Dr.WEB

Enterprise Security Suite

Управление Dr.Web для файловых серверов UNIX

Dr.Web Enterprise Security Suite. Управление Dr.Web для файловых серверов UNIX
Версия 12.0
Руководство администратора
25.05.2021

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

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 файловых серверов UNIX и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- **Руководство администратора** антивирусного решения Dr.Web для файловых серверов UNIX 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.
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.
`/home/user`	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:

- DNS — система доменных имен (Domain Name System),
- FQDN — полностью определенное имя домена (Fully Qualified Domain Name),
- FTP — протокол передачи файлов (File Transfer Protocol),
- HTML — язык разметки гипертекста (HyperText Markup Language),
- HTTP — протокол передачи гипертекста (HyperText Transfer Protocol),
- HTTPS — защищенный протокол передачи гипертекста (Hypertext Transfer Protocol Secure),
- IP — протокол Интернета (Internet Protocol),
- LKM — Linux Kernel Module,
- MBR — главная загрузочная запись (Master Boot Record),
- SMB — Server Message Block (протокол доступа к файлам),
- SNI — индикация имени сервера (Server Name Indication),

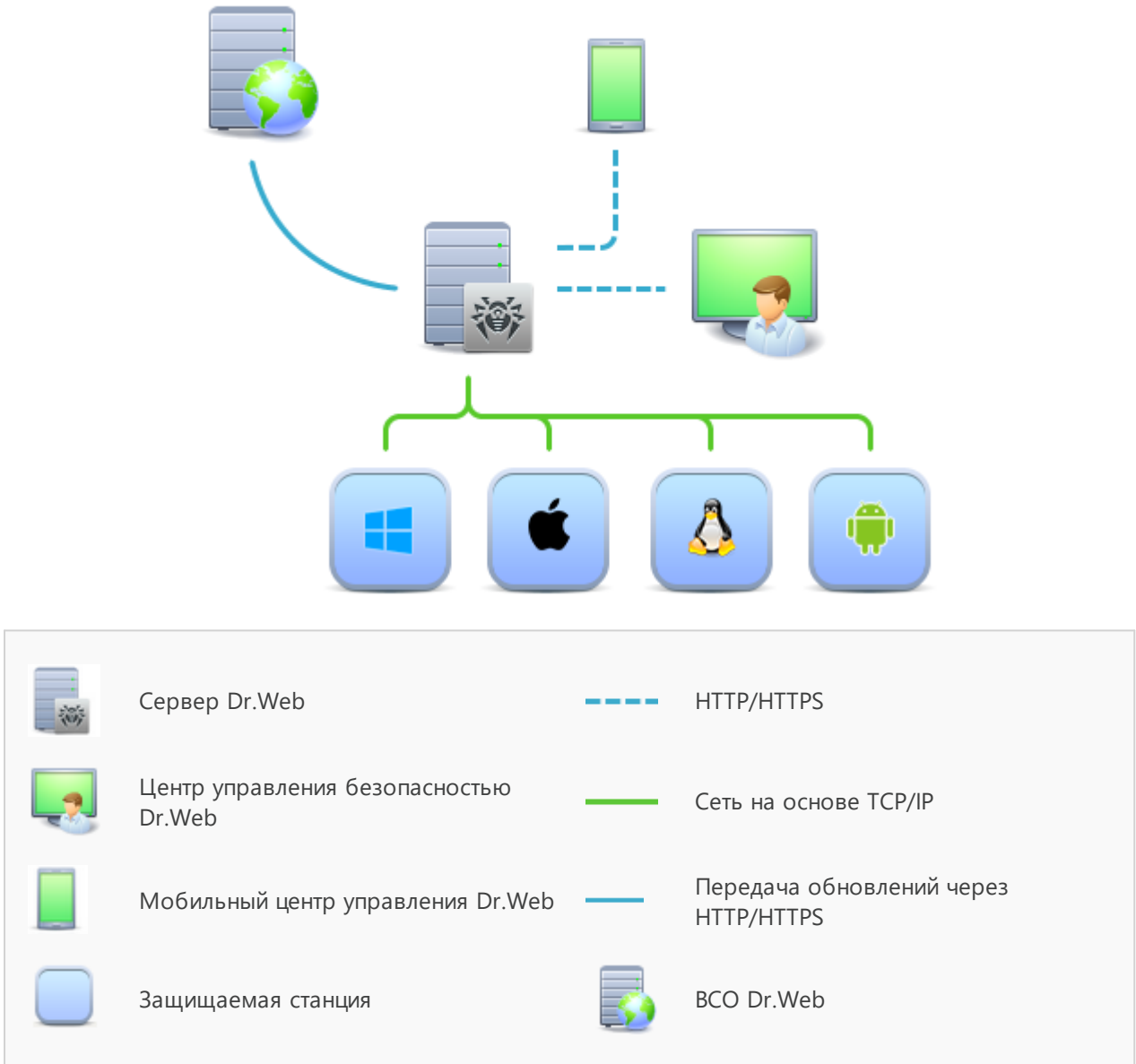
- SSL — уровни защищенных сокетов (Secure Socket Layers),
- TCP — протокол управления передачи (Transmission Control Protocol),
- TLS — защищенный транспортный уровень (Transport Layer Security),
- URL — единообразный локатор ресурса (Uniform Resource Locator),
- ВСО — Всемирная Система Обновлений Dr.Web,
- ЛВС — Локальная Вычислительная Сеть,
- ОС — Операционная Система,
- ПО — Программное Обеспечение,
- ФС — Файловая Система.

