



Dr.WEB

Enterprise Security Suite

Управление Dr.Web Server Security Suite (Unix)



© «Доктор Веб», 2025. Все права защищены

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

Материалы, приведенные в данном документе, являются собственностью ООО «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

Товарные знаки

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

Ограничение ответственности

Ни при каких обстоятельствах ООО «Доктор Веб» и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

Dr.Web Enterprise Security Suite. Управление Dr.Web Server 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	5
1.1. Назначение документа	5
1.2. Условные сокращения и обозначения	6
2. Dr.Web Enterprise Security Suite	8
2.1. О продукте	8
2.2. Защита файловых серверов Unix	9
3. Dr.Web Server Security Suite	11
3.1. Функции Dr.Web Server Security Suite	11
3.2. Компоненты Dr.Web Server Security Suite	12
3.3. Режимы работы Dr.Web Server Security Suite	14
3.4. Настройка Dr.Web Server Security Suite	17
3.4.1. Настройки SpIDer Guard	18
3.4.2. Настройки SpIDer Guard для SMB	22
3.4.3. Настройки SpIDer Guard для NSS	26
3.4.4. Настройки Агента Dr.Web для Unix	30
3.4.5. Настройки File Checker	32
3.4.6. Настройки Scanning Engine	33
3.4.7. Настройки Dr.Web ConfigD	33
4. Приложение А. Техническая поддержка	35



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 Server Security Suite и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- Руководство администратора антивирусного решения Dr.Web Server 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.
<i>Антивирусная сеть</i>	Новый термин или акцент на термине в описаниях.
<code><IP-address></code>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
<code>/home/user</code>	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте Руководства будут употребляться без расшифровки следующие сокращения:

- CSV — текстовый формат для представления табличных данных (Comma-Separated Values),
- 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),
- SMB — протокол доступа к файлам (Server Message Block),
- TCP — протокол управления передачи (Transmission Control Protocol),
- URL — единообразный локатор ресурса (Uniform Resource Locator),



- VFS — виртуальная файловая система (Virtual File System),
- XML — расширяемый язык разметки (Extensible Markup Language),
- BCO — 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*.

