Dr.WEB

Enterprise Security Suite

# Управление Dr.Web для почтовых серверов UNIX

**Dr.Web Enterprise Security Suite. Управление Dr.Web для почтовых серверов UNIX**
**Версия 12.0**
**Руководство администратора**
**28.05.2021**

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

## ООО «Доктор Веб»

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

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

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

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

**Мы благодарны пользователям за поддержку решений семейства Dr.Web!**

# Содержание

# Глава 1. Введение

## 1.1. Назначение документа

Данное руководство является частью пакета документации администратора антивирусной сети, описывающей детали реализации комплексной антивирусной защиты компьютеров и мобильных устройств компании с помощью Dr.Web Enterprise Security Suite.

Руководство адресовано администратору антивирусной сети — сотруднику организации, которому поручено руководство антивирусной защитой рабочих станций и серверов этой сети.

В руководстве приведена информация о централизованной настройке антивирусного ПО рабочих станций, осуществляемой администратором антивирусной сети через Центр управления безопасностью Dr.Web. Руководство описывает настройки антивирусного решения Dr.Web для почтовых серверов UNIX и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- **Руководство администратора** антивирусного решения Dr.Web для почтовых серверов UNIX содержит информацию о настройке антивирусного ПО, осуществляемой непосредственно на станции.
- **Документация администратора** антивирусной сети Dr.Web Enterprise Security Suite (включает **Руководство администратора**, **Руководство по установке** и **Приложения**) содержит основную информацию по установке и настройке антивирусной сети и, в частности, по работе с Центром управления безопасностью Dr.Web.

Перед прочтением документов убедитесь, что это последняя версия руководств. Руководства постоянно обновляются, и последнюю их версию можно найти на официальном веб-сайте компании «Доктор Веб» https://download.drweb.com/doc/.

# 1.2. Условные обозначения и сокращения

## Условные обозначения

В данном руководстве используются следующие условные обозначения:

| Обозначение | Комментарий |
|---|---|
|  | Важное замечание или указание. |
|  | Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание. |
| *Антивирусная сеть* | Новый термин или акцент на термине в описаниях. |
| *<IP-address>* | Поля для замены функциональных названий фактическими значениями. |
| **Сохранить** | Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса. |
| CTRL | Обозначения клавиш клавиатуры. |
| `/home/user` | Наименования файлов и каталогов, фрагменты программного кода. |
| Приложение А | Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы. |

## Сокращения

В тексте Руководства будут употребляться без расшифровки следующие сокращения:

- DNS — система доменных имен (Domain Name System),
- FQDN — полностью определенное имя домена (Fully Qualified Domain Name),
- FTP — протокол передачи файлов (File Transfer Protocol),
- HTML — язык разметки гипертекста (HyperText Markup Language),
- HTTP — протокол передачи гипертекста (HyperText Transfer Protocol),
- HTTPS — защищенный протокол передачи гипертекста (Hypertext Transfer Protocol Secure),
- IP — протокол Интернета (Internet Protocol),
- MDA — агент доставки электронной почты (Mail Delivery Agent),
- MIME — многоцелевые расширения Интернет и почты (Multipurpose Internet Mail Extensions),
- MTA — сервер электронной почты (Mail Transfer Agent),

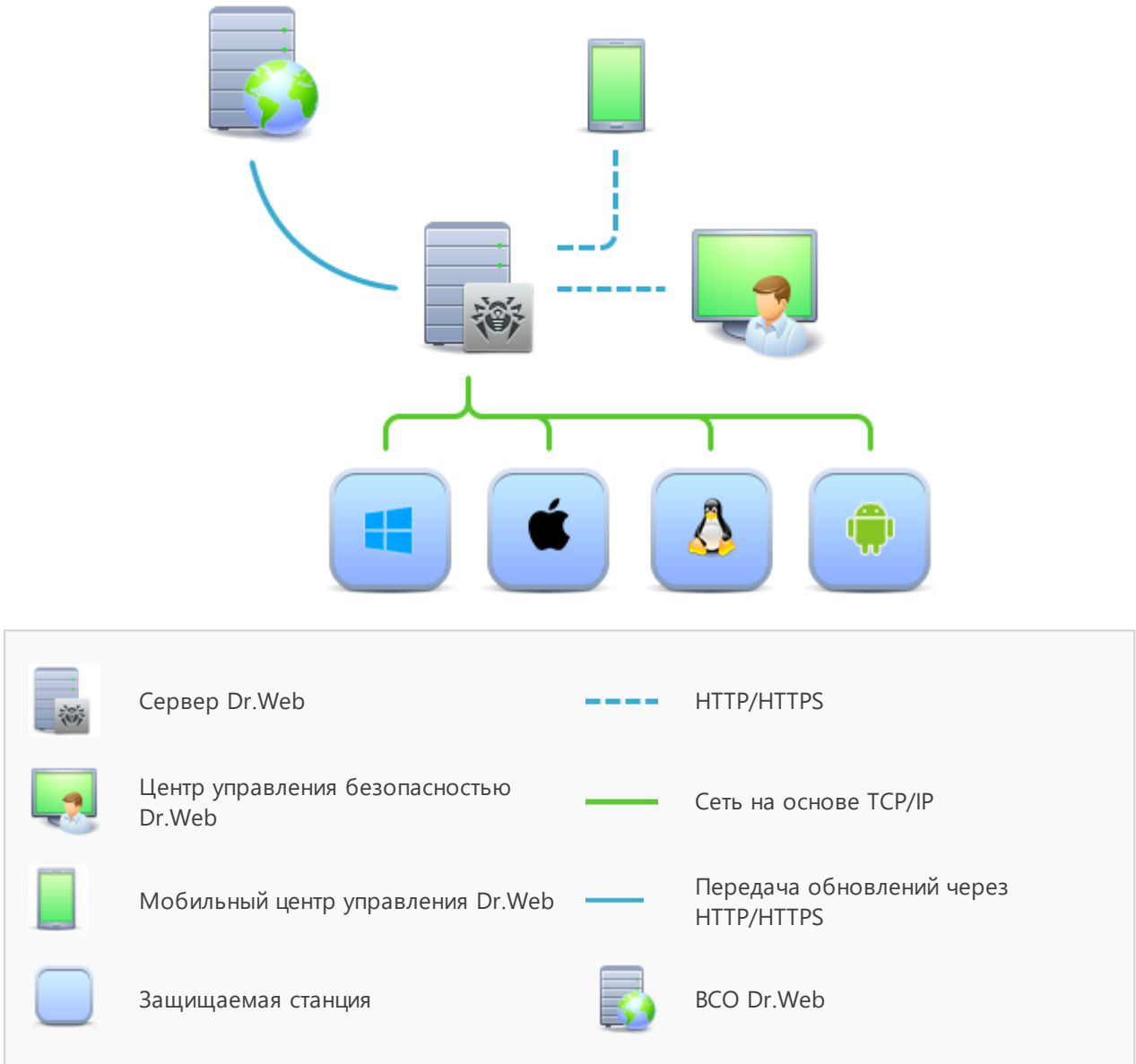
- MUA — клиент электронной почты (Mail User Agent),
- SSL — уровни защищенных сокетов (Secure Socket Layers),
- SMTP — простой протокол передачи почты ((Simple Mail Transfer Protocol),
- TCP — протокол управления передачи (Transmission Control Protocol),
- TLS — защищенный транспортный уровень (Transport Layer Security),
- URL — единообразный локатор ресурса (Uniform Resource Locator),
- ВСО — Всемирная Система Обновлений Dr.Web,
- ЛВС — Локальная Вычислительная Сеть,
- ОС — Операционная Система,
- ПО — Программное Обеспечение.

