Dr.WEB

Enterprise Security Suite

Управление Dr.Web Mail Security Suite (Unix)

Dr.Web Enterprise Security Suite. Управление Dr.Web Mail Security Suite (Unix)
Версия 13.0
Руководство администратора
19.02.2025

ООО «Доктор Веб», Центральный офис в России

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

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

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

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. Введение

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 Mail Security Suite и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- Руководство администратора антивирусного решения Dr.Web Mail Security Suite 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».

1.2. Условные сокращения и обозначения

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:

- CSV — текстовый формат для представления табличных данных (Comma-Separated Values),
- DNS — система доменных имен (Domain Name System),
- DNSxL — черные и белые списки DNS (DNS Blacklists and Whitelists),
- 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 — модуль ядра Linux (Linux Kernel Module),
- PDF — формат электронных документов (Portable Document Format),
- TCP — протокол управления передачи (Transmission Control Protocol),

- URL — единообразный локатор ресурса (Uniform Resource Locator),
- XML — расширяемый язык разметки (Extensible Markup Language),
- ВСО — Всемирная Система Обновлений Dr.Web,
- ЛВС — Локальная Вычислительная Сеть,
- ОС — Операционная Система,
- ПО — Программное Обеспечение.

2. Dr.Web Enterprise Security Suite

2.1. О продукте

Продукт 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*.