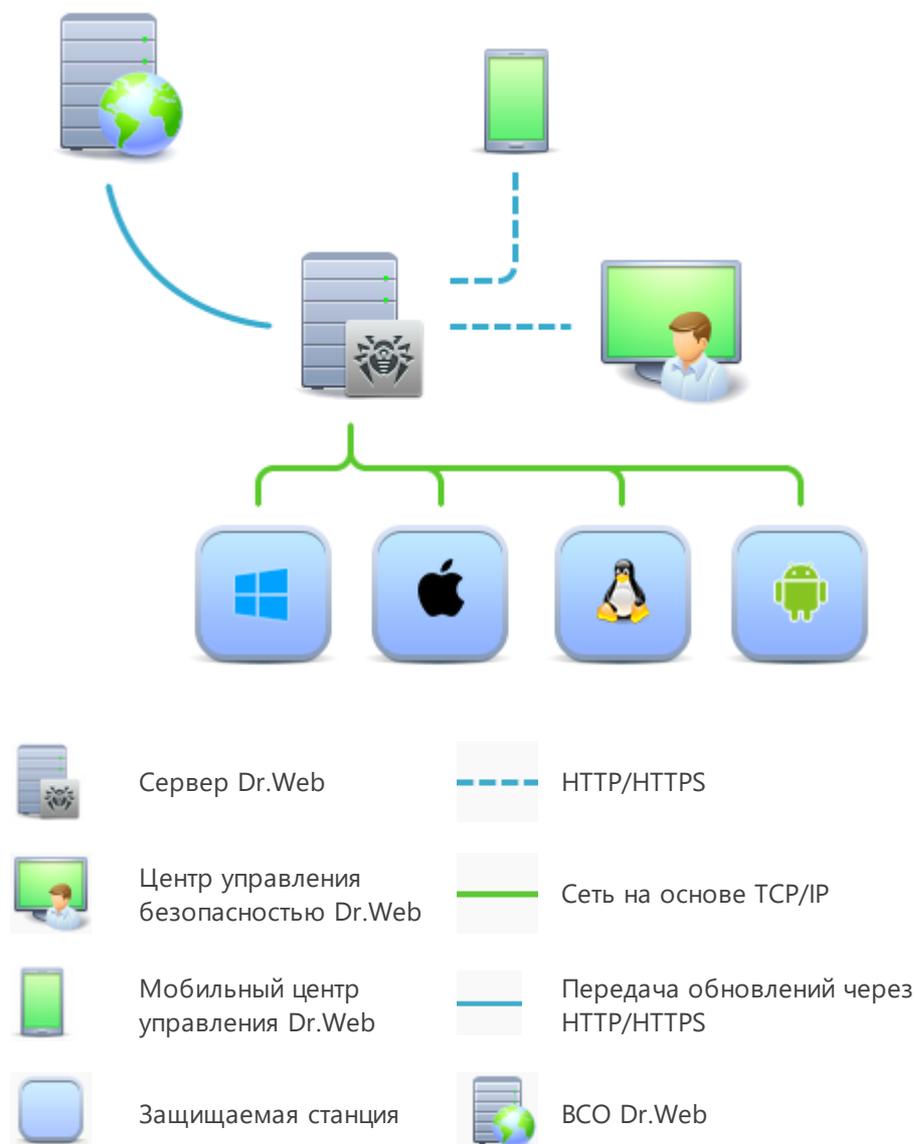


Рисунок 1. Логическая структура антивирусной сети



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 файловых серверов Unix

Защита файловых 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 Server Security Suite

3.1. Функции Dr.Web Server Security Suite

В настоящем документе рассматриваются аспекты настройки компонентов, входящих в продукт Dr.Web Server 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 Server 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 Server 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:**



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



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

3. **Надежная изоляция 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 Server Security Suite

Для защиты файловых серверов Unix предоставляются следующие антивирусные компоненты:

Основные

SplDer 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.

SplDer Guard для SMB

Монитор разделяемых каталогов Samba. Работает в резидентном режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие



файла, а также операции чтения и записи) в каталогах, отведенных для файловых хранилищ SMB-сервера Samba. Отправляет новые и измененные файлы на проверку компоненту File Checker. Для интеграции с файловым сервером использует модули VFS SMB, работающие на стороне сервера Samba.

SplDer Guard для NSS

Монитор томов NSS (Novell Storage Services). Работает в резидентном режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции записи) на томах NSS, смонтированных в указанную точку файловой системы. Отправляет новые и измененные файлы на проверку компоненту File Checker.

Dr.Web ClamD

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

Карантин

Используется SplDer Guard для изоляции вредоносных и подозрительных объектов.

Служебные

Агент Dr.Web для Unix

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

Dr.Web ConfigD

Координирует работу всех компонентов Dr.Web Server 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 Server Security Suite. Предоставляет веб-интерфейс управления.

3.3. Режимы работы Dr.Web Server Security Suite

Антивирусное решение Dr.Web Server 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 Server 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 Server Security Suite полностью управляется с защищаемого компьютера. Обновления вирусных баз получают 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 Server 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 Server 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 Server Security Suite, включая статистику инцидентов, связанных с вредоносным ПО. Обновление вирусных баз также выполняется с сервера централизованной защиты.
- В *мобильном режиме* Dr.Web Server 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 Server Security Suite), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

