Dr.WEB

Enterprise Security Suite

Управление Dr.Web Desktop Security Suite (Linux)

Dr.Web Enterprise Security Suite. Управление Dr.Web Desktop Security Suite (Linux)
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 Desktop Security Suite и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- Руководство администратора антивирусного решения Dr.Web Desktop 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),
- GUI — графический интерфейс пользователя (Graphical User Interface),
- 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*.

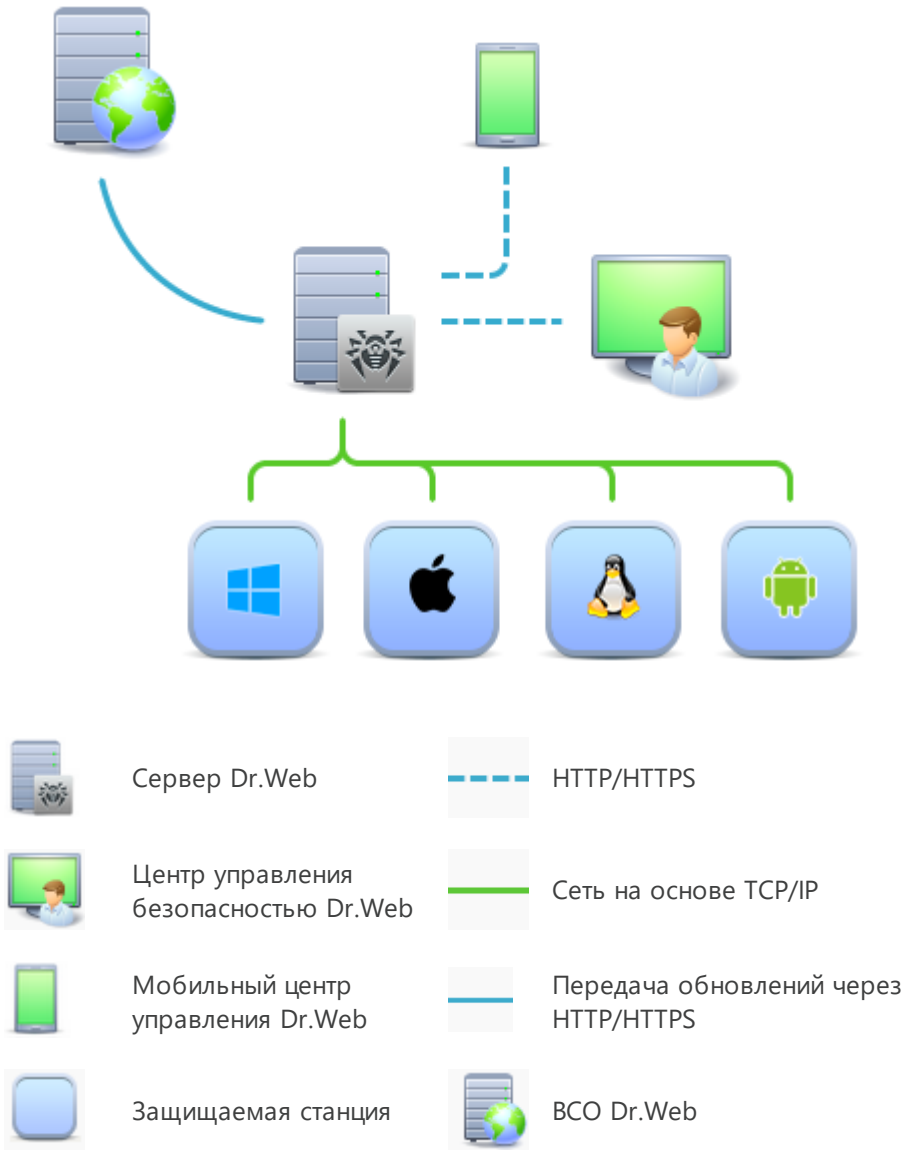

Рисунок 1. Логическая структура антивирусной сети

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 рабочих станций под Linux

Защита рабочих станций под Linux 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. Если для защищаемой станции разрешено функционирование в *мобильном режиме*, при потере связи с Сервером Dr.Web будет доступно обновление вирусных баз непосредственно с серверов ВСО Dr.Web.

Принцип работы станций в мобильном режиме описан в Главе 4 настоящего Руководства.

