Dr.WEB

Enterprise Security Suite

# Управление Dr.Web для Интернет-шлюзов UNIX

**Dr.Web Enterprise Security Suite. Управление Dr.Web для Интернет-шлюзов UNIX**
**Версия 11.0.2**
**Руководство администратора**
**27.05.2021**

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** 5
**1.1. Назначение документа** 5
**1.2. Условные обозначения и сокращения** 6
**Глава 2. Dr.Web Enterprise Security Suite** 8
**2.1. О продукте** 8
**2.2. Защита станций сети** 9
**Глава 3. Dr.Web для Интернет-шлюзов UNIX** 11
**3.1. Компоненты Dr.Web для Интернет-шлюзов UNIX** 12
**3.2. Настройка Dr.Web для Интернет-шлюзов UNIX** 14
3.2.1. Настройки Dr.Web ICAPD 15
3.2.2. Настройки SpIDer Gate 20
3.2.3. Настройки Агента Dr.Web для UNIX 22
3.2.4. Настройки File Checker 24
3.2.5. Настройки Scanning Engine 25
3.2.6. Настройки Dr.Web ConfigD 26
**Приложение A. Правила проверки трафика** 28
**Приложение B. Техническая поддержка** 42

# 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 Интернет-шлюзов UNIX и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- **Руководство администратора** антивирусного решения Dr.Web для Интернет-шлюзов 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),
- ICAP — протокол адаптации Интернет-контента (Internet Content Adaptation Protocol),
- IP — протокол Интернета (Internet Protocol),
- LDAP — легковесный протокол доступа к службам каталогов (Lightweight Directory Access Protocol),

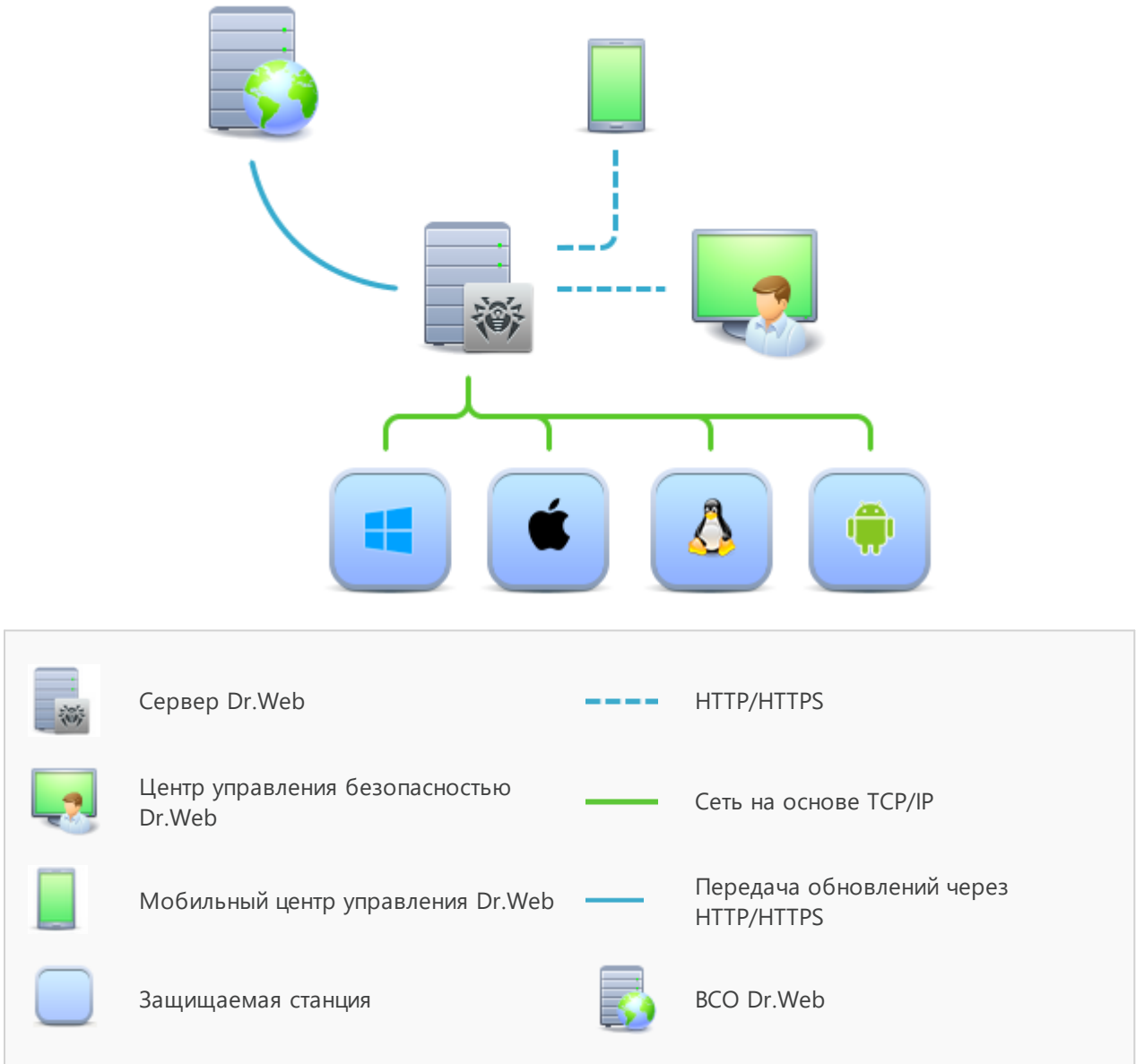
- MIME — многоцелевые расширения Интернет и почты (Multipurpose Internet Mail Extensions),
- SSL — уровни защищенных сокетов (Secure Socket Layers),
- TCP — протокол управления передачи (Transmission Control Protocol),
- TLS — защищенный транспортный уровень (Transport Layer Security),
- URL — единообразный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