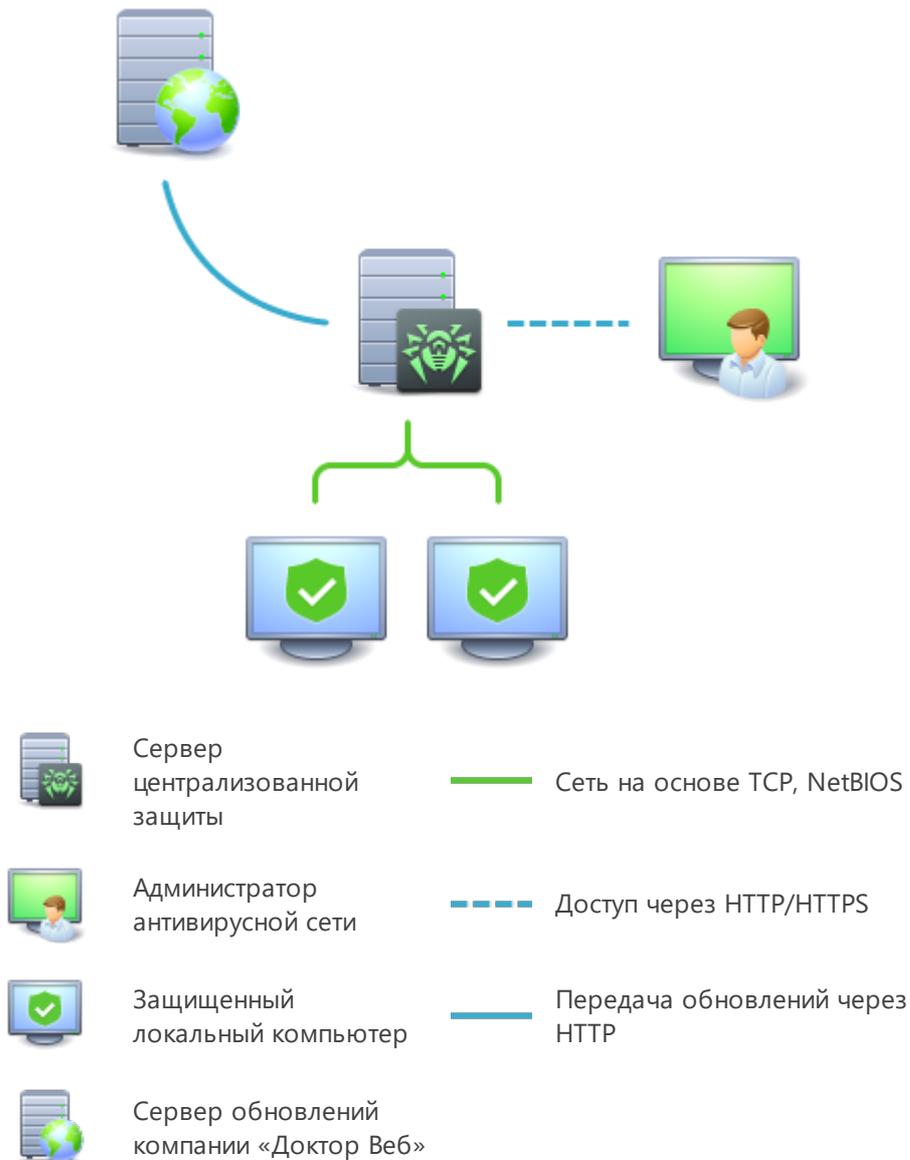


Рисунок 2. Логическая структура антивирусной сети

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



Продукт Dr.Web Server 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 Server 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 Server 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 Server Security Suite.

Если Dr.Web Server 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 Server Security Suite в мобильный режим работы зависит от разрешений, заданных на используемом сервере централизованной защиты.

Отключение от сервера централизованной защиты

Dr.Web Server 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 Server 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 внесения каких-либо изменений в настройки при помощи Центра управления, для принятия этих изменений, нажмите кнопку **Сохранить**. Настройки будут переданы на станции. Если станции были отключены в момент внесения изменений, настройки будут переданы в момент подключения станций к Серверу.



Администратор может запретить пользователю редактировать настройки на станции (см. раздел **Права пользователей станции** в Руководстве администратора). При этом редактировать настройки сможет только сам администратор через Центр управления.

3.4.1. Настройки SplDer Guard

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



Монитор файловой системы SplDer Guard может использовать два режима работы:

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



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

3.4.1.2. 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 1. 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

3.4.1.3. Контейнеры

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

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



Помните, что увеличение допустимого уровня вложенности уменьшает скорость проверки.

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

3.4.1.4. 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.