# Глава 2. Dr.Web Enterprise Security Suite

## 2.1. О продукте

Dr.Web Enterprise Security Suite предназначен для организации и управления единой и надежной комплексной антивирусной защитой как внутренней сети компании, включая мобильные устройства, так и домашних компьютеров сотрудников.

Совокупность компьютеров и мобильных устройств, на которых установлены взаимодействующие компоненты Dr.Web Enterprise Security Suite, представляет собой единую *антивирусную сеть*.




**Логическая структура антивирусной сети**

Антивирусная сеть Dr.Web Enterprise Security Suite имеет архитектуру *клиент-сервер*. Ее компоненты устанавливаются на компьютеры и мобильные устройства пользователей и администраторов, а также на компьютеры, выполняющие функции серверов ЛВС. Компоненты антивирусной сети обмениваются информацией, используя сетевые протоколы TCP/IP. Антивирусное ПО на защищаемые станции возможно устанавливать (и впоследствии управлять ими) как через ЛВС, так и через Интернет.

## 2.2. Защита станций сети

Защита рабочих станций осуществляется антивирусными пакетами Dr.Web, разработанными для соответствующих операционных систем.

Защищаемый компьютер с установленным антивирусным пакетом, в соответствии с его функциями в антивирусной сети, именуется *рабочей станцией* антивирусной сети. Необходимо помнить, что по своим функциям в локальной сети такой компьютер может быть как рабочей станцией или мобильным устройством, так и сервером локальной сети.

Антивирусные пакеты устанавливаются на защищаемых станциях и подключаются к Серверу Dr.Web. Каждая станция входит в состав одной или нескольких групп, зарегистрированных на этом Сервере. Передача информации между станцией и Сервером осуществляется по протоколу, используемому в локальной сети (TCP/IP версии 4 или 6).

### Установка

Локальная установка осуществляется на компьютере пользователя непосредственно. Может производится как администратором, так и пользователем.

Подробное описание процедур установки антивирусных пакетов на рабочие станции приведено в **Руководстве по установке** Dr.Web Enterprise Security Suite.

### Управление

При поддержке связи с Сервером Dr.Web администратору доступны следующие функции, реализуемые антивирусным пакетом на станции:

- Централизованная настройка антивирусного пакета на рабочих станциях при помощи Центра управления безопасностью.

  При этом администратор может как запретить, так и оставить возможность пользователю самостоятельно изменять настройки антивирусного пакета на станции.
- Настройка расписания антивирусных проверок и других заданий, выполняемых на станции.

- Получение статистики сканирования и прочей информации о работе антивирусных компонентов и о состоянии станции.
- Запуск и останов антивирусного сканирования и т. п. (в зависимости от функциональных возможностей антивирусного пакета, установленного на станции).

## Обновление

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

В случае временного отключения рабочей станции от антивирусной сети, антивирусный пакет на станции использует локальную копию настроек, антивирусная защита на рабочей станции сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии), но обновление ПО не производится. Если для станции разрешено функционирование в *Мобильном режиме*, при потере связи с Сервером будет доступно обновление вирусных баз непосредственно с серверов ВСО Dr.Web.

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

# Глава 3. Dr.Web для почтовых серверов UNIX

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

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

Основные функции Dr.Web для почтовых серверов UNIX:

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

   Для обнаружения угроз используются:

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

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

   При проверке файловой системы по запросу пользователя имеется возможность как полной проверки всех объектов файловой системы, доступных пользователю, так и выборочной проверки только указанных объектов (отдельных каталогов или файлов, соответствующих указанным критериям). Кроме того, доступна возможность отдельной проверки загрузочных записей томов и исполняемых файлов, из которых запущены процессы, активные в системе в данный момент. В последнем случае при обнаружении угрозы выполняется не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него.
2. **Проверка сообщений электронной почты.** Продукт поддерживает следующие режимы проверки сообщений электронной почты:

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

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

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

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

Dr.Web для почтовых серверов UNIX, в зависимости от комплектности и настроек, выполняет следующие проверки сообщений электронной почты:

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

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

## 3.1. Компоненты Dr.Web для почтовых серверов UNIX

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

### Основные

*Dr.Web MailD*

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

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

*Dr.Web Anti-Spam Engine*

Компонент проверки сообщений электронной почты на наличие признаков спама. Используется компонентом *Dr.Web MailD*, может отсутствовать в составе Dr.Web для почтовых серверов UNIX на станции.

*SpIDer Gate*

Компонент проверки сетевого трафика и URL. Предназначен для проверки данных, загружаемых на локальный узел из сети и передаваемых с него во внешнюю сеть, на наличие угроз, и предотвращения соединения с узлами сети, внесенными в как в

нежелательные категории веб-ресурсов, так и в черные списки, формируемые системным администратором.

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

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

*Консольный сканер (управляется только на станции)*

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

*Dr.Web ClamD*

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

*Карантин*

Используется для изоляции вредоносных и подозрительных объектов в специальном каталоге.

Файлы с угрозами могут быть помещены в карантин только компонентом *Консольный сканер*.

---

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

## Вспомогательные

*Агент Dr.Web для UNIX*

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

*File Checker*

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

*Network Checker*

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

*Scanning Engine*

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

*SNMP Agent*

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

*Dr.Web ConfigD*

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

*Dr.Web CloudD*

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

*Dr.Web LookupD*

Компонент, осуществляющий при помощи протокола LDAP выборку данных из служб каталогов (таких как **Active Directory**) для использования их в правилах проверки сетевого трафика.

*Dr.Web HTTPD*

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

## 3.2. Настройка Dr.Web для почтовых серверов UNIX

**Чтобы просмотреть или изменить настройки антивирусных компонентов на рабочей станции:**

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
2. В открывшемся окне в иерархическом списке нажмите на название станции под требуемой ОС (**Linux**, **Solaris** или **FreeBSD**) или группы, содержащей такие станции.
3. В открывшемся управляющем меню в разделе **Конфигурация**, в подразделе ОС **UNIX** выберите требуемый компонент.
4. Откроется окно настроек антивирусного компонента.