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 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 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 ВСО Dr.Web.

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

Глава 3. Dr.Web для файловых серверов UNIX

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

Dr.Web для файловых серверов UNIX создан для защиты файловых серверов, работающих под управлением ОС семейства UNIX (**GNU/Linux** и **FreeBSD**) от вирусов и всех прочих видов вредоносного программного обеспечения, а также для предотвращения распространения через них угроз, разработанных для различных платформ.

Основные функции Dr.Web для файловых серверов UNIX:

1. **Поиск и обезвреживание угроз.** Производится поиск как непосредственно вредоносных программ всех возможных типов (различные вирусы, включая вирусы, инфицирующие почтовые файлы и загрузочные записи дисков, троянские программы, почтовые черви и т. п.), так и нежелательных программ (рекламные программы, программы-шутки, программы автоматического дозвона).

   Для обнаружения угроз 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».

   При проверке файловой системы по запросу пользователя имеется возможность как полной проверки всех объектов файловой системы, доступных пользователю, так и выборочной проверки только указанных объектов (отдельных каталогов или файлов, соответствующих указанным критериям). 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:**

- **В файловой системе ОС.** Отслеживаются обращения к файлам с данными и попытки запуска исполняемых файлов. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках инфицирования ими файловой системы сервера.
- **В разделяемых каталогах Samba.** Отслеживаются обращения локальных и удаленных пользователей файлового сервера к файлам как на запись, так и на чтение. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках сохранения их в хранилище, что предотвращает их дальнейшее распространение по сети.
- **На томах Novell Storage Services.** Отслеживаются обращения пользователей файлового хранилища NSS к файлам на запись. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках сохранения их в хранилище NSS, что предотвращает их дальнейшее распространение по сети.

Обратите внимание, что функция мониторинга файловой системы доступна только для ОС семейства **GNU/Linux**, а функция мониторинга томов **Novell Storage Services** доступна только для **Novell Open Enterprise Server** SP2 на базе операционной системы **SUSE Linux Enterprise Server** 10 SP3 или старше. В других ОС компоненты, предоставляющие указанные функции, не поставляются.

3. **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 файловых серверов UNIX

Для защиты интернет-шлюзов UNIX-систем предоставляются следующие антивирусные компоненты:

Основные

*SpIDer Guard (для ОС **GNU/Linux**)*

Монитор файловой системы ОС **GNU/Linux**. Работает в резидентном режиме и отслеживает 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 Guard для SMB

Монитор разделяемых каталогов **Samba**. Работает в резидентном режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции чтения и записи) в каталогах, отведенных для файловых

хранилищ SMB-сервера **Samba**. Для интеграции с файловым сервером использует модули VFS SMB, работающие на стороне сервера **Samba**.

SpIDer Guard для NSS

Монитор томов NSS (**Novell Storage Services**). Работает в резидентном режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции записи) на томах NSS, смонтированных в указанную точку файловой системы.

Консольный сканер (управляется только на станции)

Компонент, позволяющий запустить проверку файлов на рабочей станции из командной строки операционной системы.

Dr.Web ClamD

Компонент, эмулирующий интерфейс антивирусного продукта **ClamAV®**. Позволяет использовать Dr.Web для файловых серверов UNIX для антивирусной проверки любым приложениям, которые могут использовать **ClamAV®**.