3. Dr.Web Desktop Security Suite

3.1. Функции Dr.Web Desktop Security Suite

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

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

Основные функции Dr.Web Desktop 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. **Мониторинг обращений к файлам.** Отслеживаются обращения к файлам с данными и попытки запуска исполняемых файлов. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках инфицирования ими компьютера.
3. **Мониторинг доступа к интернету**. Отслеживаются попытки обращения к серверам в интернете (веб-серверам, почтовым и файловым серверам) для блокировки доступа пользователя к веб-сайтам, отмеченным как нежелательные для посещения, а также для предотвращения получения и отправки сообщений электронной почты, содержащих инфицированные файлы, нежелательные ссылки или классифицированных как спам. Проверка сообщений электронной почты и файлов, загружаемых по сети, на наличие в них вирусов и других угроз, производится «на лету». Для определения нежелательных ссылок используются как поставляемая вместе с Dr.Web Desktop Security Suite автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, так и черные и белые списки, ведущиеся пользователем вручную. Дополнительно продукт обращается к сервису Dr.Web Cloud для проверки, не отмечен ли веб-сайт, к которому пытается обратиться пользователь, как вредоносный, другими антивирусными продуктами компании «Доктор Веб».
4. **Надежная изоляция вредоносных 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.

3.2. Компоненты Dr.Web Desktop Security Suite

Для защиты рабочих станций под Linux предоставляются следующие антивирусные компоненты:

Основные

Сканер для рабочих станций

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

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

Dr.Web MailD

Компонент проверки почтовых сообщений. Анализирует сообщения почтовых протоколов, разбирает сообщения электронной почты и подготавливает их к проверке на наличие угроз.

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 Desktop Security Suite на станции.

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). Передает компоненту File Checker запросы на проверку содержимого новых и изменившихся файлов, а также исполняемых файлов в момент запуска программ.

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.

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

Консольный сканер

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

Карантин

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

Служебные

Агент Dr.Web для Unix

Используется для взаимодействия Dr.Web Desktop 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.

Dr.Web ConfigD

Координирует работу всех компонентов Dr.Web Desktop Security Suite.

Dr.Web CloudD

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

3.3. Режимы работы Dr.Web Desktop Security Suite

Dr.Web Desktop Security Suite может работать как автономно, 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 Desktop 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 Desktop 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 Desktop 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 Desktop 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 Desktop Security Suite, включая статистику инцидентов, связанных с вредоносным ПО. Обновление вирусных баз также выполняется с сервера централизованной защиты.
- В *мобильном режиме* Dr.Web Desktop 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.

В случае работы Dr.Web Desktop Security Suite под управлением сервера централизованной защиты (в том числе и в мобильном режиме) блокируются следующие возможности:

1. Возможность удаления лицензионного ключевого файла в Менеджере лицензий.
2. Возможность запуска обновлений вручную и настройки параметров обновления.
3. Возможность настройки параметров проверки объектов файловой системы Сканером.

Возможность настройки монитора файловой системы SpIDer Guard, а также его включения и выключения при работе Dr.Web Desktop Security Suite под управлением сервера централизованной защиты зависит от разрешений, заданных на сервере.

В режиме централизованной защиты недоступна проверка файлов по заданному расписанию.

Если на сервере централизованной защиты включен запрет на запуск проверки файлов пользователем, то страница запуска сканирования и кнопка **Сканер** на окне Dr.Web Desktop Security Suite будут недоступны.

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 — Dr.Web Desktop Security Suite), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

