Dr.WEB®
Office Shield

Защити созданное

Руководство администратора

Dr.Web® Office Shield
Версия 7.0.0
Руководство администратора
08.08.2012

«Доктор Веб», Центральный офис в России
125124
Россия, Москва
3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: www.drweb.com
Телефон: +7 (495) 789-45-87

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

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

«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

Введение

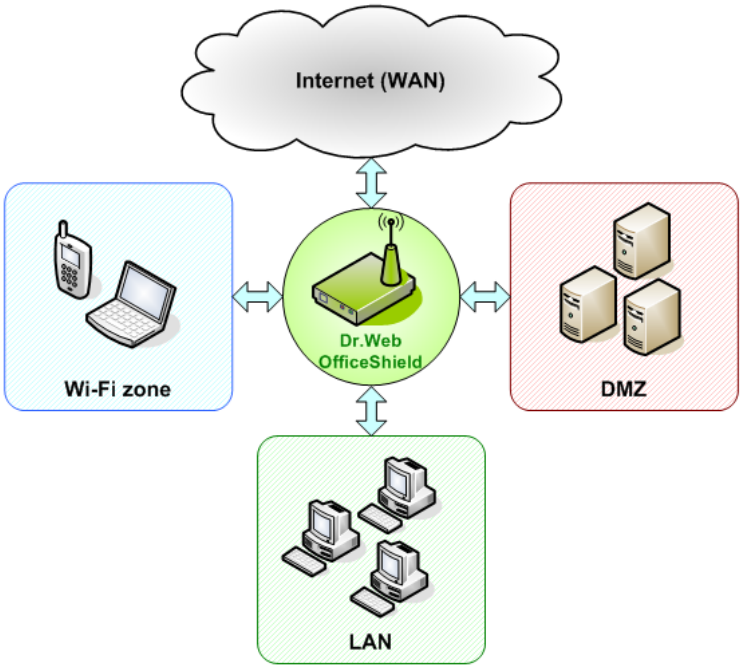
О продукте Dr.Web Office Shield

Dr.Web Office Shield является высокопроизводительным и отказоустойчивым сервером централизованной антивирусной и антиспам-защиты рабочих станций и файловых серверов, почтового и интернет-трафика. Модульность решения и гибкость системы лицензирования позволяют использовать устройство в самых различных конфигурациях локальных сетей предприятий и организаций, реализуя их внутреннюю политику безопасности.

Dr.Web Office Shield позволяет разделить локальную сеть предприятия на два сегмента:

- Защищенная локальная сеть (LAN) — часть компьютерной сети, в которой работают пользователи. Для LAN обеспечивается защита почтового и интернет-трафика от вирусов, разного рода вредоносных объектов и спама, а также реализуются политики предотвращения доступа пользователей к нежелательным Интернет-ресурсам.
- Демилитаризованная зона (DMZ) — особо выделенная часть компьютерной сети, для узлов которой запрещена инициация сетевых соединений с узлами, находящимися в других сетях. Узлы данной сети могут только отвечать на входящие соединения.
- Встроенная в комплекс **Dr.Web Office Shield** точка доступа Wi-Fi позволяет организовать подключение устройств к сети LAN посредством беспроводного соединения Wi-Fi по спецификациям IEEE 802.11b/g.

Схематическое разбиение локальной сети предприятия на сегменты посредством **Dr.Web Office Shield** представлено на рисунке ниже:



Для каждой зоны сети посредством встроенного межсетевого экрана и набора настраиваемых правил маршрутизации обеспечивается выход в Интернет (зона сети WAN), а также связь с компьютерами других зон сети.

Обратите внимание, что "зона Wi-Fi", изображенная на рисунке, не является самостоятельной сетевой зоной. Клиенты и устройства, подключающиеся через точку доступа Wi-Fi, находятся в сетевой зоне LAN.

Dr.Web Office Shield может быть использован:

- В качестве прокси-сервера, предназначенного для обеспечения защиты почтового и интернет-трафика от вирусов, разного рода вредоносных объектов и спама. Использование **Dr.Web Office Shield** в качестве шлюза значительно снижает затраты компаний на организацию безопасного доступа пользователей корпоративной

интранет-сети к ресурсам сети Интернет и позволяет существенно экономить интернет-трафик;

- В качестве внутреннего сервера централизованной антивирусной защиты локальной сети, обеспечивающего централизованную защиту рабочих станций и файловых серверов, входящих в локальную сеть организации. Для обеспечения централизованной антивирусной защиты на базе локальной стети организуется **Антивирусная сеть**, включающая в себя все защищаемые рабочие станции, а также центральный сервер защиты, называемый **Enterprise-сервером**.

Перечень функций защиты, предоставляемых **Dr.Web Office Shield**, зависит от типа приобретенной лицензии и может варьироваться при необходимости посредством приобретения лицензий, разрешающих или запрещающих те или иные возможности, в зависимости от потребностей организации. В случае отсутствия или истечения срока действия лицензии устройство может работать в качестве сетевого шлюза, отделяющего локальные сети организации от сети Интернет.