   Управление настройками антивирусных компонентов через Центр управления имеет некоторые отличия от управления настройками непосредственно через соответствующие компоненты антивируса на станции:

   - для управления отдельными параметрами используйте кнопки, расположенные справа от соответствующих настроек:

     **Установить в начальное значение** — восстановить значение, которое параметр имел до редактирования (последнее сохраненное значение).

**Сбросить в значение по умолчанию** — установить для параметра значение по умолчанию.

- для управления совокупностью всех параметров раздела используйте кнопки на панели инструментов:

  **Установить все параметры в начальные значения** — восстановить значения, которые все параметры данного раздела имели до текущего редактирования (последние сохраненные значения).

  **Установить все параметры в значения по умолчанию** — установить для всех параметров данного раздела значения, заданные по умолчанию.

  **Распространить эти настройки на другой объект** — скопировать настройки из данного раздела в настройки другой станции, группы или нескольких групп и станций.

  **Установить наследование настроек от первичной группы** — удалить персональные настройки станций и установить наследование настроек данного раздела от первичной группы.

  **Скопировать настройки из первичной группы и установить их в качестве персональных** — скопировать настройки данного раздела из первичной группы и задать их для выбранных станций. Наследование при этом не устанавливается, и настройки станции считаются персональными.

  **Экспортировать настройки из данного раздела в файл** — сохранить все настройки из данного раздела в файл специального формата.

  **Импортировать настройки в данный раздел из файла** — заменить все настройки в данном разделе настройками из файла специального формата.

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

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

## 3.2.1. Настройки Dr.Web MailD

Раздел **Dr.Web MailD** содержит следующие настройки функционирования Dr.Web для почтовых серверов UNIX:

- Общие — настройка основных параметров работы компонента.
- Шаблоны уведомлений — настройка параметров почтовых уведомлений клиентам.
- Подключения через Milter — настройка подключения к почтовым системам через интерфейс *Milter*.

- Подключения через Spamd — настройка подключения к почтовым системам через интерфейс *Spamd*.
- Подключения через Rspamd — настройка подключения к почтовым системам через интерфейс *Rspamd*.

### 3.2.1.1. Общие

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

- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Dr.Web MailD.
- **Метод ведения журнала** — управляет способом сохранения сообщений Dr.Web MailD в журнал. Возможные значения:
  - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
  - *Syslog* — используется системный сервис **syslog** для ведения журнала Dr.Web MailD. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от Dr.Web MailD.
  - *Path* — сообщения журнала от Dr.Web MailD сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.
- **Пользователь** — позволяет указать имя пользователя UNIX, с правами и полномочиями которого работает компонент на защищаемом почтовом сервере.

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

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

### 3.2.1.2. Шаблоны уведомлений

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

- **Каталог шаблонов** — задает путь к каталогу, в котором располагаются шаблоны генерации писем, сообщающим клиентам об обнаруженных угрозах.

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

### 3.2.1.3. Подключения через Milter

В данном разделе вы можете управлять параметрами взаимодействия Dr.Web MailD на защищаемом почтовом сервере с почтовыми системами (MTA) через интерфейс *Milter*:

- **Эвристический анализ** — управляет использованием Dr.Web MailD эвристического анализа для поиска неизвестных угроз в письмах, поступающих на проверку через интерфейс *Milter*. Использование эвристического анализа замедляет проверку, но повышает ее надежность.
- **Тайм-аут на проверку одного письма** — определяет максимальный период времени, который отводится на проверку одного письма, поступившего на проверку через интерфейс *Milter*. Если указано *0*, время проверки одного письма не ограничивается.
- **Максимальный уровень вложенности.** В данном разделе вы можете управлять параметрами проверки Dr.Web MailD вложенных в письма составных файлов, таких, как архивы, почтовые файлы, упакованные объекты и прочие контейнеры (т. е. составные файлы, не отнесенные ни к одному из предыдущих типов).

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

  Помните, что увеличение допустимого уровня вложенности уменьшает скорость проверки.

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

- **Сокет для подключения MTA через Milter** — задает сокет для подключения к MTA (на этот сокет MTA будет выполнять подключение при использовании Dr.Web MailD как *Milter*-фильтр). Допускается указание UNIX-сокета (пути в локальной файловой системе защищаемого сервера) или сетевого сокета (пары *IP-адрес*:*порт*).
- **Блокировать непроверенные почтовые сообщения** — установите этот флажок, если вы хотите блокировать сообщения, поступившие на проверку через интерфейс *Milter*, которые Dr.Web MailD не смог проверить.
- **Правила проверки почты через Milter** — укажите в этой секции правила проверки, которые Dr.Web MailD будет применять к письмам, поступившим через интерфейс *Milter*.

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

  Чтобы ознакомиться с правилами проверки, см. Приложение А. Правила проверки трафика.

### 3.2.1.4. Подключения через Spamd

В данном разделе вы можете управлять параметрами взаимодействия Dr.Web MailD на защищаемом почтовом сервере с почтовыми системами (MTA) через интерфейс *Spamd*:

Параметры работы аналогичны тем, что задаются в секции Подключения через Milter.

### 3.2.1.5. Подключения через Rspamd

В данном разделе вы можете управлять параметрами взаимодействия Dr.Web MailD на защищаемом почтовом сервере с почтовыми системами (MTA) через интерфейс *Rspamd*:

Параметры работы аналогичны тем, что задаются в секции Подключения через Milter.

## 3.2.2. Настройки SplDer Gate

В разделе **SplDer Gate** представлены следующие разделы настройки функционирования Dr.Web для почтовых серверов UNIX:

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

### 3.2.2.1. Общие

В данном разделе вы можете управлять следующими параметрами SpIDer Gate на защищаемой станции (Интернет-шлюзе):

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

### 3.2.2.2. Действия

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

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

### 3.2.2.3. 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 сети Интернет.
- В списке **Блокировать следующие категории сайтов** выберите категории интернет-ресурсов, доступ к которым необходимо заблокировать.
- В разделах **Белый список**/**Черный список** добавьте пути к сайтам, доступ к которым нужно разрешить/ограничить:

- Чтобы добавить в список определенный сайт, введите полный адрес его домена (например, `www.example.com`). Доступ ко всем ресурсам, расположенным на этом домене, будет определяться данной записью.

### 3.2.2.4. 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.

### 3.2.2.5. Дополнительно

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**.

## 3.2.3. Настройки Агента Dr.Web для UNIX

В разделе **Агент Dr.Web** представлены следующие разделы настройки функционирования Dr.Web для почтовых серверов UNIX:

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

### 3.2.3.1. Общие

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

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

выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от Агента Dr.Web для UNIX.