# 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 Интернет-шлюзов UNIX

В настоящем документе рассматриваются аспекты настройки компонентов, входящих в продукт Dr.Web для Интернет-шлюзов 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 Интернет-шлюзов UNIX создан для защиты Интернет-шлюзов, 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 Интернет-шлюзов 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. **Анализ данных, передаваемых в сеть Интернет.** Отслеживаются и проверяются как запросы пользователей (т. е. попытки подключиться к веб-серверу и загрузить на него некоторый файл), так и непосредственно данные, направляемые веб-серверами

в ответ на запросы пользователей. Для анализа запросов и возвращаемых данных, продукт подключается по протоколу ICAP как внешний фильтр к прокси-серверу, обрабатывающему HTTP-соединения пользователей локальной сети. Кроме того, при помощи компонента SpIDer Gate можно реализовать функции барьера, предотвращающего прием и передачу инфицированных файлов публичным веб-сервером организации (*данная возможность доступна только в ОС GNU/Linux*). Для ограничения доступа к нежелательным веб-сайтам используются как автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, поставляемая вместе с Dr.Web для Интернет-шлюзов UNIX, так и черные и белые списки, ведущиеся системным администратором вручную. Также производится обращение к сервису Dr.Web Cloud для проверки наличия информации, не отмечен ли веб-ресурс, к которому пытается обратиться пользователь, как вредоносный, другими антивирусными продуктами Dr.Web.

## 3.1. Компоненты Dr.Web для Интернет-шлюзов UNIX

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

### Основные

*Dr.Web ICAPD*

ICAP-сервер, выполняющий анализ запросов и трафика, проходящего через прокси-серверы HTTP (такие, как **Squid**). Предотвращает передачу инфицированных файлов и доступ к узлам сети, внесенными в как в нежелательные категории веб-ресурсов, так и в черные списки, формируемые системным администратором. При запрете доступа к внешним серверам и при обнаружении угроз в передаваемых данных предписывает прокси-серверу вернуть клиенту специальную страницу ответа, содержащую сообщение о невозможности доступа к запрошенному ресурсу или загрузки инфицированного файла.

Центральный компонент Dr.Web для Интернет-шлюзов UNIX. Позволяет интегрировать его с приложениями, использующими протокол ICAP (как правило, это защищаемый прокси-сервер HTTP, использующийся для доступа рабочих станций, включенных в состав ЛВС, к сети Интернет).