Структура документации

Документация состоит из следующих разделов:

- **Краткое руководство** — обзор об основных задачах, решаемых с помощью **Dr.Web Office Shield**.
- **Установка** — подключение устройства **Dr.Web Office Shield** к корпоративной сети.
- **Общие настройки** — первичные настройки для начала работы с **Dr.Web Office Shield**: приобретение и активация лицензии, настройка web-интерфейса (например, языка), смена пароля, включение компонентов обеспечения безопасности.
- **Управление сетями** — подключение к сетям DMZ, LAN, WAN, Wi-Fi и настройка DHCP, DNS, VPN.
- **Управление безопасностью** — проверка корпоративной почты и web-трафика с помощью модулей **Dr.Web**, настройка корпоративного межсетевого экрана и защиты рабочих станций.
- **Настройка системы** — управление системой (перезагрузка и завершение работы системы, сохранение и восстановление системы, обновление, настройка

системного времени).

- **Компоненты** — настройка компонентов **Webmin**.
- **Рекомендации по обеспечению безопасности**.
- **Информация о технической поддержке**.

Назначение документа

В настоящем Руководстве содержится информация об общих принципах и деталях реализации комплексной защиты корпоративных локальных сетей с использованием **Dr.Web® Office Shield.**

Данное Руководство адресовано администратору локальной сети, которому поручено руководство антивирусной защитой рабочих станций, почтовых и файловых серверов, а также осуществление контроля за использованием веб-трафика. Администратор локальной сети должен быть компетентным в вопросах стратегии антивирусной защиты и детально знать антивирусные пакеты **Dr.Web®** для всех используемых в сети ОС.

Начальные главы Руководства могут быть полезны руководителю организации, принимающему решение о приобретении и установке системы централизованной антивирусной и антиспам-защиты.

Перед прочтением документа убедитесь, что это последняя версия Руководства Администратора. Руководство постоянно обновляется, и последнюю его версию всегда можно найти на официальном веб-сайте компании **«Доктор Веб».**

Состав Dr.Web Office Shield

В состав **Dr.Web Office Shield** входят следующие компоненты:

- **Dr.Web Enterprise Server**. Обеспечивает организацию **Антивирусной сети Dr.Web**, используемой для централизованной защиты рабочих станций, файловых серверов и компьютеров корпоративной локальной сети.
- **Центр управления Dr.Web**. Обеспечивает управление как **Dr.Web Enterprise Server**, так и всей настроенной **Антивирусной сетью** в целом.
- **Dr.Web Веб-прокси**. Защищает доступ пользователей внутренней интранет-сети к ресурсам сети Интернет.
- **Dr.Web Почтовый прокси**. Обеспечивает антивирусную и антиспам-защиту почтового трафика.
- **Корпоративный межсетевой экран**. Блокирует несанкционированный доступ и разрешает санкционированные соединения.
- **VPN-сервер**. Обеспечивает безопасную регистрацию удаленных пользователей в сети.
- **DHCP-сервер**. Упрощает администрирование сетевых адресов.
- **DNS-сервер**. Устанавливает соответствие между внешними доменными адресами и числовыми IP-адресами и улучшает процесс определения имен в корпоративной сети.
- **Точка доступа Wi-Fi** обеспечивает беспроводное подключение к корпоративной сети.

Программный комплекс **Dr.Web Office Shield** функционирует в среде ОС **Debian GNU/Linux** (версия 5).

Для работы **Dr.Web Office Shield** помимо компонентов, разработанных компанией **«Доктор Веб»**, используется следующее программное обеспечение:

- Межсетевой экран (firewall) **Shorewall** 4;
- Прокси-сервер для HTTP **Squid** 3;
- Прокси-сервер для FTP **frox**;

- DNS-сервер **BIND** 9;
- Утилита безопасного доступа **OpenSSH** 5.1;
- Веб-интерфейс управления **Webmin** 1.510.

В первоначальном (заводском) состоянии службы VPN, DHCP и DNS выключены, а компоненты защиты **Dr.Web Enterprise Server, Веб-прокси** и **Почтовый прокси** не функционируют до загрузки в устройство соответствующих ключей.