- *Path* — сообщения журнала от Агента Dr.Web для UNIX сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

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

### 3.2.3.2. Конфигурация

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

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

Обратите внимание, что:

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

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

### 3.2.4. Настройки File Checker

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

Доступны следующие настройки:

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

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

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

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

### 3.2.5. Настройки Scanning Engine

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

Доступны следующие настройки:

- **Путь к файлу сокета фиксированной копии компонента** — определяет путь к файлу UNIX-сокета постоянно работающей копии Scanning Engine. Этот сокет может использоваться для сканирования файлов внешними программами. Если параметр пуст, сканирование недоступно для внешних программ, а Scanning Engine запускается и завершает свою работу автоматически, по мере необходимости.
- **Количество сканирующих процессов** — определяет количество вспомогательных процессов, которые Scanning Engine может создать при сканировании файлов. При изменении значения этого параметра следует учесть количество процессорных ядер, доступных на защищаемой станции.
- **Сторожевой таймер** — определяет период времени, который Scanning Engine использует для автоматического обнаружения зависания вспомогательных сканирующих процессов.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Scanning Engine.
- **Метод ведения журнала** — управляет способом сохранения сообщений Scanning Engine в журнал. Возможные значения:
  - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
  - *Syslog* — используется системный сервис **syslog** для ведения журнала Scanning Engine. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от Scanning Engine.
  - *Path* — сообщения журнала от Scanning Engine сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

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

### 3.2.6. Настройки Dr.Web ConfigD

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

Доступны следующие настройки:

- **Путь к публичному коммуникационному сокету** — определяет путь к UNIX-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web для почтовых серверов UNIX.
- **Путь к административному коммуникационному сокету** — определяет путь к UNIX-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web для почтовых серверов UNIX, работающими с полномочиями суперпользователя.
- **Путь к каталогу временных файлов** — определяет каталог, в котором компоненты Dr.Web для почтовых серверов UNIX хранят свои временные файлы.
- **Путь к каталогу PID-файлов и файлов коммуникационных сокетов** — определяет каталог, в котором компоненты Dr.Web для почтовых серверов UNIX хранят PID-файлы и UNIX-сокеты для внутреннего взаимодействия.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Dr.Web ConfigD.
- **Метод ведения журнала** — управляет способом сохранения сообщений Dr.Web ConfigD в журнал. Возможные значения:
  - *Syslog* — используется системный сервис **syslog** для ведения журнала Dr.Web ConfigD. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую **syslog** подсистему (метку) для сохранения сообщений от Dr.Web ConfigD.
  - *Path* — сообщения журнала от Dr.Web ConfigD сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

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

# Приложение А. Правила проверки трафика

Правила представляют собой цепочку продукций вида ЕСЛИ <*условие*> ТО <*действие*>. При этом в части <*условие*> перечисляются проверки вида *«Переменная (не) имеет заданное значение»* или *«Значение переменной (не) входит в указанное множество»*, а <*действие*> содержит *конечную резолюцию* (пропустить или заблокировать трафик), или действие вида *«Присвоить переменной значение»* или *«Добавить указанное значение к множеству значений переменной»*.

Часть <*действие*> правила выполняется, только если истинна часть <*условие*>. Если <*условие*> ложно, действие не выполняется, осуществляется переход к следующему правилу. Правила перебираются сверху вниз до тех пор, пока не сработает какая-либо конечная резолюция. После этого все нижележащие правила игнорируются.

## Формат правил

Формат продукции правила имеет вид:

```
[<условие>[, <условие>[, ...]]] : <действие>
```

Условная часть правила (перед '`:`') может отсутствовать, в этом случае часть <*действие*> выполняется безусловно. Если условная часть правила отсутствует, то разделитель '`:`' может быть опущен. Запятая между условиями в условной части играет роль конъюнкции (т. е. логического «И»), и условная часть считается истинной, только если истинны все перечисленные в ней условия. Ключевые слова, имена переменных и параметров из конфигурации в правилах не чувствительны к регистру.

## Условия

В условной части правил могут встречаться следующие типы условий:

| Условие | Смысл условия |
|---|---|
| <*переменная*> <*значение*> | Значение указанной переменной совпадает с заданным.<br><br>*Может быть использовано только для переменных, которые не могут принимать множества значений.* |
| <*переменная*> `[not] in` <*множество значений*> | Значение указанной переменной содержится в указанном множестве значений (*для not — не совпадает ни с одним из значений указанного множества*). |

| Условие | Смысл условия |
|---|---|
| <*переменная*> `[not] match` <*множество значений*> | Значение указанной переменной соответствует любому регулярному выражению из указанного набора (*для not — не соответствует ни одному из выражений в указанном наборе*).<br><br>Регулярные выражения записываются с использованием синтаксиса *POSIX* (*BRE*, *ERE*) или *Perl* (*PCRE*, *PCRE2*). |
| <*переменная*> `[not] gt` <*значение*> | Значение указанной переменной (не) больше заданного.<br><br>*Может быть использовано только для переменных, которые принимают единственное числовое значение.* |
| <*переменная*> `[not] lt` <*значение*> | Значение указанной переменной (не) меньше заданного.<br><br>*Может быть использовано только для переменных, которые принимают единственное числовое значение.* |

*) Необязательное ключевое слово `not` обозначает отрицание.

Часть <*множество значений*>, с которым сравнивается переменная, может быть указано следующим способами:

| Запись | Смысл |
|---|---|
| `(`<*значение 1*>`[, `<*значение 2*>`[, ...]])` | В скобках перечисляется непосредственно множество проверяемых значений (не менее одного). Для случая с одним значением и использованием условия `in` скобки можно опустить (получится случай <*переменная*> <*значение*>). |
| "<*секция*>.<*параметр*>" | Множество значений некоторого параметра конфигурации, где в кавычках указывается имя параметра из конфигурации (с указанием содержащей его секции), значение (или набор значений) которого проверяется.<br><br>Перечни параметров, которые можно использовать в условии, зависят от |

| Запись | Смысл |
|---|---|
| | компонента, для которого заданы правила, и приведены ниже. |
| `file("<имя файла>")` | Перечень значений считывается из текстового файла <*имя файла*> (одна строка файла — один элемент списка, ведущие и завершающие пробелы в строках не учитываются). Путь к файлу должен быть абсолютным. Кавычки и апострофы, если они встречаются в <*имя файла*>, необходимо экранировать символом косой черты '\'.<br>  <br>Размер файла не должен быть больше 64 МБ.<br><br>Содержимое файла считывается и подставляется в правила один раз — при запуске Dr.Web для почтовых серверов UNIX. Если указанный файл отсутствует или его размер слишком велик, при загрузке настроек будет выдана ошибка `x102`.<br><br>В случае если содержимое файла изменено в процессе работы программного комплекса, для применения внесенных изменений необходимо после сохранения файла перезагрузить Dr.Web для почтовых серверов UNIX.<br><br>Не для всех переменных можно получать множество значений из файла. Для каждой переменной ниже указывается, можно ли использовать для проверки ее значений множество значений, получаемые из файла. |
| <*mun_LOOKUP_запроса*>`@`<*тег*>`[@`<*значение*>`]` | Множество значений запрашивается через Dr.Web LookupD у внешнего источника данных (LDAP, ActiveDirectory), где <*mun_LOOKUP_запроса*> — это тип источника (LDAP или AD); <*тег*> — это имя секции, |