*SpIDer Gate*

Компонент, предназначенный для защиты веб-сервера компании от получения и передачи данных, содержащих угрозы и/или нежелательные ссылки:

- Проверяет наличие URL в базах категорий веб-ресурсов и черных списках; блокирует доступ к веб-сайтам, если ведущие к ним URL зарегистрированы в черном списке или категориях, отмеченных как нежелательные для посещения.
- Выполняет проверку файлов, загружаемых из сети Интернет на сервер, и блокирует их загрузку, если они содержат угрозы.

Если доступ к некоторому ресурсу или его загрузка запрещены, возвращает клиенту HTML-страницу с указанием на ошибку доступа.

*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 Интернет-шлюзов 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 Интернет-шлюзов 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 Интернет-шлюзов UNIX с внешними системами мониторинга посредством протокола SNMP.

*Dr.Web ConfigD*

Координирует работу всех компонентов Dr.Web для Интернет-шлюзов 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 Интернет-шлюзов UNIX. Предоставляет веб-интерфейс управления.

## 3.2. Настройка Dr.Web для Интернет-шлюзов 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 ICAPD

Раздел **Dr.Web ICAPD** содержит следующие настройки функционирования Dr.Web для Интернет-шлюзов UNIX:

- Общие — настройка основных параметров работы компонента.
- Дополнительно — настройка дополнительных параметров работы компонента.
- Веб-фильтр — настройка проверки URL и блокировки доступа к веб-сайтам.
- Исключения — настройка исключений в блокировке доступа к веб-сайтам.
- Файловый фильтр — настройка проверки файлов и данных, загружаемых из Интернета.
- Правила проверки трафика — настройка правил проверки.

### 3.2.1.1. Общие

В данном разделе вы можете управлять следующими параметрами работы Dr.Web ICAPD на защищаемой станции (Интернет-шлюзе):

- **Запускать компонент при старте** — управляет запуском компонента на защищаемом Интернет-шлюзе.
- **Сокет для клиентских подключений** — сетевой сокет (<*IP-адрес*>:<*порт*>), через который ICAP-клиенты (такие, как **Squid**) будут подключаться к Dr.Web ICAPD.
- **Пользователь** — позволяет указать имя пользователя UNIX, с правами и полномочиями которого работает компонент на защищаемом Интернет-шлюзе.

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

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

### 3.2.1.2. Дополнительно

В данном разделе вы можете управлять следующими дополнительными параметрами работы Dr.Web ICAPD на защищаемой станции (Интернет-шлюзе):

- **Использовать режим ICAP preview** — флажок управляет использованием Dr.Web ICAPD режима ICAP preview.
- **Использовать режим ICAP 204** — флажок определяет, может ли Dr.Web ICAPD возвращать код ответа 204 не только в режиме ICAP preview.
- **Использовать “ранние” ответы ICAP** — флажок определяет, может ли Dr.Web ICAPD использовать режим «раннего» ответа ICAP, т. е. начинать отправлять ответ клиенту, не прочитав до конца запрос от прокси-сервера HTTP.

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

### 3.2.1.3. Веб-фильтр

В данном разделе вы можете управлять параметрами проверки доступа к сайтам Dr.Web ICAPD на защищаемом Интернет-шлюзе:

- Установите флажок **Блокировать сайты, содержащие вредоносное ПО**, чтобы включить блокировку сайтов, которые используются для распространения вирусов и других вредоносных программ.
- 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.
- Для блокирования сайтов, относящихся к той или иной категории веб-ресурсов установите соответствующие флажки с именами категорий, доступ к которым необходимо заблокировать (**Блокировать сайты для взрослых**, **Блокировать сайты, посвященные насилию** и так далее).
- В разделе **Список рекламных сайтов** укажите список регулярных выражений, которые определяют принадлежность URL к рекламным сайтам. Попытки перехода пользователей по URL, соответствующему любому из указанных здесь регулярных выражений будут блокироваться.

Реальное использование списка выражений, указанного в данном параметре, зависит от того, *как* он используется в правилах управления доступом к веб-ресурсам, заданных для Dr.Web ICAPD.

В перечне правил, заданных по умолчанию, гарантируется, что переход по URL, соответствующему любому из указанных здесь регулярных выражений будет заблокирован.