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

3.4.2. Настройки SplDer Guard для SMB

3.4.2.1. Общие настройки

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

- **Запускать компонент при старте** — управляет запуском SplDer Guard для SMB на защищаемой станции.
- **Использовать эвристический анализ** — управляет использованием SplDer Guard для SMB на защищаемой станции эвристического анализа при проверке файлов «на лету». Использование эвристического анализа замедляет проверку, но повышает ее надежность.
- **Размер кэша проверенных файлов** — определяет размер кэша, в котором SplDer Guard для SMB временно сохраняет результаты проверки файлов.
- **Время проверки одного файла** — определяет максимальный период времени, который отводится на проверку одного файла SplDer Guard для SMB на станции. Допустимые значения: от 1 секунды до 1 часа. Значение по умолчанию: 30 секунд.

3.4.2.2. Действия

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

- **Создавать файл с причиной блокировки** — установите этот флажок, чтобы SplDer Guard для SMB создавал в разделяемом каталоге рядом с инфицированным файлом специальный файл, содержащий причину его блокировки.
- **Блокировать файл для доступа при ошибке проверки** — установите этот флажок, чтобы SplDer Guard для SMB блокировал доступ к тем файлам в разделяемом каталоге, которые не удалось проверить.



- **Период задержки перед применением действия** — задайте период времени, в течение которого файл после обнаружения угрозы будет заблокирован до применения к нему действия (см. ниже).

Типы угроз, на которые может реагировать SpIDer Guard для SMB:

- **Вредоносные** — в проверенном файле обнаружена известная угроза;
- **Подозрительные** — проверенный файл отмечен как *подозрительный*;
- **Неизлечимые** — в файле была обнаружена угроза, к которой невозможно применить действие «лечить»;
- **Рекламные программы** — в проверенном файле обнаружена рекламная программа;
- **Программы дозвона** — в проверенном файле обнаружена программа дозвона;
- **Программы-шутки** — в проверенном файле обнаружена программа-шутка;
- **Потенциально опасные** — в проверенном файле обнаружена потенциально опасная программа;
- **Программы взлома** — в проверенном файле обнаружена программа взлома.

Доступные действия:

- **Лечить** — восстановить состояние объекта до заражения.
Данное действие возможно только для объектов, зараженных известной излечимой угрозой, за исключением троянских программ и зараженных файлов внутри составных объектов.
- **Удалять** — удалить объект, представляющий угрозу.
Наиболее эффективный способ устранения компьютерных угроз любых типов.
- **Запрещать** — сохранить файл в разделяемом каталоге, но заблокировать доступ к нему со стороны пользователей.
- **Перемещать в карантин** — поместить обнаруженную угрозу в специальный каталог, изолированный от остальной системы.
- **Сообщать** — оповестить об угрозе, не выполняя других действий.
- **Игнорировать** — пропустить объект без оповещения, не выполняя других действий.



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

Таблица 2. Действия SpIDer Guard для SMB над обнаруженными вредоносными объектами

Объект	Действие					
	Лечить	Удалять	Запрещать	Перемещать в карантин	Сообщать	Игнорировать
Вредоносные	+/*	+	+	+		



Объект	Действие					
	Лечить	Удалять	Запрещать	Перемещать в карантин	Сообщать	Игнорировать
Подозрительные		+	+	+/*	+	+
Неизлечимые		+	+	+/*		
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 для SMB составных файлов, таких, как архивы, почтовые файлы, упакованные объекты и прочие контейнеры (т. е. составные файлы, не отнесенные ни к одному из предыдущих типов).

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

Помните, что увеличение допустимого уровня вложенности уменьшает скорость проверки.

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



3.4.2.4. Пути проверки

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

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

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

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

3.4.2.5. Разделяемые каталоги

В данном разделе вы можете управлять индивидуальными параметрами SplDer Guard для SMB для сканирования файлов в различных разделяемых каталогах Samba.

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

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



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

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

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



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

3.4.2.6. Дополнительные настройки

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

Доступны следующие дополнительные настройки SplDer Guard для SMB:

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

3.4.3. Настройки SplDer Guard для NSS

3.4.3.1. Общие настройки

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

- **Запускать компонент при старте** — управляет запуском SplDer Guard для NSS на защищаемой станции.