| Запись | Смысл |
|---|---|
| | описывающей подключение для выборки проверяемого параметра, а необязательное <*значение*> — значение, которое должно находиться в множестве значений, извлеченных из источника данных.<br><br>Не для всех переменных можно получать значения через Dr.Web LookupD. Также не для всех переменных используется условие <*проверка*>. Для каждой переменной ниже указывается, можно ли использовать для проверки ее значений значения, получаемые через Dr.Web LookupD. |
| `dnsxl(`<*DNSxL-сервер 1*>`[: [mask] `<*IP*>`] [, ...])` | В скобках перечисляется перечень DNSxL-серверов (DNSBL и т. п.), которые должны проверить вхождение IP-адреса, или FQDN (предварительно разрешенного до IP-адреса) в свои списки IP-адресов.<br><br>Если проверяемый IP-адрес зарегистрирован в списках некоторого из перечисленных в скобках DNSxL-серверов, то в ответе этого сервера присутствует одна или более DNS-записей типа A, причем возвращаемый сервером фиктивный IP-адрес может содержать в себе причину, по которой проверяемый IP-адрес был внесен в списки данного сервера (как правило, тип причины определяется значением последнего октета возвращенного фиктивного IP-адреса). Для каждого DNSxL-сервера в списке можно указать проверку на ожидаемое возвращенное значение фиктивного IP-адреса. Проверка указывается после двоеточия в форме:<br>• <*DNSxL-сервер*>: <*IP-адрес*><br>• <*DNSxL-сервер*>: *mask* <*IP-адрес*><br><br>В первом случае указывается требование, чтобы возвращенный сервером <*DNSxL-сервер*> фиктивный IP-адрес в точности совпадал бы с указанным адресом <*IP-адрес*>. Во втором случае указывается требование, |

| Запись | Смысл |
|---|---|
| | чтобы возвращенный сервером <*DNSxL-сервер*> фиктивный IP-адрес в точности равнялся бы указанной маске в ее ненулевых октетах. Если параметры проверки не указаны, то условие сработает, если <*DNSxL-сервер*> вернет любой фиктивный IP-адрес в ответ на запрос.<br><br>**Примеры:**<br><br>`<IP> in dnsxl("dnsxl.server.org")` — для IP-адреса, содержащегося в переменной <*IP*>, сервер должен вернуть любой фиктивный IP-адрес;<br>`<IP> in dnsxl("dnsxl.server.org": 127.0.0.2)` — для IP-адреса, содержащегося в переменной <*IP*>, сервер должен вернуть фиктивный IP-адрес `127.0.0.2`;<br>`<IP> in dnsxl("dnsxl.server1.org": mask 0.0.0.8, "dnsxl.server2.org": 127.0.0.3, "dnsxl.server3.org")` — для IP-адреса, содержащегося в переменной <*IP*>, либо первый сервер вернет фиктивный IP-адрес с младшим октетом `8`, либо второй — фиктивный IP-адрес `127.0.0.3`, либо третий — любой фиктивный IP-адрес.<br><br>Использование инструкции проверки <*переменная*> `in dnsxl(`<*список серверов*>`)` допустимо только в том случае, если <*переменная*> представляет собой IP-адрес или доменное имя, которое может быть разрешено службой DNS до IP-адреса (FQDN).<br><br>Таким образом, в качестве переменной для данного условия могут быть использованы только следующие переменные: `src_ip`, `url_host` (см. ниже). |

## Действия

Действия делятся на *конечные* резолюции, определяющие запрет или разрешение на пропуск трафика; *модифицирующие* резолюции, не прерывающие проверку, а фиксирующие действие, которое должно быть применено к соединению или проверяемому объекту по достижении резолюции, разрешающей пропуск трафика, и *действия, изменяющие значения некоторой переменной*, что может быть использовано при проверке нижележащих условий.

### Конечные резолюции

| Резолюция | Описание (смысл) |
|---|---|
| **Общие резолюции** | |
| `PASS` | Пропустить трафик (разрешить создать соединение). Последующие правила (если имеются) не проверяются.<br><br>Для правил обработки почты имеет смысл команды пропуска письма к получателю, применив к нему все накопленные изменения (т. е. все сработавшие действия `REPACK`, `ADD_HEADER`, `CHANGE_HEADER`, см. ниже). |
| `BLOCK as <reason>` | Заблокировать трафик (отказать в создании соединения). Последующие правила (если имеются) не проверяются.<br><br>В журнале фиксируется, что блокировка случилась по причине <*reason*>. Эта же причина используется для определения, какую страницу с уведомлением показать пользователю в браузере. В качестве <*reason*> для `BLOCK` может быть использовано две стандартные причины:<br>• `BlackList` — считается, что данные заблокированы по причине попадания в черный список пользователя.<br>• `_match` — причиной блокировки является попадание веб-ресурса или файла с угрозой в категорию, из-за которой сработало правило (для условий `*_category in (...)`). Переменная `_match` хранит список блокируемых категорий, для которых сработало соответствие.<br><br>*Для правил обработки почты данное действие является синонимом действия* `REJECT`. *Причина блокировки* <*reason*> *при этом игнорируется* |
| **Специальные резолюции для правил обработки почты** | |
| `REJECT ["<description>"]` | Отклонить письмо (не допустить его прием или отправку).<br><br>В случае работы с данными, передаваемыми по протоколу SMTP, сформировать код ответа SMTP 541 (класс постоянных ошибок). Необязательный параметр <*description*>, если указан, будет |

| Резолюция | Описание (смысл) |
|---|---|
| | использован в качестве ответа. При проверке письма, поступившего от MTA через интерфейс *Spamd/Rspamd*, <*description*> будет использовано как значение заголовка 'Message', добавленного к письму после сообщения результатов проверки. |
| TEMPFAIL ["<*description*>"] | Ответить отправителю ошибкой типа «временная ошибка».<br><br>В случае работы с данными, передаваемыми по протоколу SMTP, сформировать код ответа SMTP 451 (класс временных ошибок). Необязательный параметр <*description*>, если указан, будет использован в качестве ответа. При проверке письма, поступившего от MTA через интерфейс *Spamd/Rspamd*, <*description*> будет использовано как значение заголовка 'Message', добавленного к письму после сообщения результатов проверки. |
| DISCARD | Отвергнуть письмо, т. е. принять его без возврата отправителю кода ошибки, но уничтожить его вместо передачи получателю. |

### Модифицирующие резолюции

Модифицирующие резолюции не прерывают проверку правил, а фиксируют действия, которые должны быть применены к проверяемым данным по достижении разрешающей резолюции PASS.