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

### 3.2.1.4. Исключения

В данном разделе вы можете управлять исключениями в проверке сайтов компонентом Dr.Web ICAPD на защищаемом Интернет-шлюзе:

- В разделе **Белый список доменов, подключение к которым разрешено администратором** укажите список доменов, подключение к которым должно быть разрешено пользователям, даже если эти домены относятся к блокируемым категориям веб-ресурсов. При этом доступ пользователей будет разрешаться и ко всем поддоменам доменов, указанных в этом списке).

  Реальное использование списка доменов, указанного в данном параметре, зависит от того, *как* он используется в правилах управления доступом к веб-ресурсам, заданных для Dr.Web ICAPD.

  В перечне правил, заданных по умолчанию, гарантируется, что доступ к доменам (и их поддоменам) из данного списка будет обеспечен, даже если там будут находиться домены из блокируемых категорий веб-ресурсов. Кроме этого набор правил по умолчанию гарантирует, что данные, загружаемые с доменов из белого списка, *будут проверяться на наличие угроз*.

- В разделе **Черный список доменов, подключение к которым запрещено администратором** укажите список доменов, подключение к которым должно быть запрещено пользователям, даже если эти домены не относятся к блокируемым категориям веб-ресурсов. При этом доступ пользователей будет запрещаться и ко всем поддоменам доменов, указанных в этом списке).

  Реальное использование списка доменов, указанного в данном параметре, зависит от того, *как* он используется в правилах управления доступом к веб-ресурсам, заданных для Dr.Web ICAPD.

  В перечне правил, заданных по умолчанию, гарантируется, что доступ к доменам (и их поддоменам) из данного списка будет запрещен всегда. Если домен добавлен одновременно в белый и черный список доменов, то правила, заданные по умолчанию, гарантируют, что доступ пользователей к нему будет *заблокирован*.

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

### 3.2.1.5. Файловый фильтр

В данном разделе вы можете управлять параметрами проверки Dr.Web ICAPD на защищаемом Интернет-шлюзе файлов и данных, загружаемых из сети Интернет:

- В разделе **Блокировать файлы** выберите типы небезопасных получаемых объектов, которые будут блокироваться компонентом Dr.Web ICAPD.

- **Инфицированные** — в проверенном файле обнаружен известный вирус.
- **Подозрительные** — проверенный файл отмечен как *подозрительный*.
- **Рекламные программы** — в проверенном файле обнаружена рекламная программа.
- **Программы дозвона** — в проверенном файле обнаружена программа дозвона.
- **Программы-шутки** — в проверенном файле обнаружена программа-шутка.
- **Потенциально опасные** — в проверенном файле обнаружена потенциально опасная программа.
- **Программы взлома** — в проверенном файле обнаружена программа взлома.
- **Непроверенные файлы** — файл не удалось проверить.

- **Использовать эвристический анализ** — управляет использованием Dr.Web ICAPD на защищаемом Интернет-шлюзе 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 Dr.Web ICAPD на защищаемом Интернет-шлюзе. Если указано *0*, время проверки одного файла не ограничивается.
- В разделе **Максимальный уровень вложенности** вы можете управлять параметрами проверки Dr.Web ICAPD 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 ICAPD. Например, чтобы проверять содержимое архивов, вложенных в архивы, необходимо указать уровень вложенности для них не менее *2*. Чтобы запретить проверку вложенных объектов, укажите уровень вложенности *0* для соответствующего типа контейнеров.

  Помните, что увеличение допустимого уровня вложенности уменьшает скорость проверки.

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

### 3.2.1.6. Правила проверки трафика

В данном разделе вы можете управлять правилами проверки сайтов и данных компонентом Dr.Web ICAPD на защищаемом Интернет-шлюзе.

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.