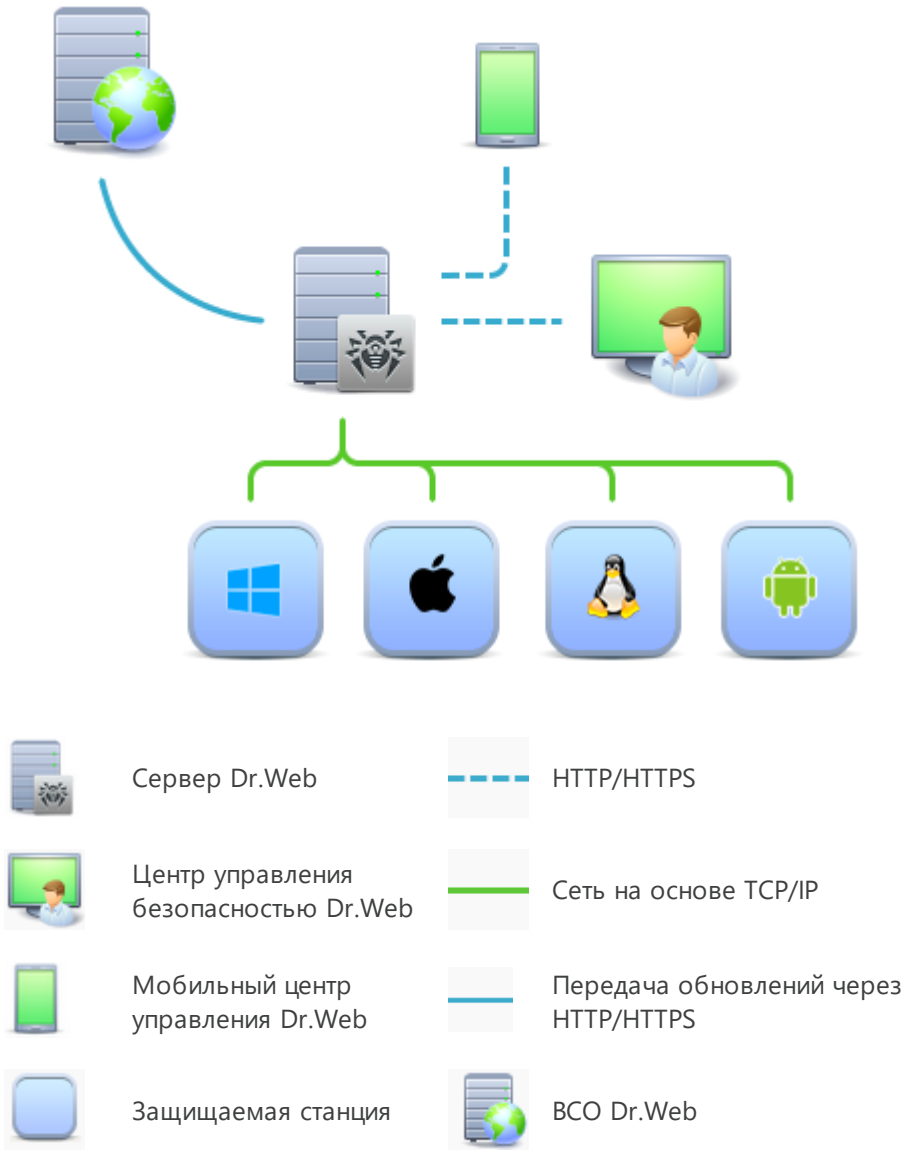

Рисунок 1. Логическая структура антивирусной сети

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 почтовых серверов Unix

Защита почтовых серверов Unix осуществляется с помощью антивирусных пакетов Dr.Web.

Рабочей станцией антивирусной сети называется защищаемое устройство с установленным на нем антивирусным пакетом.
Термин «станция» может быть употреблен по отношению к персональному компьютеру, мобильному устройству или серверу 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 с Сервера Dr.Web на защищаемую станцию осуществляется по протоколу, используемому в локальной сети (TCP/IP версии 4 или 6).

Установка

Локальная установка осуществляется непосредственно на защищаемой станции и может быть выполнена как администратором этой станции, так и администратором антивирусной сети.

Подробное описание процедур установки антивирусных пакетов на защищаемые 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 защищаемой станции:

- Централизованная настройка антивирусного пакета на защищаемой станции при помощи Центра управления безопасностью.

  При этом администратор может как запретить, так и оставить возможность пользователям самостоятельно изменять настройки антивирусного пакета на защищаемой станции.

- Настройка расписания антивирусных проверок и других заданий, выполняемых на защищаемой станции.
- Получение статистики сканирования и прочей информации о работе антивирусных компонентов и о состоянии защищаемой станции.
- Запуск и остановка антивирусного сканирования и т. п. (в зависимости от функциональных возможностей антивирусного пакета, установленного на защищаемой станции).

Обновление

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

В случае временного отключения защищаемой станции от антивирусной сети, антивирусный пакет на сервере использует локальную копию настроек, антивирусная защита на защищаемой станции сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии), но обновление ПО не производится.

3. Dr.Web Mail Security Suite

3.1. Функции Dr.Web Mail Security Suite

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

Продукт Dr.Web Mail Security Suite создан для защиты серверов, работающих под управлением ОС семейства GNU/Linux и FreeBSD от вирусов и всех прочих видов вредоносного программного обеспечения, а также для предотвращения распространения угроз, разработанных для различных платформ.

Основные функции Dr.Web Mail Security Suite:

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, которая затем рассылается различным антивирусным продуктам «Доктор Веб».

   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, 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. **Проверка сообщений электронной почты.** Продукт поддерживает следующие режимы проверки сообщений электронной почты:
   - *Режим внешнего фильтра, подключенного к почтовому серверу (MTA)*. Продукт может быть интегрирован с любым почтовым сервером, поддерживающим интерфейсы подключения внешних фильтров *Milter*, *Spamd* и *Rspamd*. В режиме фильтра все письма, поступающие на почтовый сервер, по инициативе MTA передаются Dr.Web Mail Security Suite через интерфейс сопряжения для проверки. В зависимости от возможностей интерфейса, работающий в качестве фильтра Dr.Web Mail Security Suite может:
     - *Сообщить серверу результаты проверки письма*. В этом случае почтовый сервер должен *самостоятельно* обработать письмо в соответствии с полученными результатами (отклонить его прием или передачу, добавить заголовки или модифицировать содержимое письма, если результат проверки содержит информацию о наличии угроз).
     - *Отдать почтовому серверу команду пропустить или отклонить письмо*.
     - *Модифицировать письмо*, добавив к нему указанные заголовки, или удалив из него выявленное вредоносное или нежелательное содержимое. Вырезанное содержимое прикрепляется к письму в виде архива, защищенного паролем. Пароль для распаковки защищенного архива получатель письма может запросить у администратора почтового сервера. При необходимости, хотя это и не рекомендуется, администратор может настроить использование архивов, не защищенных паролем.