| Резолюция | Описание (смысл) |
|---|---|
| REPACK [<*reason*>] | Перепаковать сообщение, т. е. создать (на основе одного из предопределенных шаблонов) новое сообщение, содержащее содержимое из старого сообщения и некоторый текст, информирующий получателя о наличии угроз. Вырезанное нежелательное содержимое помещается в архив, защищенный паролем. Данный архив будет добавлен к сообщению, отправленному получателю, как вложение. Продолжить проверку почтового сообщения до достижения резолюции *PASS*. Имеются следующие предопределенные шаблоны перепаковки:<br>1. *Сообщение признано спамом*;<br>2. *Наличие в сообщении одной или более угроз*;<br>3. *Наличие в сообщении одного или более вредоносных/нежелательных URL*;<br>4. *Нарушение сообщением политик безопасности, указанных администратором*. |

| Резолюция | Описание (смысл) |
|---|---|
| | В журнале фиксируется, что перепаковка случилась по причине <*reason*>. Эта же причина используется для определения, на основании какого из четырех шаблонов сформировать письмо-уведомление получателю. В качестве <*reason*> для `REPACK` могут быть использованы следующие причины:<br>• `as _match` — причиной перепаковки является признание письма спамом, попадание веб-ресурса или файла с угрозой, содержащихся в письме, в категорию, из-за которой сработало правило (для условий `*_category in (...)`). Переменная `_match` хранит список нежелательных категорий, для которых сработало соответствие. Для перепаковки выбирается шаблон 1, 2 или 3 (см. выше), в зависимости от того, что было обнаружено в сообщении:<br>▫ если сообщение признано спамом, то выбирается шаблон 1;<br>▫ если найдена хотя бы одна угроза, то выбирается шаблон 2;<br>▫ если найден хотя бы один вредоносный/нежелательный URL, то шаблон 3;<br>▫ если угроз не обнаружено, то выбирается шаблон 4.<br>• "*текстовое сообщение*" — письмо перепаковано в силу срабатывания настроек, заданных администратором, а сообщение указывает произвольное сообщение от администратора. Например: `REPACK "Virus found!"`. Для перепаковки будет выбран шаблон 4. |
| `ADD_HEADER("<Name>", "<Value>")` | Добавить в письмо заголовок <*Name*> со значением <*Value*> и продолжить проверку письма до достижения резолюции *PASS*. Например: `ADD_HEADER ("X-SPAM", "Virus found!")`.<br><br>Значение перекодируется в ASCII в соответствии с RFC 2047. |
| `CHANGE_HEADER("<Name>", "<Value>" \| _value [+ "<Value>" \| _value [+ ...]])` | Заменить значение первого найденного заголовка с именем <*Name*>. Новое значение — конкатенация значений после запятой, разделённых символом '+'. Каждое значение может быть либо строковым |

| Резолюция | Описание (смысл) |
|---|---|
| | литералом в кавычках, либо специальной переменной `_value`, в которую подставляется исходное значение модифицируемого заголовка. Продолжить проверку письма до достижения резолюции *PASS*. Например: `CHANGE_HEADER("Subject", "[SPAM] '" + _value + "' (do not read!)")`. |

Особенности обработки резолюций:

- `BLOCK as BlackList` всегда отрабатывает как *«попал в черный список»* (вне зависимости от того, что за условие указано в правиле с данной резолюцией).
- `BLOCK as _match`, если в `_match` не пусто, отрабатывает как *«попал в _match категорию(и)»*.
- `BLOCK as _match`, если в `_match` пусто, отрабатывает как *«попал в черный список»* (вне зависимости от того, что за условие указано в правиле с данной резолюцией).
- Если были просмотрены все правила, а ни одно правило с резолюцией не сработало (или резолюции отсутствуют в правилах), то это равносильно применению к соединению действия `PASS`.

**Изменение значения переменной**

Для изменения значения переменной используется инструкция

```
SET <переменная> = ([<значение 1>[, <значение 2>[, ...]]])
```

Если скобки пустые — это означает очистку списка значений переменной. Для случая с одним значением скобки необходимо опустить, т. е. использовать синтаксис

```
SET <переменная> = <значение>
```

## Переменные, используемые в правилах

При указании переменных в правилах регистр символов не учитывается. Переменные, название которых состоит из нескольких слов, могут быть записаны с использованием подчеркивания для разделения слов, или записаны без подчёркивания. Таким образом, записи `variable_name`, `VariableName` и `variablename` представляют одну и ту же переменную. В данном разделе все переменные записаны с использованием подчеркивания (т. е. используется вариант написания `variable_name`).