- **Использовать эвристический анализ** — управляет использованием SpiDer Guard для NSS на защищаемой станции эвристического анализа при проверке файлов «на лету». Использование эвристического анализа замедляет проверку, но повышает ее надежность.
- **Время проверки одного файла** — определяет максимальный период времени, который отводится на проверку одного файла SpiDer Guard для NSS на станции. Допустимые значения: от 1 секунды до 1 часа. Значение по умолчанию: 30 секунд.



SpiDer Guard для NSS работает только в среде Novell Open Enterprise Server SP2 на базе операционной системы SUSE Linux Enterprise Server 10 SP3 или старше.

3.4.3.2. Действия

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

Типы угроз, на которые может реагировать SpiDer Guard для NSS:

- **Вредоносные** — в проверенном файле обнаружена известная угроза;
- **Подозрительные** — проверенный файл отмечен как *подозрительный*;
- **Неизлечимые** — в файле была обнаружена угроза, к которой невозможно применить действие «лечить»;
- **Рекламные программы** — в проверенном файле обнаружена рекламная программа;
- **Программы дозвона** — в проверенном файле обнаружена программа дозвона;
- **Программы-шутки** — в проверенном файле обнаружена программа-шутка;
- **Потенциально опасные** — в проверенном файле обнаружена потенциально опасная программа;
- **Программы взлома** — в проверенном файле обнаружена программа взлома.

Доступные действия:

- **Лечить** — восстановить состояние объекта до заражения.
Данное действие возможно только для объектов, зараженных известной излечимой угрозой, за исключением троянских программ и зараженных файлов внутри составных объектов.
- **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 3. Действия SpIDer Guard для NSS над обнаруженными вредоносными объектами

Объект	Действие			
	Лечить	Удалять	Перемещать в карантин	Сообщать
Вредоносные	+/*	+	+	
Подозрительные		+	+/*	+
Неизлечимые		+	+/*	
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

3.4.3.3. Контейнеры

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

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

Помните, что увеличение допустимого уровня вложенности уменьшает скорость проверки.

Поле **Максимальный коэффициент сжатия архива** устанавливает максимальную допустимую степень сжатия проверяемых объектов (как отношение сжатого объема



файла к несжатию). Если степень сжатия проверяемого объекта превысит указанную величину, он будет пропущен при проверке.

3.4.3.4. Пути проверки

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

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

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

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

3.4.3.5. Дополнительные настройки

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

Доступны следующие дополнительные настройки SplDer Guard для NSS:

- **Точка монтирования томов NSS** — определяет путь к каталогу в файловой системе файлового сервера, в который примонтированы защищаемые тома NSS.
- **Защищаемые тома NSS** — определяет список имен томов NSS, находящихся в точке монтирования, указанной в предыдущем параметре, и подлежащих защите монитором SplDer Guard для NSS. Если для этого параметра не указано никакого значения, все тома NSS в точке монтирования будут находиться под защитой.

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

- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом SplDer Guard для NSS.
- **Метод ведения журнала** — управляет способом сохранения сообщений SplDer Guard для NSS в журнал. Возможные значения:
 - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.



- *Syslog* — используется системный сервис syslog для ведения журнала SplDer Guard для NSS. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую syslog подсистему (метку) для сохранения сообщений от SplDer Guard для NSS.
- *Path* — сообщения журнала от SplDer Guard для NSS сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

3.4.4. Настройки Агента Dr.Web для Unix

3.4.4.1. 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 BCO, используя локальный компонент обновления, работающий на станции, либо получать обновления от Dr.Web Enterprise Security Suite, в зависимости от того, какое соединение доступно и качество какого соединения лучше).
 - *Использовать* — использовать мобильный режим, если он разрешен администратором на сервере Dr.Web Enterprise Security Suite (получать обновления с серверов BCO, используя локальный компонент обновления, работающий на станции).
 - *Запретить* — не разрешать Dr.Web Server Security Suite на станции получать обновления с серверов BCO 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.

3.4.4.2. Конфигурация

В данном разделе вы можете задавать настройки для любого из компонентов Dr.Web Server 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 Server 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.



3.4.5. 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*.

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



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



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