Передача команд почтовому серверу или возврат модифицированного письма поддерживаются только интерфейсом *Milter*. Интерфейсы *Spamd* и *Rspamd* не позволяют Dr.Web Mail Security Suite отправлять серверу команды и возвращать измененное почтовое сообщение. Серверу будет возвращен один из двух вердиктов: «*письмо является спамом*» или «*письмо не является спамом*». Для косвенной модификации отвергнутого сообщения в данном случае вы можете использовать в правилах действие `REJECT` <*description*>. Параметр <*description*>, если указан, будет использован как значение заголовка `Message`, добавленного MTA к письму после сообщения результатов проверки.

   - *Режим прозрачного прокси почтовых протоколов*. В этом режиме продукт (при помощи компонента SplDer Gate) реализует функции прокси-сервера, встроенного в канал обмена данными между MTA и/или MUA прозрачно для обменивающихся сторон, и проверяющего проходящие сообщения при их получении и оправке. Поддерживается прозрачное встраивание антивируса в основные почтовые протоколы: SMTP, POP3, IMAP. В этом режиме, также в зависимости от возможностей протокола, в который он встроен, Dr.Web Mail Security Suite может пропустить письмо получающей стороне (в неизменном виде или после модификации, добавив заголовки или перепаковав письмо), или заблокировать его передачу, в том числе — вернув отправившей или получающей стороне корректную ошибку протокола.

Режим прозрачного прокси доступен только для ОС семейства GNU/Linux.

Dr.Web Mail Security Suite, в зависимости от комплектности и настроек, выполняет следующие проверки сообщений электронной почты:

- *Выявление вредоносных вложений*, содержащих угрозы;
- *Поиск ссылок на вредоносные веб-сайты* или веб-сайты, отнесенные к нежелательным категориям;
- *Выявление признаков спама* (как с использованием автоматически обновляемой базы правил спам-фильтрации, так и при помощи механизма проверки наличия адреса отправителя в черных списках DNSxL);
- *Соответствие критериям безопасности, заданным администратором* почтовой системы самостоятельно (проверка тела и заголовков сообщений при помощи регулярных выражений).

Для проверки ссылок на нежелательные веб-сайты, которые могут присутствовать в сообщениях электронной почты, используется автоматически обновляемая база данных категорий веб-ресурсов, поставляемая вместе с Dr.Web Mail Security Suite. Также производится обращение к сервису Dr.Web Cloud для проверки наличия информации, не отмечен ли веб-ресурс, ссылка на который встретилась в почтовом сообщении, как вредоносный, другими антивирусными продуктами Dr.Web.

3.2. Компоненты Dr.Web Mail Security Suite

Для защиты почтовых серверов Unix предоставляются следующие антивирусные компоненты:

Основные

Dr.Web MailD

Компонент проверки почтовых сообщений. Анализирует сообщения почтовых протоколов, разбирает сообщения электронной почты и подготавливает их к проверке на наличие угроз. Может работать в двух режимах:

- фильтр для почтовых серверов (Sendmail, Postfix и т. п.), подключаемый через интерфейс *Milter*, *Spamd* или *Rspamd*;
- прозрачный прокси почтовых протоколов (SMTP, POP3, IMAP). В этом режиме использует *SpIDer Gate*.

Dr.Web Anti-Spam Engine

Компонент проверки сообщений электронной почты на наличие признаков спама. Используется компонентом Dr.Web MailD, может отсутствовать в составе Dr.Web Mail Security Suite на станции.

SpIDer Gate

Компонент проверки сетевого трафика и URL. Предназначен для проверки данных, загружаемых на локальный узел из сети и передаваемых с него во внешнюю сеть, на наличие угроз, и предотвращения соединения с узлами сети, внесенными в нежелательные категории веб-ресурсов и черные списки, формируемые системным администратором.

Используется компонентом *Dr.Web MailD* в режиме прозрачного прокси почтовых протоколов (SMTP, POP3, IMAP).

Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Dr.Web ClamD

Компонент, эмулирующий интерфейс антивирусного продукта ClamAV®. Позволяет использовать Dr.Web Mail Security Suite для антивирусной проверки любым приложениям, которые могут использовать ClamAV®.