### Переменные общего назначения

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| `protocol` | Тип сетевого протокола, используемого соединением.<br><br>*Переменная может принимать множество значений.*<br><br>**Возможные значения:** `HTTP`, `SMTP`, `IMAP`, `POP3`.<br><br>**Особенности использования:**<br>• Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL.<br>• Множество значений для проверки значения переменной можно получать из файла.<br><br>**Примеры:**<br>`protocol in (HTTP, SMTP)`<br>`protocol in (POP3)`<br>`protocol in file("/etc/file")` | Да | Нет |
| `sni_host` | SNI (адрес) хоста, с которым устанавливается соединение через SSL/TLS.<br><br>**Особенности использования:**<br>• Если SSL не используется, то значение переменной не определено, условие будет ложным.<br>• Множество значений для проверки значения переменной можно получать из файла.<br><br>**Примеры:**<br>`sni_host not in ('vk.com', 'ya.ru')`<br>`sni_host in "LinuxFirewall.BlackList"`<br>`sni_host in file("/etc/file")` | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| `sni_category` | Список категорий, к которым в базах категорий веб-ресурсов относится хост (определенный по SNI), с которым устанавливается соединение через SSL/TLS (*AdultContent*, и т. п.).<br><br>*Переменная может принимать множество значений.*<br><br>**Особенности использования:**<br>• Если SSL не используется, то значение переменной не определено, условие будет ложным.<br>• Для правил, используемых Dr.Web MailD, условие с `not in` будет *истинным*, даже если по результатам проверки хост не принадлежит никакой из предопределенных категорий («безопасный» хост).<br>• Если базы данных категорий веб-ресурсов не установлены, то переменную нельзя использовать в правилах (попытка проверить истинность условия в правиле будет приводить к ошибке x112).<br>• Множество значений для проверки значения переменной можно получать из файла.<br><br>**Примеры:**<br>`sni_category not in (AdultContent, Chats)`<br>`sni_category in "LinuxFirewall.BlockCategory"`<br>`sni_category in (FreeEmail)`<br>`sni_category not in file("/etc/file")` | Да | Нет |
| `url_host` | URL/хост, с которым устанавливается соединение.<br><br>**Особенности использования:**<br>• Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL. | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | • Для проверки значения переменной можно использовать Dr.Web LookupD.<br>• Данная переменная может быть проверена на вхождение в черные списки DNSxL (DNSBL и т. п.).<br>• Множество значений для проверки значения переменной можно получать из файла.<br>**Примеры:**<br>`url_host in ('vk.com', 'ya.ru')`<br>`url_host not in "ICAPD.Whitelist"`<br>`url_host in LDAP@hosts`<br>`url_host not in file("/etc/file")`<br>`url_host not in dnsxl("multi.surbl.org": 127.0.0.2, "multi2.surbl.org")` | | |
| `url_category` | Список категорий, к которым (по базам категорий веб-ресурсов или по ответу из <%CLOUD_SERVICE%>) относится URL/хост, с которым установлено соединение.<br>*Переменная может принимать множество значений.*<br>**Особенности использования:**<br>• Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL.<br>• Для правил, используемых компонентами Dr.Web MailD, условие с `not in` будет *истинным*, даже если по результатам проверки URL/хост не принадлежит никакой из предопределенных категорий («безопасный» URL/хост).<br>• Если базы данных категорий веб-ресурсов не установлены, то переменную нельзя использовать в правилах (попытка проверить | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | истинность условия в правиле будет приводить к ошибке x112).<br>• Множество значений для проверки значения переменной можно получать из файла.<br>**Примеры:**<br>`url_category not in (AdultContent, Chats)`<br>`url_category in "LinuxFirewall.BlockCategory"`<br>`url_category in (FreeEmail)`<br>`url_category in file("/etc/file")` | | |
| `threat_category` | Список категорий, к которым по информации из вирусных баз относится угроза, обнаруженная в передаваемых данных.<br>*Переменная может принимать множество значений.*<br>**Особенности использования:**<br>• Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL.<br>• Для правил, используемых компонентами Dr.Web MailD, условие с `not in` будет *истинным*, даже если по результатам проверки объект не содержит угроз ни из одной из предопределенных категорий («безопасный» объект).<br>• Множество значений для проверки значения переменной можно получать из файла.<br>**Примеры:**<br>`threat_category in "LinuxFirewall.BlockThreat"`<br>`threat_category not in (Joke)`<br>`threat_category in file("/etc/file")` | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| src_ip | IP-адрес хоста, со стороны которого следует соединение.<br><br>**Особенности использования:**<br>• Для проверки значения переменной можно использовать Dr.Web LookupD.<br>• Данная переменная не может быть использована в правилах для интерфейса *Spamd*: этот протокол не предоставляет информацию об отправителе письма.<br>• Данная переменная может быть проверена на вхождение в черные списки DNSxL (DNSBL и т. п.).<br>• Множество значений для проверки значения переменной можно получать из файла.<br><br>**Примеры:**<br>`src_ip not in (127.0.0.1, 10.20.30.41, 198.126.10.0/24)`<br>`src_ip in LDAP@AllowedAddresses`<br>`src_ip not in file("/etc/file")`<br>`src_ip in dnsxl("zen.spamhouse.org": mask 0.0.0.2, "zen2.spamhouse.org")` | Да | Нет |
| proc | Процесс, устанавливающий соединение (полный путь к исполняемому файлу).<br><br>**Особенности использования:**<br>• Множество значений для проверки значения переменной можно получать из файла.<br><br>**Примеры:**<br>`proc in ('/usr/bin/ls')`<br>`proc not in ('/home/user/myapp', '/bin/bin1')`<br>`proc in` | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | `"LinuxFirewall.ExcludedProc" proc in file("/etc/file")` | | |
| `direction` | Тип трафика, идущего по соединению.<br><br>**Возможные значения:** `request` (клиентский запрос), `response` (ответ сервера).<br><br>*Переменная не может иметь множества значений, условия типа* `match` *и* `in` *неприменимы.*<br><br>**Примеры:**<br>`direction request`<br>`direction not response` | Да | Нет |
| `divert` | Направление соединения.<br><br>**Возможные значения:** `input` (входящее — создано/инициировано извне локального хоста), `output` (исходящее — создано/инициировано на локальном хосте).<br><br>*Переменная не может иметь множества значений, условия типа* `match` *и* `in` *неприменимы.*<br><br>**Примеры:**<br>`divert input`<br>`divert not output` | Да | Нет |
| `content_type` | MIME-тип данных, передающихся по соединению.<br><br>**Особенности использования:**<br>• Может быть определен, только если не используется SSL/TLS или было разрешено вскрытие SSL.<br>• Выражению "`*/*`" соответствуют данные любого MIME-типа, а также HTTP-ответы без заголовка `Content-Type`.<br>• Для проверки значения переменной можно использовать Dr.Web LookupD. | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | • Множество значений для проверки значения переменной можно получать из файла.<br>**Примеры:**<br>`content_type in ("multipart/byteranges", "application/octet-stream")`<br>`content_type not in ("text/*", "image/*")`<br>`content_type not in ("audio/*")`<br>`content_type in ("*/*")`<br>`content_type in LDAP@BlockedContent`<br>`content_type not in file("/etc/file")` | | |
| `unwrap_ssl` | Используется ли раскрытие защищенного трафика, передаваемого через SSL/TLS.<br>**Возможные значения:** `true`, `false`.<br>**Особенности использования:**<br>• Переменная не может не иметь значения, т. е. инструкция `SET unwrap_ssl = ()` недопустима.<br>• Переменная не может использоваться в условиях, а нужна только для управления вскрытием SSL (например, чтобы продемонстрировать пользователю веб-страницу с уведомлением о блокировке от нашего имени).<br>**Примеры:**<br>`SET unwrap_ssl = TRUE`<br>`set Unwrap_SSL = false` | Нет | Да |