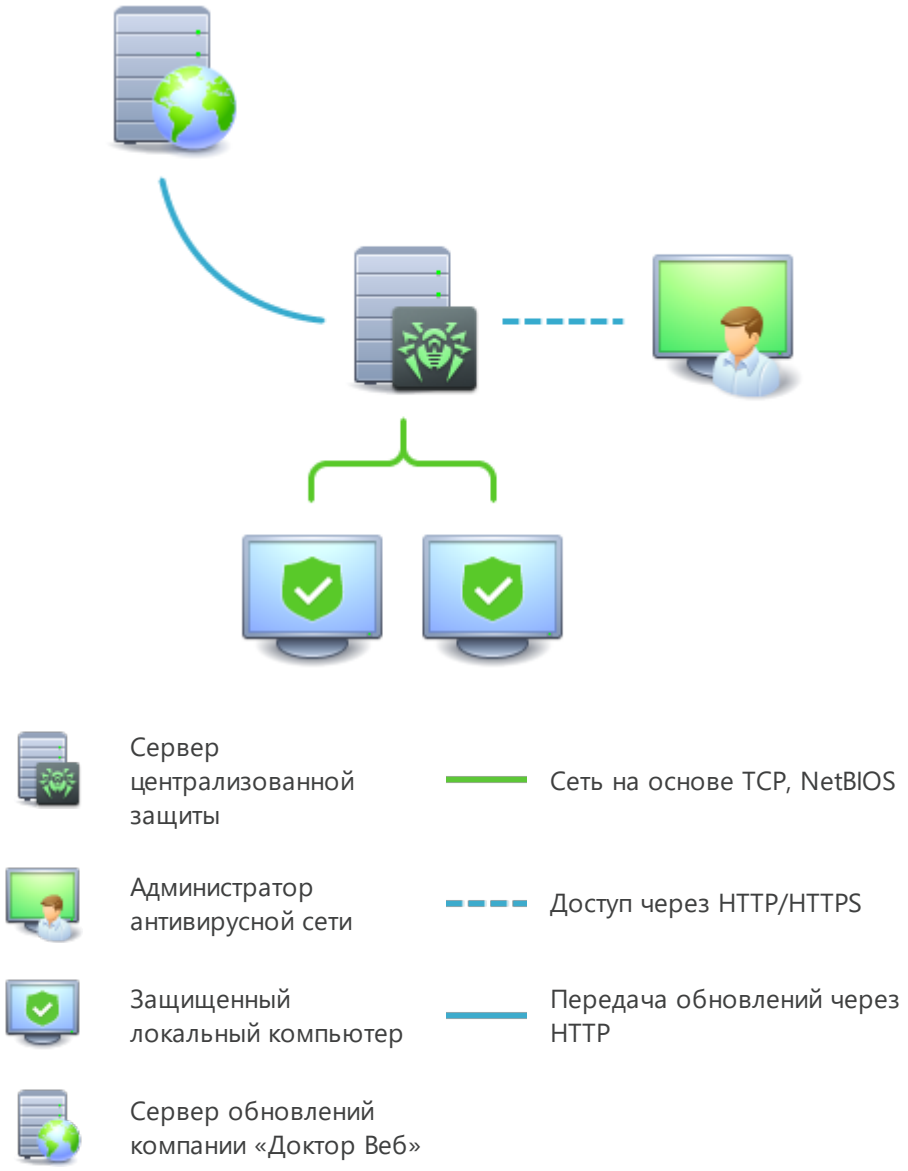

Рисунок 2. Логическая структура антивирусной сети

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 Linux версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы и потере важных данных.

Продукт Dr.Web Desktop 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 Desktop Security Suite с помощью сервера централизованной защиты. Поддерживается экспорт и сохранение отчетов в форматах HTML, CSV, PDF и XML.

Подключение к антивирусной сети

Dr.Web Desktop Security Suite может быть подключен к антивирусной сети следующими способами:

- На вкладке **Режим** страницы настроек окна Dr.Web Desktop Security Suite.
- При помощи команды `esconnect` утилиты управления из командной строки `drweb-ctl`.

Отключение от антивирусной сети

Dr.Web Desktop Security Suite может быть отключен от антивирусной сети следующими способами:

- На вкладке **Режим** страницы настроек окна Dr.Web Desktop Security Suite.
- При помощи команды `esdisconnect` утилиты управления из командной строки `drweb-ctl`.

3.4. Настройка Dr.Web Desktop 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 группы, содержащей такие станции.
3. В открывшемся управляющем меню в разделе **Конфигурация**, в подразделе требуемой ОС (GNU/Linux) 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. Сканер для рабочих станций

Сканер Dr.Web осуществляет быструю или полную проверку объектов файловой системы или проверяет только критические файлы и каталоги.

Настройки Сканера Dr.Web для компьютеров под управлением операционных систем семейства GNU/Linux задаются в разделе **Сканер для рабочих станций**. В этом разделе задаются настройки только GUI-версии Сканера Dr.Web. Управление настройками консольного сканера осуществляется локально на станции.