Карантин

Используется для изоляции вредоносных и подозрительных объектов.

Служебные

Агент Dr.Web для Unix

Используется для взаимодействия Dr.Web Mail Security Suite, 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 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 Mail Security Suite с внешними системами мониторинга посредством протокола SNMP.

Dr.Web ConfigD

Координирует работу всех компонентов Dr.Web Mail Security Suite.

Dr.Web CloudD

Компонент, получающий сведения о вредоносности посещаемых URL и передаваемых файлов из облачного сервиса.

Dr.Web HTTPD

Веб-сервер управления компонентами Dr.Web Mail Security Suite. Предоставляет веб-интерфейс управления.

3.3. Режимы работы Dr.Web Mail Security Suite

Антивирусное решение Dr.Web Mail Security Suite может работать как в одиночном режиме, так и в составе корпоративной или частной *антивирусной сети*, управляемой каким-либо *сервером централизованной защиты*. Такой режим работы называется *режимом централизованной защиты*. Использование этого режима не требует установки дополнительного программного обеспечения, переустановки или удаления Dr.Web Mail Security Suite.

- В *одиночном режиме* защищаемый компьютер не включен в антивирусную сеть и управляется локально. В этом режиме конфигурационный и лицензионный ключевой файлы находятся на локальных дисках, а Dr.Web Mail Security Suite полностью управляется с защищаемого компьютера. Обновления вирусных баз получаются с серверов обновлений компании «Доктор Веб».
- В *режиме централизованной защиты* защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки Dr.Web Mail Security Suite могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты, принятой в антивирусной сети. В этом режиме на компьютере используется особый лицензионный ключевой файл, полученный с выбранного сервера централизованной защиты, к которому подключен Dr.Web Mail Security Suite. Лицензионный или демонстрационный ключевой файл пользователя, если он имеется на локальном компьютере, не используется. На сервер централизованной защиты отсылается статистика работы Dr.Web Mail Security Suite, включая статистику инцидентов, связанных с вредоносным ПО. Обновление вирусных баз также выполняется с сервера централизованной защиты.
- В *мобильном режиме* Dr.Web Mail Security Suite получает обновления вирусных баз с серверов обновлений компании «Доктор Веб», но использует локально хранящиеся настройки и особый лицензионный ключевой файл, полученные от сервера централизованной защиты. Возможность использования данного режима зависит от разрешений, заданных на сервере централизованной защиты.

Принципы централизованной защиты

Решения компании «Доктор Веб» по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (см. иллюстрацию ниже).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз *локальными антивирусными компонентами* (в данном случае компонентами Dr.Web Mail Security Suite), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