## 3.2.2. Настройки SpIDer Gate

В разделе **SpIDer Gate** представлены следующие разделы настройки функционирования Dr.Web для Интернет-шлюзов UNIX:

- Общие — общие настройки SpIDer Gate.
- Действия — настройки действий при обнаружении угроз SpIDer Gate.
- Веб-фильтр — настройки проверки веб-трафика и контроль доступа к интернет-ресурсам компонентом SpIDer Gate.
- Контейнеры — настройки проверки составных объектов (архивов, почтовых файлов и т. п.).
- Дополнительно — дополнительные настройки SpIDer 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.
  - Чтобы настроить доступ к веб-сайтам со схожими именами, введите общую часть их доменных имен. Пример: если вы введете текст `example`, то доступ к адресам `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru` и другим подобным веб-сайтам будет определяться данной записью.
  - Чтобы настроить доступ к веб-сайтам определенного домена, укажите имя домена с символом «`.`». В таком случае доступ ко всем ресурсам, находящиеся на этом домене, будет определяться данной записью. Если при указании домена используется символ прямого слэша «`/`», то та часть подстроки, что стоит слева от символа «`/`», будет считаться доменным именем, а части справа от символа — частью разрешенного на данном домене адреса. Пример: если вы введете текст `example.com/test`, SpIDer Gate будет определять доступ к веб-страницам таким как `example.com/test11`, `template.example.com/test22` и т. п.

### 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 Интернет-шлюзов UNIX:

- Общие — настройки Агента Dr.Web для UNIX.
- Конфигурация — редактор настроек всех компонентов Dr.Web для Интернет-шлюзов 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 Интернет-шлюзов 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 файла конфигурации `.ini`) настройки для любого из компонентов Dr.Web для Интернет-шлюзов 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 Интернет-шлюзов UNIX.
- **Путь к административному коммуникационному сокету** — определяет путь к UNIX-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web для Интернет-шлюзов UNIX, работающими с полномочиями суперпользователя.
- **Путь к каталогу временных файлов** — определяет каталог, в котором компоненты Dr.Web для Интернет-шлюзов UNIX хранят свои временные файлы.
- **Путь к каталогу PID-файлов и файлов коммуникационных сокетов** — определяет каталог, в котором компоненты Dr.Web для Интернет-шлюзов 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>  <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 Интернет-шлюзов UNIX. Если указанный файл отсутствует или его размер слишком велик, при запуске Dr.Web для Интернет-шлюзов UNIX 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 перезапустить Dr.Web для Интернет-шлюзов 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 |

| Запись | Смысл |
|---|---|
| | (LDAP или AD); <*тег*> — это имя секции, 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. |

## Действия

Действия делятся на *конечные* резолюции, определяющие запрет или разрешение на 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. |
| `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 |

| Резолюция | Описание (смысл) |
|---|---|
| | сработало правило (для условий `*_category in (...)`). Переменная `_match` хранит список блокируемых категорий, для которых сработало соответствие. |

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`).