Карантин

Используется для изоляции вредоносных и подозрительных объектов в специальном каталоге.

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

Вспомогательные

Агент Dr.Web для UNIX

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

File Checker

Используется *Консольным сканером* для передачи на проверку в *Scanning Engine* файлов и управления *Карантином* на рабочей станции.

Network Checker

Используется для передачи на проверку в *Scanning Engine* данных, отправленных компонентами программного комплекса через сеть. Данный компонент используется для работы всех основных компонентов.

Scanning Engine

Используется компонентами *File Checker* и *Network Checker* для антивирусной проверки и управления вирусными базами.

SNMP Agent

Предназначен для интеграции Dr.Web для файловых серверов UNIX с внешними системами мониторинга посредством протокола SNMP.

Dr.Web ConfigD

Координирует работу всех компонентов Dr.Web для файловых серверов UNIX.

Dr.Web CloudD

Компонент, получающий сведения о вредоносности посещаемых URL и передаваемых файлов в облачном сервисе *Dr.Web Cloud*.

Dr.Web HTTPD

Веб-сервер управления компонентами Dr.Web для файловых серверов UNIX. Предоставляет веб-интерфейс управления.

3.2. Настройка Dr.Web для файловых серверов UNIX

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 требуемой ОС (**Linux**, **Solaris** или **FreeBSD**) или группы, содержащей такие станции.
3. В открывшемся управляющем меню в разделе **Конфигурация**, в подразделе ОС **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 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**). При этом редактировать настройки сможет только сам администратор через Центр управления.

3.2.1. 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 **SpIDer Guard** представлены следующие разделы настройки функционирования Dr.Web для файловых серверов UNIX:

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

3.2.1.1. Общие

В данном разделе вы можете управлять следующими параметрами SpIDer Guard на защищаемой станции (файловом сервере):

- **Включить SpIDer Guard для Linux** — управляет запуском SpIDer Guard на защищаемой станции.
- **Использовать эвристический анализ** — управляет использованием SpIDer 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 SpIDer Guard на станции. Если указано *0*, время проверки одного файла не ограничивается.

3.2.1.2. Действия

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

В качестве событий, на которые может реагировать SpIDer 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.

3.2.1.3. Контейнеры

В данном разделе вы можете управлять параметрами проверки SpIDer 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 SpIDer 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.

3.2.1.4. Пути проверки

В данном разделе вы можете управлять списками путей к каталогам и файлам на защищаемой станции (файловом сервере), которые будут проверяться или пропускаться SpIDer 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 SpIDer 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 SpIDer 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 SpIDer 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.

3.2.1.5. Дополнительно

В данном разделе вы можете управлять дополнительными настройками работы SpIDer Guard на защищаемой станции (файловом сервере).

Доступны следующие дополнительные настройки SpIDer Guard:

- **Режим работы** — управляет способом работы SpIDer 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 SpIDer Guard.
- **Метод ведения журнала** — управляет способом сохранения сообщений SpIDer 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 SpIDer Guard. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от SpIDer Guard.
  - *Path* — сообщения журнала от SpIDer Guard сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

3.2.2. Настройки SpIDer Guard для SMB

В разделе **SpIDer Guard для SMB** представлены следующие разделы настройки функционирования Dr.Web для файловых серверов UNIX:

- Общие — общие настройки SpIDer Guard для SMB.

- Действия — настройки действий при обнаружении угроз SpIDer Guard для SMB.
- Контейнеры — настройки проверки составных объектов (архивов, почтовых файлов и т. п.).
- Пути проверки — настройки исключений в проверке файлов.
- Разделяемые каталоги — настройки индивидуальной проверки разделяемых каталогов **Samba**.
- Дополнительно — дополнительные настройки SpIDer Guard для SMB.

3.2.2.1. Общие

В данном разделе вы можете управлять следующими параметрами SpIDer Guard для SMB на защищаемой станции (файловом сервере):

- **Запускать компонент при старте** — управляет запуском SpIDer Guard для SMB на защищаемой станции.
- **Использовать эвристический анализ** — управляет использованием SpIDer Guard для SMB на защищаемой станции эвристического анализа при проверке файлов «на лету». Использование эвристического анализа замедляет проверку, но повышает ее надежность.
- **Размер кэша проверенных файлов** — определяет размер кэша, в котором SpIDer Guard для SMB временно сохраняет результаты проверки файлов.
- **Время проверки одного файла** — определяет максимальный период времени, который отводится на проверку одного файла SpIDer Guard для SMB на станции. Если указано *0*, время проверки одного файла не ограничивается.