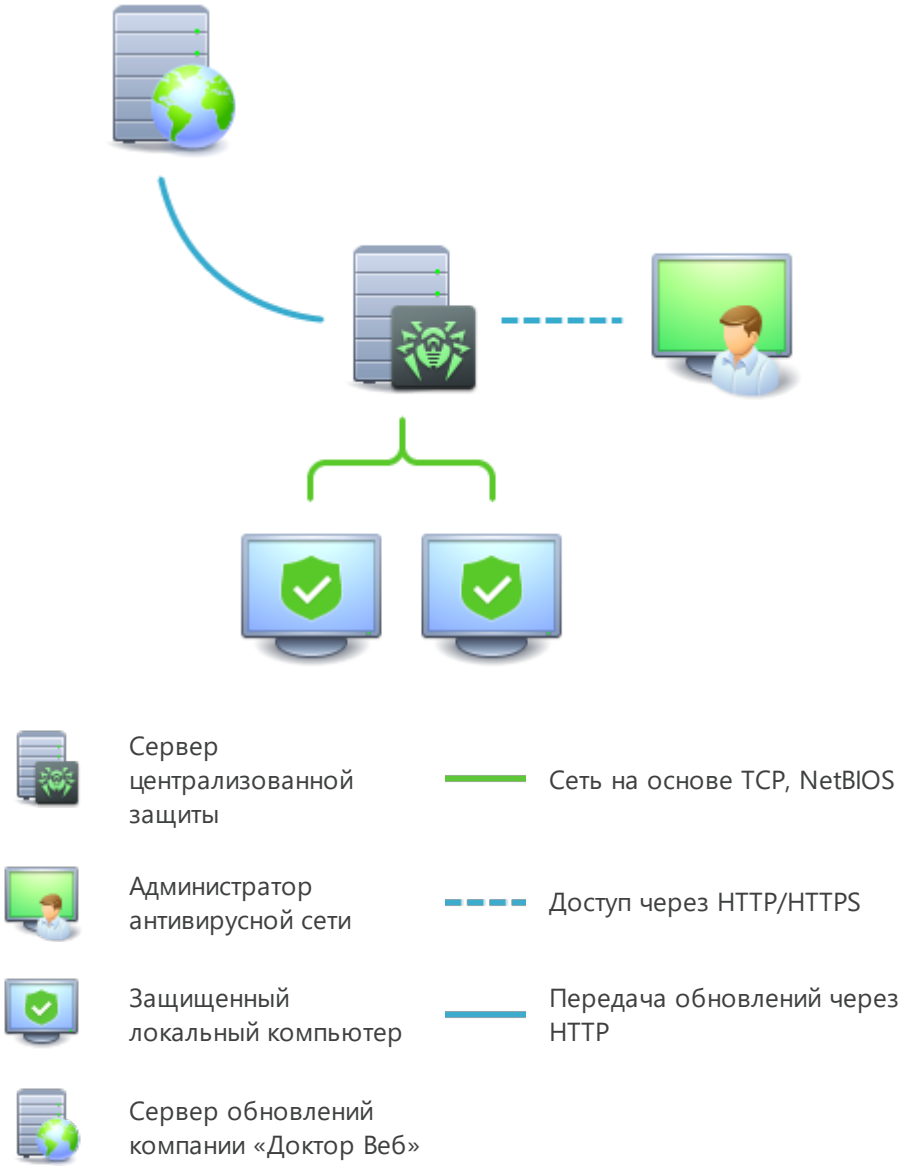

Рисунок 2. Логическая структура антивирусной сети

Обновление и конфигурация локальных компонентов производится через *сервер централизованной защиты*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты. Объем

трафика между защищенными компьютерами и сервером централизованной защиты может быть весьма значительным, поэтому предусматривается возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.

Все необходимые обновления загружаются на сервер централизованной защиты с серверов обновлений компании «Доктор Веб».

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется сервером централизованной защиты по указанию администраторов антивирусной сети. Администраторы управляют конфигурацией сервера централизованной защиты и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной станции к сети), а также, при необходимости, задают настройки работы конкретных локальных антивирусных компонентов.

Локальные антивирусные компоненты несовместимы с антивирусным программным обеспечением как других компаний, так и антивирусными решениями Dr.Web, не поддерживающими режим централизованной защиты (например, Dr.Web для почтовых серверов UNIX версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы и потере важных данных.

Продукт Dr.Web Mail Security Suite версии 11.1, работающий в режиме централизованной защиты, совместим с Dr.Web Enterprise Security Suite версий 11, 12, 13 и 13.0.1.

В режиме централизованной защиты возможен экспорт и сохранение отчетов о функционировании Dr.Web Mail Security Suite с помощью сервера централизованной защиты. Поддерживается экспорт и сохранение отчетов в форматах HTML, CSV, PDF и XML.

Подключение к серверу централизованной защиты

Dr.Web Mail Security Suite может быть подключен к серверу централизованной защиты антивирусной сети при помощи команды `esconnect` утилиты управления из командной строки `drweb-ctl`.

Для верификации сервера централизованной защиты используется сертификат, соответствующий уникальному открытому ключу шифрования, используемому сервером. По умолчанию агент централизованной защиты Dr.Web ES Agent не позволит произвести подключение к серверу, если вы не укажете файл сертификата сервера, к которому производится подключение. Файл сертификата необходимо предварительно получить у администратора антивирусной сети, обслуживаемой сервером, к которому вы хотите подключить Dr.Web Mail Security Suite.