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| `protocol` | Тип сетевого протокола, используемого соединением. | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | *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>• В правилах для Dr.Web ICAPD не имеет смысл указывать значение, отличное от `HTTP`: для него протокол может быть только HTTP.<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")` | | |
| `url` | URL, запрошенный клиентом. Может быть сравнен с указанной строкой или регулярным выражением.<br><br>**Особенности использования:**<br>• Для проверки значения переменной можно использовать Dr.Web LookupD.<br>• Множество значений для проверки значения переменной можно получать из файла.<br><br>**Примеры:**<br>`url match ("drweb.com", "example\..*", "aaa\.ru/")`<br>`url match "ICAPD.Adlist"`<br>`url not match LDAP@BadURLs`<br>`url match file("/etc/file")` | Да | Нет |
| `url_host` | URL/хост, с которым устанавливается соединение. | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | **Особенности использования:**<br>• Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL.<br>• Для проверки значения переменной можно использовать Dr.Web LookupD.<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")` | | |
| `url_category` | Список категорий, к которым (по базам категорий веб-ресурсов или по ответу из Dr.Web Cloud) 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 Dr.Web ICAPD 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 истинность условия в правиле будет приводить к ошибке). | 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>`url_category not in (AdultContent, Chats)`<br>`url_category in "ICAPD.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 Dr.Web ICAPD 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 "ICAPD.BlockThreat"`<br>`threat_category not in (Joke)`<br>`threat_category in file("/etc/file")` | Да | Нет |
| `user` | Имя пользователя, с правами которого запущен процесс-отправитель (или получатель) трафика. | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | **Особенности использования:**<br>• В правилах для Dr.Web ICAPD имеет смысл имени пользователя, прошедшего аутентификацию на прокси-сервере (если прокси-сервер поддерживает аутентификацию). Если прокси-сервер не аутентифицирует пользователей, переменная имеет пустое значение.<br>• Для проверки значения переменной можно использовать Dr.Web LookupD.<br>• Если требуется проверить вхождение пользователя в некоторую группу пользователей, используйте источник данных LDAP или Active Directory, возвращающий перечень групп. Также запрос должен содержать условие сравнения имени группы, которой принадлежит пользователь, с требуемым (используйте формат <*тип источника LookupD*>@<*источник групп*>@<*требуемая группа*>). Запросы к Active Directory (AD@) возвращают только перечни групп, поэтому для них использование части @<*требуемая группа*> обязательно.<br>• Множество значений для проверки значения переменной можно получать из файла.<br>**Примеры:**<br>`user in ('user1', 'user2')`<br>`user in AD@Winusergroups@Admins`<br>`user in LDAP@AllowedUsers`<br>`user not in file("/etc/file")` | | |
| `src_ip` | IP-адрес хоста, со стороны которого следует соединение.<br>**Особенности использования:**<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>`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")` | | |
| `direction` | Тип трафика, идущего по соединению.<br>**Возможные значения:** `request` (клиентский запрос), `response` (ответ сервера).<br>*Переменная не может иметь множества значений, условия типа* `match` *и* `in` *неприменимы.*<br>**Примеры:**<br>`direction request`<br>`direction not response` | Да | Нет |
| `divert` | Направление соединения.<br>**Возможные значения:** `input` (входящее — создано/инициировано извне локального хоста), `output` (исходящее — создано/инициировано на локальном хосте).<br>*Переменная не может иметь множества значений, условия типа* `match` *и* `in` *неприменимы.*<br>**Примеры:**<br>`divert input`<br>`divert not output` | Да | Нет |
| `content_type` | MIME-тип данных, передающихся по соединению. | Да | Нет |

| Переменная | Описание | Может быть использована в | |
|---|---|---|---|
| | | условной части | части действия (SET) |
| | **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.<br>• 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")` | | |
| `http_templates_dir` | Путь к каталогу, из которого брать шаблон страницы уведомления о блокировке HTTP-запроса/ответа.<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 протокола HTTP(S).<br>**Примеры:**<br>`SET http_templates_dir = "/etc/mytemplates"` | Нет | Да |

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

## 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).*

## Параметры конфигурации, которые можно использовать в условиях правил

Параметры, используемые в правилах компонента Dr.Web ICAPD (указываются с префиксом `ICAPD.`):

| Параметр | Описание и пример использования |
|---|---|
| `Whitelist` | Белый список. Хранит перечень доменов, доступ к которым разрешается, даже если эти домены находятся в базе категорий.<br>**Примеры:**<br>`url_host not in "ICAPD.Whitelist" : BLOCK as BlackList` |
| `Blacklist` | Черный список. Хранит перечень доменов, доступ к которым запрещен самим пользователем (или администратором).<br>**Примеры:**<br>`url_host in "ICAPD.Blacklist" : BLOCK as BlackList` |
| `Adlist` | Рекламный список. Хранит перечень регулярных выражений, которые описывают рекламные сайты. Задается самим пользователем (или администратором).<br>**Примеры:**<br>`url match "ICAPD.Adlist" : BLOCK as BlackList` |

| Параметр | Описание и пример использования |
|---|---|
| `BlockCategory` | «Мета-параметр»: Его значениями является список названий категорий (*Chats, AdultContent* и т. д.), для которых соответствующие параметры **`Block*`** в секции `[ICAPD]` установлены в `Yes`.<br><br>**Примеры:**<br><br>`url_category in "ICAPD.BlockCategory" : BLOCK as _match` |
| `BlockThreat` | «Мета-параметр»: его значениями является список названий типов угроз (*KnownVirus, Joke* и т. д.), для которых соответствующие параметры **`Block*`** в секции `[ICAPD]` установлены в `Yes`.<br><br>**Примеры:**<br><br>`threat_category in "ICAPD.BlockThreat" : BLOCK as _match` |

# 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/.