3.2.2.2. Действия

В данном разделе вы можете управлять параметрами антивирусной зашиты, которые SpIDer Guard для SMB будет применять при проверке файлов в разделяемых каталогах.

- **Создавать файл с причиной блокировки** — установите этот флажок, чтобы SpIDer Guard для SMB создавал в разделяемом каталоге рядом с инфицированным файлом специальный файл, содержащий причину его блокировки.
- **Блокировать файл для доступа при ошибке проверки** — установите этот флажок, чтобы Guard для SMB блокировал доступ к тем файлам в разделяемом каталоге, которые не удалось проверить.
- **Период задержки перед применением действия** — задайте период времени, в течение которого файл после обнаружения угрозы будет заблокирован до применения к нему действия (см. ниже).

В качестве событий, на которые может реагировать SpIDer Guard для SMB, доступны следующие:

- **Инфицированные** — в проверенном файле обнаружен известный вирус.
- **Подозрительные** — проверенный файл отмечен как *подозрительный*.

- **Неизлечимые** — в файле была обнаружена угроза, к которой невозможно применить действие «лечить».
- **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:

- *Запрещать* — сохранить файл в разделяемом каталоге, но заблокировать доступ к нему со стороны пользователей.
- *Лечить* — восстановить состояние объекта до заражения. 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.

3.2.2.3. Контейнеры

В данном разделе вы можете управлять параметрами проверки SplDer Guard для SMB 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 Guard для SMB. 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 (файловом сервере), которые будут проверяться или пропускаться SpIDer Guard для SMB 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 SpIDer Guard для SMB.

Пути, подлежащие проверке на защищаемой станции, указываются в поле **Проверяемые пути** (по одному пути на строку). Монитор SpIDer Guard для SMB 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. Разделяемые каталоги

В данном разделе вы можете управлять индивидуальными параметрами мониторинга SpIDer Guard для SMB доступа к файлам на различных разделяемых каталогах **Samba**.

Каждый разделяемый каталог, к проверке которого требуется применить индивидуальные настройки, идентифицируется уникальным тегом (эти тег задаются в настройках сервера **Samba**). Для привязки индивидуальных настроек проверки к каталогу укажите его тег в поле **Тег разделяемого каталога**.

Для добавления индивидуальных настроек проверки для нового разделяемого каталога нажмите кнопку  в списке разделяемых каталогов. Для удаления индивидуальных настроек проверки разделяемого каталога нажмите кнопку  в соответствующей строке списка разделяемых каталогов.

К разделяемым каталогам, для которых не указаны индивидуальные настройки проверки, применяются общие настройки, заданные на страницах **Действия**, **Контейнеры** и **Пути проверки**.

В секции разделяемого каталога, поименованного тегом, вы можете указать значения индивидуальных параметров проверки этого каталога. Для этого в поле **Настройка разделяемого каталога** из выпадающего списка выберите нужный параметр проверки, а в поле **Параметр настройки** укажите значение этого параметра.

Для добавления нового индивидуального параметра проверки в список нажмите кнопку  в соответствующей секции разделяемого каталога. Для удаления некоторого

индивидуального параметра из списка нажмите кнопку  в соответствующей строке списка параметров в секции разделяемого каталога.

3.2.2.6. Дополнительно

В данном разделе вы можете управлять дополнительными настройками работы SpIDer Guard для SMB на защищаемой станции (файловом сервере).

Доступны следующие дополнительные настройки SpIDer Guard для SMB:

- **Виртуальный корневой каталог** — определяет путь к каталогу файловой системы, используемому сервером **Samba** в качестве виртуального корневого каталога (переопределяется через **chroot**). Используется как префикс, подставляемый в начало всех путей, используемых сервером **Samba**, включая пути к файлам и каталогам, находящимся в разделяемых каталогах, и описывает путь к ним относительно корня локальной файловой системы. Если этот путь не указан, используется путь к корню файловой системы `/`.
- **Путь к файлу сокета** — определяет путь к файлу сокета для взаимодействия с модулем VFS SMB. Этот путь всегда является относительным и дополняет путь к виртуальному корневому каталогу.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом SpIDer Guard для SMB.
- **Метод ведения журнала** — управляет способом сохранения сообщений SpIDer Guard для SMB 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 SpIDer Guard для SMB. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от SpIDer Guard для SMB.
  - *Path* — сообщения журнала от SpIDer Guard для SMB сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

3.2.3. Настройки SpIDer Guard для NSS

Этот монитор работает только в среде **Novell Open Enterprise Server** SP2 на базе операционной системы **SUSE Linux Enterprise Server** 10 SP3 или старше.