Если Dr.Web Mail Security Suite подключен к серверу централизованной защиты, то имеется возможность перевести его в мобильный режим и вернуть назад в режим централизованной защиты. Включение и выключение мобильного режима регулируется параметром конфигурации `MobileMode` компонента Dr.Web ES Agent.

Возможность перехода Dr.Web Mail Security Suite в мобильный режим работы зависит от разрешений, заданных на используемом сервере централизованной защиты.

Отключение от сервера централизованной защиты

Dr.Web Mail Security Suite может быть отключен от сервера централизованной защиты антивирусной сети при помощи команды `esdisconnect` утилиты управления из командной строки `drweb-ctl`.

3.4. Настройка Dr.Web Mail Security Suite

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 (GNU/Linux или FreeBSD) или группы, содержащей такие станции.
3. В открывшемся управляющем меню в разделе **Конфигурация**, в подразделе требуемой ОС (GNU/Linux или FreeBSD) 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.

3.4.1. Настройки Dr.Web MailD

3.4.1.1. Общие настройки

В данном разделе вы можете управлять следующими параметрами работы Dr.Web MailD на защищаемой станции (почтовом сервере):

- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Dr.Web MailD.
- **Метод ведения журнала** — управляет способом сохранения сообщений Dr.Web MailD 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 Dr.Web MailD. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую syslog подсистему (метку) для сохранения сообщений от Dr.Web MailD.
  - *Path* — сообщения журнала от Dr.Web MailD сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

- **Пользователь** — позволяет указать имя пользователя Unix-подобной ОС, с правами и полномочиями которого работает компонент на защищаемом почтовом сервере.

  

  Если имя пользователя не указано, работа компонента завершится ошибкой сразу после попытки его запуска.

- **Файл настроек подсистемы DNS Resolver** — задает путь к используемому файлу настроек подсистемы разрешения доменных имен (DNS resolver).
- **Путь к файлу сокета фиксированной копии компонента** — задает путь к файлу Unix-сокета фиксированной копии компонента. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD на почтовом сервере следит за тем, чтобы всегда имелась запущенная копия компонента, доступная клиентам через этот сокет.

3.4.1.2. Шаблоны уведомлений

В данном разделе вы можете управлять параметрами генерации Dr.Web MailD на защищаемом почтовом сервере писем с уведомлениями об угрозах:

- **Контакты администратора почтовой системы** — позволяет указать текст, который будет добавлен к отправляемым уведомлениям об обнаруженных угрозах и позволит пользователям связаться с администратором почтовой системы.
- **Языки уведомлений** — указывает язык, на котором будут отправляться уведомления клиентам.
- **Режим генерации пароля** — указывает режим генерации пароля для архивов с обнаруженными угрозами, которые будут вкладываться в уведомления, направляемые получателям. Доступны следующие режимы генерации пароля:
  - *None* — архивы не будут защищены паролем (не рекомендуется).
  - *Plain* — все архивы будут защищены одинаковым паролем. В случае выбора этого значения необходимо также указать пароль в поле **Пароль**.
  - *HMAC* — каждый архив будет защищен уникальным паролем, сгенерированным на основе идентификатора сообщения и заданного секретного слова. В случае выбора этого значения необходимо указать секретное слово в поле **Секретное слово**.

3.4.1.3. Интеграция с MTA

В данных трех разделах вы можете управлять параметрами взаимодействия Dr.Web MailD на защищаемом почтовом сервере с почтовыми системами (MTA) через интерфейсы *Milter*, *Spamd* и *Rspamd* (для всех трех интерфейсов используются одинаковые параметры настройки):

- **Эвристический анализ** — управляет использованием Dr.Web MailD эвристического анализа для поиска неизвестных угроз в письмах, поступающих на проверку через используемый интерфейс. Использование эвристического анализа замедляет проверку, но повышает ее надежность.