Общие

На вкладке **Общие** задайте общие параметры работы Сканера Dr.Web.

- В поле **Время проверки одного файла** укажите максимальное время проверки одного файла. Значение по умолчанию: 0 (время проверки одного файла не ограничено).

Включение проверки архивов и почтовых файлов, а также увеличение максимального времени проверки одного файла могут привести к замедлению работы системы и увеличить общее время проверки.

Действия

В этом разделе настроек вы можете настроить действия, которые должны быть применены к угрозам, обнаруженным Сканером Dr.Web. Действия задаются отдельно для каждого типа вредоносных и подозрительных объектов. Состав доступных действий при этом зависит от типа объектов.

Типы угроз, на которые может реагировать Сканер Dr.Web:

- **Вредоносные** — в проверенном файле обнаружена известная угроза;
- **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.

Доступные действия:

- **Лечить, перемещать в карантин неизлечимые** — восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет перемещен в карантин.

  Данное действие возможно только для объектов, зараженных известной излечимой угрозой, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).
- **Лечить, удалять неизлечимые** — восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет удален.

  Данное действие возможно только для объектов, зараженных известной излечимой угрозой, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).
- **Удалять** — удалить объект, представляющий угрозу.

  Наиболее эффективный способ устранения компьютерных угроз любых типов.
- **Перемещать в карантин** — поместить обнаруженную угрозу в специальный каталог, изолированный от остальной системы.
- **Сообщать** — оповестить об угрозе, не выполняя других действий.

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

Выберите **Автоматически применять действия к угрозам**, чтобы автоматически применять действия, указанные выше, к угрозам при проверке. Если эта опция отключена, то пользователь будет информирован о найденной угрозе, но меры по ее нейтрализации предприняты не будут.

Вы также можете отключить проверку архивов и почтовых файлов. По умолчанию проверка этих объектов включена.

Таблица 1. Действия Сканера Dr.Web над обнаруженными вредоносными объектами

Объект	Действие				
	Лечить, перемещать в карантин неизлечимые	Лечить, удалять неизлечимые	Удалять	Перемещать в карантин	Сообщать
Вредоносные	+/*	+	+	+	

Объект	Действие				
	Лечить, перемещать в карантин неизлечимые	**Лечить, удалять неизлечимые**	**Удалять**	**Перемещать в карантин**	**Сообщать**
Подозрительные			+	+/*	+
Рекламные программы			+	+/*	+
Программы дозвона			+	+/*	+
Программы-шутки			+	+	+/*
Потенциально опасные			+	+	+/*
Программы взлома			+	+	+/*

Условные обозначения

+	действие разрешено для данного типа объектов
+/*	действие установлено как реакция по умолчанию для данного типа объектов

Исключаемые пути

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

3.4.2. Настройки SplDer Guard

3.4.2.1. Общие настройки

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

- **Включить SplDer Guard для Linux** — управляет запуском SplDer Guard на защищаемой станции.
- **Использовать эвристический анализ** — управляет использованием SplDer Guard на защищаемой станции эвристического анализа при проверке файлов «на лету».

Использование эвристического анализа замедляет проверку, но повышает ее надежность.

- **Время проверки одного файла** — определяет максимальный период времени, который отводится на проверку одного файла SpIDer Guard на станции. Допустимые значения: от 1 секунды до 1 часа. Значение по умолчанию: 30 секунд.

Монитор файловой системы SpIDer 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 SpIDer Guard не запускается, выполните на защищаемой станции сборку и установку загружаемого модуля ядра из поставляемого исходного кода.

3.4.2.2. Действия

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

Типы угроз, на которые может реагировать SpIDer Guard:

- **Вредоносные** — в проверенном файле обнаружена известная угроза;
- **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.

Доступные действия:

- **Лечить, перемещать в карантин неизлечимые** — восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет перемещен в карантин.

  Данное действие возможно только для объектов, зараженных известной излечимой угрозой, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).
- **Лечить, удалять неизлечимые** — восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет удален.

  Данное действие возможно только для объектов, зараженных известной излечимой угрозой, за исключением троянских программ и зараженных файлов внутри составных

объектов (архивов, файлов электронной почты или файловых контейнеров).

- **Удалять** — удалить объект, представляющий угрозу.