В разделе **SpIDer Guard для NSS** представлены следующие разделы настройки функционирования Dr.Web для файловых серверов UNIX:

- Общие — общие настройки SpIDer Guard для NSS.

- Действия — настройки действий при обнаружении угроз SpIDer Guard для NSS.
- Контейнеры — настройки проверки составных объектов (архивов, почтовых файлов и т. п.).
- Пути проверки — настройки исключений в проверке файлов.
- Дополнительно — дополнительные настройки SpIDer Guard для NSS.

3.2.3.1. Общие

В данном разделе вы можете управлять следующими параметрами SpIDer Guard для NSS на защищаемой станции (файловом сервере):

- **Запускать компонент при старте** — управляет запуском SpIDer Guard для NSS на защищаемой станции.
- **Использовать эвристический анализ** — управляет использованием SpIDer Guard для NSS 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 SpIDer Guard для NSS на станции. Если указано *0*, время проверки одного файла не ограничивается.

3.2.3.2. Действия

В данном разделе вы можете управлять параметрами антивирусной зашиты, которые SpIDer Guard для NSS будет применять при проверке файлов на защищаемом томе NSS.

В качестве событий, на которые может реагировать SpIDer Guard для NSS, доступны следующие:

- **Инфицированные** — в проверенном файле обнаружен известный вирус.
- **Подозрительные** — проверенный файл отмечен как *подозрительный*.
- **Неизлечимые** — в файле была обнаружена угроза, к которой невозможно применить действие «лечить».
- **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* — восстановить состояние объекта до заражения. 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.

3.2.3.3. Контейнеры

В данном разделе вы можете управлять параметрами проверки SpIDer Guard для NSS 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 SpIDer Guard для NSS. 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.

3.2.3.4. Пути проверки

В данном разделе вы можете управлять списками путей к каталогам и файлам на защищаемой станции (файловом сервере), которые будут проверяться или пропускаться SpIDer Guard для NSS при мониторинге защищаемого тома NSS.

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

Пути, подлежащие проверке на защищаемом томе, указываются в поле **Проверяемые пути** (по одному пути на строку). Монитор SpIDer Guard для NSS 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.

3.2.3.5. Дополнительно

В данном разделе вы можете управлять дополнительными настройками работы SpIDer Guard для NSS на защищаемой станции (файловом сервере).

Доступны следующие дополнительные настройки SpIDer Guard для NSS:

- **Точка монтирования томов NSS** — определяет путь к каталогу в файловой системе файлового сервера, в который примонтированы защищаемые тома NSS.
- **Защищаемые тома NSS** — определяет список имен томов NSS, находящихся в точке монтирования, указанной в предыдущем параметра, и подлежащих защите монитором SpIDer Guard для NSS.

  Для добавления нового тома список нажмите кнопку  . Для удаления некоторого тома из списка нажмите кнопку  в соответствующей строке списка.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом SpIDer Guard для NSS.
- **Метод ведения журнала** — управляет способом сохранения сообщений SpIDer Guard для NSS 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 SpIDer Guard для NSS. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от SpIDer Guard для NSS.
  - *Path* — сообщения журнала от SpIDer Guard для NSS 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 файловых серверов UNIX:

- Общие — настройки Агента Dr.Web для UNIX.
- Конфигурация — редактор настроек всех компонентов Dr.Web для файловых серверов UNIX.

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 ВСО, 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 ВСО, используя локальный компонент обновления, работающий на станции).
  - *Запретить* — не разрешать Dr.Web для файловых серверов UNIX на станции получать обновления с серверов ВСО 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 файловых серверов UNIX, 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 SpIDer Guard** — сохранять в журнал сведения о запросах от SpIDer 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 файловых серверов UNIX.
- **Путь к административному коммуникационному сокету** — определяет путь к UNIX-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web для файловых серверов UNIX, работающими с полномочиями суперпользователя.
- **Путь к каталогу временных файлов** — определяет каталог, в котором компоненты Dr.Web для файловых серверов UNIX хранят свои временные файлы.
- **Путь к каталогу PID-файлов и файлов коммуникационных сокетов** — определяет каталог, в котором компоненты Dr.Web для файловых серверов UNIX 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/.