- **Тайм-аут на проверку одного письма** — определяет максимальный период времени, который отводится на проверку одного письма, поступившего на проверку через интерфейс Milter. Допустимые значения: от 1 секунды до 1 часа. Значение по умолчанию: 3 минуты.
- **Максимальный уровень вложенности**. В данном разделе вы можете управлять параметрами проверки Dr.Web MailD вложенных в письма 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 Dr.Web MailD. 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.
- **Сокет для подключения MTA через Milter (Spamd, Rspamd)** — задает сокет для подключения к MTA (на этот сокет MTA будет выполнять подключение при использовании Dr.Web MailD в качестве фильтра). Допускается указание Unix-сокета (пути в локальной файловой системе защищаемого сервера) или сетевого сокета (пары *IP-адрес*:*порт*).
- **Блокировать непроверенные почтовые сообщения** — установите этот флажок, если вы хотите блокировать сообщения, поступившие на проверку через используемый интерфейс, которые Dr.Web MailD не смог проверить.
- **Правила проверки почты через Milter (Spamd, Rspamd)** — укажите в этом разделе правила проверки, которые Dr.Web MailD будет применять к письмам, поступившим через используемый интерфейс.

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

3.4.2. Настройки Агента Dr.Web для Unix

3.4.2.1. Общие настройки

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

- **Собирать информацию о станциях** — разрешить или запретить Агенту Dr.Web для Unix собирать информацию о состоянии станций.
- **Период сбора информации о станциях** — периодичность (в минутах), с которой Агент Dr.Web для Unix отправляет запросы к станциям для сбора информации.
- **Периодичность отправки статистики** — периодичность, с которой Агент Dr.Web для Unix отправляет статистику на сервер.
- **Мобильный режим получения обновлений** — использование 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 Mail Security Suite на станции получать обновления с серверов ВСО в случае невозможности подключения к серверу Dr.Web Enterprise Security Suite.
- **Обрабатывать discovery-запросы** — разрешить или запретить агенту принимать discovery-запросы от сервера Dr.Web Enterprise Security Suite (используются для проверки структуры и состояния антивирусной сети).
- **Уровень журнала** — уровень подробности ведения журнала компонентом Агент Dr.Web для Unix.
- **Метод ведения журнала** — способ 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.

3.4.2.2. Конфигурация

В данном разделе вы можете задавать настройки для любого из компонентов Dr.Web Mail Security Suite, установленного на станции, в формате файла конфигурации `.ini`. Для этого внесите необходимые изменения в поле **Конфигурационный файл drweb.ini**.

Обратите внимание, что:

- Центр управления не поддерживает настройку всех имеющихся параметров. Для детальной настройки компонентов Агента Dr.Web для Unix используйте редактор настроек Dr.Web Mail Security Suite.
- 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 приведены в редакторе **Конфигурационный файл drweb.ini**, неуказанные параметры 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 импорта и экспорта содержимого редактора в виде файла конфигурации `.ini`. Для этого нажмите соответствующую кнопку, расположенную 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 администратора продукта, установленного на станции.

3.4.3. Настройки SplDer Gate

3.4.3.1. Общие настройки

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 SpIDer Guard на станции. Допустимые значения: от 1 секунды до 1 часа. Значение по умолчанию: 30 секунд.

3.4.3.2. Действия

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

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

3.4.3.3. 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 нерекомендуемые 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 интернете.
- 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 или 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.

3.4.3.4. Контейнеры

В данном разделе вы можете управлять параметрами проверки SpIDer 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 SpIDer 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.

3.4.3.5. Дополнительные настройки

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

Доступны следующие дополнительные настройки SpIDer Gate:

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

3.4.4. Настройки File Checker

В данном разделе вы можете управлять настройками работы на защищаемой станции служебного 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.

3.4.5. Настройки Scanning Engine

В данном разделе вы можете управлять настройками работы на защищаемой станции служебного 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.

3.4.6. Настройки Dr.Web ConfigD

В данном разделе вы можете управлять настройками работы на защищаемой станции служебного 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 Mail Security Suite.
- **Путь к административному коммуникационному сокету** — определяет путь к Unix-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web Mail Security Suite, работающими с полномочиями.
- **Путь к каталогу временных файлов** — определяет каталог, в котором компоненты Dr.Web Mail Security Suite хранят свои временные файлы.
- **Путь к каталогу PID-файлов и файлов коммуникационных сокетов** — определяет каталог, в котором компоненты Dr.Web Mail Security Suite 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.

4. 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:

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

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

1. Заполните веб-форму в соответствующей секции раздела https://support.drweb.com/.
2. Позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

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