  Наиболее эффективный способ устранения компьютерных угроз любых типов.
- **Перемещать в карантин** — поместить обнаруженную угрозу в специальный каталог, изолированный от остальной системы.
- **Сообщать** — оповестить об угрозе, не выполняя других действий.

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

Таблица 2. Действия Dr.Web SpIDer Guard над обнаруженными вредоносными объектами

Объект	Действие				
	Лечить, перемещать в карантин неизлечимые	**Лечить, удалять неизлечимые**	**Удалять**	**Перемещать в карантин**	**Сообщать**
Вредоносные	+/*	+	+	+	
Подозрительные			+	+/*	+
Рекламные программы			+	+/*	+
Программы дозвона			+	+/*	+
Программы-шутки			+	+	+/*
Потенциально опасные			+	+	+/*
Программы взлома			+	+	+/*

Условные обозначения

+	действие разрешено для данного типа объектов
+/*	действие установлено как реакция по умолчанию для данного типа объектов

3.4.2.3. 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 объектов для проверки (как отношение сжатого объема файла к несжатому). Если степень сжатия проверяемого объекта превысит указанную величину, он будет пропущен при проверке.

3.4.2.4. Пути проверки

В данном разделе вы можете управлять списками путей к каталогам и файлам на защищаемой станции, 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.

3.4.2.5. Дополнительные настройки

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

Доступны следующие дополнительные настройки SpIDer Guard:

- **Режим работы** — способ 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** — уровень подробности ведения журнала компонентом SpIDer Guard.
- **Метод ведения журнала** — способ 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**.

3.4.3. Настройки Агента Dr.Web для Unix

3.4.3.1. 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 Desktop 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.

3.4.3.2. Конфигурация

В данном разделе вы можете задавать настройки для любого из компонентов Dr.Web Desktop 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 Desktop 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 пользователя продукта, установленного на станции.

3.4.4. Настройки SplDer Gate

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

3.4.4.2. Действия

В данном разделе вы можете управлять следующими параметрами SplDer 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 SplDer Gate.

3.4.4.3. 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.

3.4.4.4. 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.

3.4.4.5. 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**.

3.4.5. 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.

3.4.6. 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.

3.4.7. 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 Desktop Security Suite.
- **Путь к административному коммуникационному сокету** — определяет путь к Unix-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web Desktop Security Suite, работающими с полномочиями.
- **Путь к каталогу временных файлов** — определяет каталог, в котором компоненты Dr.Web Desktop Security Suite хранят свои временные файлы.
- **Путь к каталогу PID-файлов и файлов коммуникационных сокетов** — определяет каталог, в котором компоненты Dr.Web Desktop 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. Обновление мобильных агентов Dr.Web

Общая информация

Если у пользовательской рабочей станции в течение длительного времени отсутствует доступ к Серверу Dr.Web, Агент Dr.Web на станции может получать обновления с серверов ВСО Dr.Web в *мобильном режиме*. Мобильный режим должен быть настроен на станции, а также разрешен на сервере.

Настройки мобильного режима на станции устанавливаются путем изменения значения параметра `EsAgent.MobileMode`:

```
# drweb-ctl cfset EsAgent.MobileMode <требуемое значение>
```

Параметр может принимать следующие значения:

- *on* — использовать только мобильный режим, если разрешено на сервере, и получать обновления только с серверов ВСО;
- *off* — не использовать мобильный режим и получать обновления только с сервера централизованной защиты;
- *auto* — использовать мобильный режим, если разрешено на сервере, и получать обновления как серверов ВСО, так и с сервера централизованной защиты (в зависимости от того, какое именно соединение доступно и у какого соединения выше качество).

Мобильный режим с настройками по умолчанию: особенности функционирования

Значение *auto* установлено по умолчанию. В этом случае переход станция будет получать обновления с серверов ВСО, если:

- с сервера централизованной защиты не было успешных обновлений в течение 24 часов;
- к серверу централизованной защиты не удается подключиться в течение 10 минут.

В мобильном режиме Агент Dr.Web предпринимает попытки восстановить связь с сервером централизованной защиты примерно раз в минуту. Если после успешной попытки соединение сохранится в течение 10 минут, можно будет снова получать обновления с сервера централизованной защиты.

5. 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/.