек отображаются только те параметры конфигурации, значения которых были изменены на этой странице.
- Значения параметров конфигурации, указанные в редакторе, имеют приоритет по отношению к значениям настроек, задаваемых на страницах настроек компонентов: в случае если на странице настройки задано одно значение некоторого параметра, а на странице **Конфигурация** — другое, на станции будет использовано значение, указанное на странице **Конфигурация**. В частности, для компонентов, секции которых указаны в редакторе **Конфигурационный файл drweb.ini**, значения не указанных параметров конфигурации принимают значения по умолчанию.
- Редактор настроек поддерживает контекстную подсказку: нажатие комбинации клавиш CTRL+SPACE открывает выпадающий список доступных параметров (или секций параметров, в зависимости от контекста).
- Имеется возможность экспорта и импорта содержимого редактора в виде заполненного файла конфигурации `.ini`. Для импорта или экспорта настроек в виде файла конфигурации `.ini` нажмите соответствующие кнопки, расположенные на странице над редактором настроек.



Для получения полного перечня компонентов на станции, доступных для настройки, а также для ознакомления с описанием их параметров в конфигурационном файле `drweb.ini` обратитесь к руководству пользователя или руководству администратора продукта, установленного на станции.

3.2.5. Настройки File Checker

В данном разделе вы можете управлять настройками работы на защищаемой станции вспомогательного компонента File Checker.

Доступны следующие настройки:

- **Размер кэша проверенных файлов** — определяет размер кэша, в котором File Checker временно сохраняет результаты проверки файлов.



- **Период актуальности кэша** — определяет период времени, в течении которого File Checker не проверяет файлы повторно, если информация об их проверке уже содержится в кэше.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом File Checker.
- **Метод ведения журнала** — управляет способом сохранения сообщений File Checker в журнал. Возможные значения:
 - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
 - *Syslog* — используется системный сервис **syslog** для ведения журнала File Checker. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от File Checker.
 - *Path* — сообщения журнала от File Checker сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

Также вы можете указать, какую дополнительную информацию следует записывать в журнал, если он ведется на уровне *Отладка*.

- **IPC** — сохранять в журнал все сообщения внутреннего протокола взаимодействия компонентов.
- **Проверка файлов** — сохранять в журнал сведения о проверке файлов.
- **Мониторинг файлов SplDer Guard** — сохранять в журнал сведения о запросах от SplDer Guard.
- **Состояние кэша проверенных файлов** — сохранять в журнал сведения о состоянии кэша проверенных файлов.



Как правило, для настроек этого компонента по умолчанию заданы оптимальные значения, изменять которые не рекомендуется без необходимости.

3.2.6. Настройки Scanning Engine

В данном разделе вы можете управлять настройками работы на защищаемой станции вспомогательного компонента Scanning Engine.

Доступны следующие настройки:

- **Путь к файлу сокета фиксированной копии компонента** — определяет путь к файлу UNIX-сокета постоянно работающей копии Scanning Engine. Этот сокет может использоваться для сканирования файлов внешними программами. Если параметр пуст, сканирование недоступно для внешних программ, а Scanning Engine запускается и завершает свою работу автоматически, по мере необходимости.
- **Количество сканирующих процессов** — определяет количество вспомогательных процессов, которые Scanning Engine может создать при сканировании файлов. При



изменении значения этого параметра следует учесть количество процессорных ядер, доступных на защищаемой станции.

- **Сторожевой таймер** — определяет период времени, который Scanning Engine использует для автоматического обнаружения зависания вспомогательных сканирующих процессов.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Scanning Engine.
- **Метод ведения журнала** — управляет способом сохранения сообщений Scanning Engine в журнал. Возможные значения:
 - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
 - *Syslog* — используется системный сервис **syslog** для ведения журнала Scanning Engine. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от Scanning Engine.
 - *Path* — сообщения журнала от Scanning Engine сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.



Как правило, для настроек этого компонента по умолчанию заданы оптимальные значения, изменять которые не рекомендуется без необходимости.

3.2.7. Настройки Dr.Web ConfigD

В данном разделе вы можете управлять настройками работы на защищаемой станции вспомогательного управляющего компонента Dr.Web ConfigD.

Доступны следующие настройки:

- **Путь к публичному коммуникационному сокету** — определяет путь к UNIX-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web для Linux.
- **Путь к административному коммуникационному сокету** — определяет путь к UNIX-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web для Linux, работающими с полномочиями суперпользователя.
- **Путь к каталогу временных файлов** — определяет каталог, в котором компоненты Dr.Web для Linux хранят свои временные файлы.
- **Путь к каталогу PID-файлов и файлов коммуникационных сокетов** — определяет каталог, в котором компоненты Dr.Web для Linux хранят PID-файлы и UNIX-сокеты для внутреннего взаимодействия.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Dr.Web ConfigD.



- **Метод ведения журнала** — управляет способом сохранения сообщений Dr.Web ConfigD в журнал. Возможные значения:
 - *Syslog* — используется системный сервис **syslog** для ведения журнала Dr.Web ConfigD. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от Dr.Web ConfigD.
 - *Path* — сообщения журнала от Dr.Web ConfigD сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.



Как правило, для настроек этого компонента по умолчанию заданы оптимальные значения, изменять которые не рекомендуется без необходимости.



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/>.