### Переменные, используемые в правилах обработки почты

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| `header` | Содержимое области заголовков письма.<br><br>**Особенности использования:**<br>• Используется для сравнения области заголовков со списком задаваемых шаблонов (используются регулярные выражения).<br>• Может быть проверен любой из заголовков, представленных в письме.<br>• Сравнение нечувствительно к регистру, допустимо использовать Unicode.<br>• Множество значений для проверки значения переменной можно получать из файла.<br><br>**Примеры:**<br>`header match ("su..ect: sp.m", "From: sales.*@.*")`<br>`Header not match ("Subject: .*купи.*")`<br>`header match file("/etc/file")` | Да | Нет |
| `body` | Текстовое содержимое тела письма.<br><br>**Особенности использования:**<br>• Используется для сравнения тела письма со списком задаваемых шаблонов (используются регулярные выражения).<br>• Может быть проверена любая текстовая часть тела письма.<br>• Сравнение нечувствительно к регистру, допустимо использовать Unicode.<br>• Множество значений для проверки значения переменной можно получать из файла. | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | **Примеры:**<br>`body match ("в.чност[ьи]")`<br>`body not match file("/etc/file")` | | |
| `body_part_header` | Заголовки частей тела письма (MIME part).<br>**Особенности использования:**<br>• Используется для сравнения заголовков, имеющихся в разделах тела письма, со списком задаваемых шаблонов (используются регулярные выражения).<br>• Могут быть проверены заголовки любой части тела письма.<br>• Сравнение нечувствительно к регистру, допустимо использовать Unicode.<br>• Множество значений для проверки значения переменной можно получать из файла.<br>**Примеры:**<br>`body_part_header match ('Content-Disposition: attachment; .*filename="вирус.exe"')`<br>`BodyPartHeader not match ("Content-Disposition: attachment; .*")`<br>`body_part_header match file("/etc/file")` | Да | Нет |
| `attachment_name` | Имена файлов, прикрепленных к письму.<br>**Особенности использования:**<br>• Используется для сравнения имен файлов (*Content-Disposition: attachment*), прикрепленных к письму, со списком задаваемых шаблонов (используются регулярные выражения). | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | • Сравнение нечувствительно к регистру, допустимо использовать Unicode.<br>• Множество значений для проверки значения переменной можно получать из файла.<br>**Примеры:**<br>`attachment_name match ("\.ex.$", "\.js$", "^virus.*")`<br>`attachment_name not match ("\.txt$", "\.rtf$")`<br>`attachment_name not match file("/etc/file")` | | |
| `total_spam_score` | Нормализованная оценка письма, как спама (от 0 до 1), полученная от Dr.Web ASE.<br>*Нормализация балльной оценки спама, полученной от Dr.Web ASE, производится по следующим правилам:*<br>1. *Число баллов 0 и меньше — 0.0;*<br>2. *Число баллов 100 — 0.8;*<br>3. *Число баллов 1000 и больше — 1.0.*<br>*В указанных интервалах нормализованная оценка возрастает.*<br>**Особенности использования:**<br>• Переменная числовая, всегда имеет одно значение может использоваться только с условиями типа `lt` и `gt`.<br>• Если Dr.Web ASE не установлен, то проверка писем на спам не производится, и переменную `total_spam_score` нельзя использовать в правилах (попытка проверить истинность условия в правиле будет приводить к ошибке «*Dr.Web ASE не доступен*»). | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | **Пример:**<br>`total_spam_score gt 0.32`<br>`total_spam_score gt 0.5,`<br>`total_spam_score lt 0.95` | | |
| `smtp_mail_from` | Адрес отправителя письма, переданный в рамках SMTP-сессии командой `MAIL FROM`.<br>**Особенности использования:**<br>• Используется для сравнения имени отправителя, указанного в рамках SMTP-сессии, со списком задаваемых шаблонов (используются регулярные выражения).<br>• Сравнение нечувствительно к регистру.<br>• Эта переменная не может быть использована в правилах интерфейса *Spamd*: данный протокол не предоставляет информацию об отправителе письма.<br>• Множество значений для проверки значения переменной можно получать из файла.<br>**Примеры:**<br>`smtp_mail_from match ("^john@.*", ".*@domain.com$")`<br>`smtp_mail_from not match ("^user@domain.com$")`<br>`smtp_mail_from match file("/etc/file")` | Да | Нет |
| `smtp_rcpt_to` | Перечень адресов получателей письма, переданный в рамках SMTP-сессии командой `RCPT TO`.<br>**Особенности использования:**<br>• Используется для сравнения имен получателей, указанных в рамках SMTP-сессии, со списком задаваемых шаблонов (используются регулярные выражения). | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | • Сравнение нечувствительно к регистру.<br>• Эта переменная не может быть использована в правилах интерфейса *Spamd*: данный протокол не предоставляет информацию о получателе письма.<br>• Если перед `match` указано `all`, то условие с данной переменной будет истинно только в случае совпадения *всех значений из перечня* с указанными шаблонами.<br>• Множество значений для проверки значения переменной можно получать из файла.<br>**Примеры:**<br>`smtp_rcpt_to match ("^user1@domain.com$", ".*@domain2.com$")`<br>`smtp_rcpt_to all match ("^john@.*", ".*@domain.com$")`<br>`smtp_rcpt_to match file("/etc/file")` | | |
| `maild_templates_dir` | Путь к каталогу, из которого брать шаблон, используемый для перепаковки почтовых сообщений.<br>Если путь начинается с / — это абсолютный путь, если с любого другого символа — то это относительный путь. Корнем при этом считается путь из параметра **`TemplatesDir`**.<br>**Особенности использования:**<br>• Имеет смысл только для почтовых протоколов (*POP3*, *IMAP*, *SMTP*) и для интерфейсов MTA (*Milter*, *Spamd*, *Rspamd*).<br>**Примеры:**<br>`SET maild_templates_dir = "/etc/my_mail_templates"` | Нет | Да |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | `set MaildTemplatesDir = "templates_for_my_MTA"` | | |

## Категории нежелательных веб-сайтов и угроз

1. Категории нежелательных веб-сайтов (для переменных `sni_category`, `url_category`)

| Обозначение | Категория веб-сайтов |
|---|---|
| *InfectionSource* | Сайты, содержащие вредоносное ПО («источники распространения вирусов»). |
| *NotRecommended* | Сайты, используемые для мошенничества («социальной инженерии») и не рекомендованные к посещению. |
| *AdultContent* | Сайты, содержащие материалы для взрослых. |
| *Violence* | Сайты, содержащие сцены насилия. |
| *Weapons* | Сайты, посвященные оружию. |
| *Gambling* | Сайты, содержащие азартные игры и игры на деньги. |
| *Drugs* | Сайты, посвященные наркотикам. |
| *ObsceneLanguage* | Сайты, содержащие нецензурную лексику. |
| *Chats* | Сайты чатов. |
| *Terrorism* | Сайты, посвященные терроризму. |
| *FreeEmail* | Сайты бесплатных почтовых служб. |
| *SocialNetworks* | Сайты социальных сетей. |
| *DueToCopyrightNotice* | Сайты, ссылки на которые указаны правообладателями некоторого произведения, защищенного авторскими правами (кинофильмы, музыкальные произведения и т. д.). |

*В качестве значения переменных* `sni_category` *и* `url_category` *можно также использовать имена параметров, управляющих блокировкой (см. ниже).*

2. Категории угроз (для переменной `threat_category`)

| Обозначение | Категория угроз |
|---|---|
| *KnownVirus* | Известная угроза (вирус). |
| *VirusModification* | Модификация известной угрозы (вируса). |
| *UnknownVirus* | Неизвестная угроза, подозрительный объект. |
| *Adware* | Рекламная программа. |
| *Dialer* | Программа дозвона. |
| *Joke* | Программа-шутка. |
| *Riskware* | Потенциально опасная программа. |
| *Hacktool* | Программа взлома. |

*В качестве значения переменной* `threat_category` *можно также использовать имена параметров, управляющих блокировкой (см. ниже).*

# Приложение В. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

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

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

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