Преимущества Dr.Web Office Shield

Преимущества продукта **Dr.Web Office Shield**:

- **Dr.Web Office Shield** может быть установлен в уже существующую сеть, либо использован в качестве основы для вновь создаваемой сети.
- Система управления **Dr.Web Office Shield** доступна для администраторов любой квалификации. За счет интуитивно понятного интерфейса процесс администрирования устройства достаточно прост и может осуществляться с помощью любого интернет-браузера. При необходимости доступ к устройству можно получить и с консоли, в том числе – удаленно, по сети.
- Высокая стабильность работы, предварительно настроенная конфигурация, функции автоматической диагностики и профилактики сводят к минимуму необходимость контроля администратора над работой **Dr.Web Office Shield**. Система оповещения администратора о проблемах, возникающих в антивирусной сети защищаемого предприятия, позволяет максимально оперативно реагировать на вирусные угрозы и активно им противодействовать.
- Наличие встроенных механизмов контроля работоспособности системы позволяет автоматически восстанавливать работоспособность устройства в случае возникновения каких-либо проблем.
- Операционная система и основные программные модули **Dr.Web Office Shield** недоступны для несанкционированной модификации как за счет реализации эффективной политики доступа, так и за счет использования предустановленного межсетевого экрана.
- Использование репозитория для проведения обновлений позволяет оперативно устранять выявленные уязвимости в используемом программном обеспечении и поддерживать высокий уровень защищенности **Dr.Web Office Shield**.
- Широкий спектр поддерживаемых операционных систем и уникальная система обновлений компонентов и вирусных баз **Dr.Web Office Shield** не требуют от предприятия единообразия платформ защищаемых рабочих станций.

Условные обозначения и сокращения

В данном руководстве применяются следующие условные обозначения:

Обозначение	Комментарий
Полужирное начертание	Названия элементов графического интерфейса и примеры ввода, который необходимо выполнить в точности так, как он приведен в руководстве.
Зеленое и полужирное начертание	Наименования продуктов **«Доктор Веб»** или их компонентов.
Зеленое и подчеркнутое начертание	Ссылки на страницы руководства и веб-сайты.
`Моноширинный шрифт`	Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением.
Курсив	Термины и замещающий текст (приводится вместо информации, которую необходимо ввести пользователю). В случае примеров ввода командной строки курсив указывает на значения параметров.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Знак плюса (+)	Указывает на одновременность нажатия клавиш клавиатуры. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
Восклицательный знак (!)	Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях.

Расшифровка сокращений, используемых в данном руководстве:

Обозначение	Расшифровка
DHCP	Dynamic Host Configuration Protocol — сетевой протокол (служба), позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP
DMZ	Демилитаризованная зона — особый сегмент сети, в котором располагаются серверы, отвечающие на запросы из внешней сети. Серверы, расположенные в DMZ, ограничены в доступе к основным сегментам сети с помощью межсетевого экрана (файрвола), с целью минимизировать ущерб при взломе одного из общедоступных сервисов, находящихся в DMZ
DNS	Domain Name System — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для установления соответствия между именем хоста (компьютера или устройства) и его IP-адресом
FTP	File Transfer Protocol — протокол передачи файлов в компьютерных сетях
HTML	HyperText Markup Language — язык разметки гипертекста, используемый в Интернет
HTTP	HyperText Transfer Protocol — протокол прикладного уровня передачи данных в виде гипертекстовых документов, в т.ч. HTML
HTTPS	HTTP Secure — расширение протокола HTTP, поддерживающее шифрование с "упаковкой" сообщений в в криптографический протокол SSL или TLS
IP-адрес	Уникальный сетевой адрес узла в компьютерной сети TCP/IP, представленный в числовой форме
LAN	Local Area Network — компьютерная сеть, объединяющая компьютеры, расположенные на небольшой территории (здание, офис, комната)
MAC-адрес	MAC-адрес (Hardware Address) — уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей.

Обозначение	Расшифровка
MIME	Multipurpose Internet Mail Extensions (многоцелевое расширение интернет-почты) — стандарт, описывающий передачу различных типов данных по электронной почте, а также спецификация для кодирования информации и форматирования сообщений таким образом, чтобы их можно было пересылать по Интернет
MTA	Mail Transfer Agent – почтовый сервер или релей
NTP	Network Time Protocol – протокол сетевого времени, с помощью которого производится синхронизация системного времени компьютеров через Интернет
SSH	Secure SHell — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. Обеспечивает безопасность шифрованием всего трафика, включая и передаваемые пароли
URI	Uniform Resource Identifier – унифицированный (единообразный) идентификатор ресурса. Символьная строка, позволяющая идентифицировать какой-либо ресурс: документ, изображение, файл, службу, ящик электронной почты и т.д.
VPN	Virtual Private Network — виртуальная частная сеть, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет)
WAN	Wide Area Network — компьютерная сеть, охватывающая большие территории и включающая в себя большое число компьютеров, в частности, сеть Интернет
Wi-Fi	Технология организации беспроводных сетей на базе стандарта IEEE 802.11
ОС	Операционная система

Установка Dr.Web Office Shield

Установка и ввод в эксплуатацию **Dr.Web Office Shield** состоят всего из нескольких простых шагов. В большинстве случаев необходимо только подключить устройство к сети, сконфигурировать его под конкретные параметры локальной сети, и оно будет выполнять все возложенные на него задачи. Это стало возможным за счет использования оптимизированного программного обеспечения, удобной системы управления и настройки и применения предустановленного сценария антивирусной безопасности.

Начало работы с Dr.Web Office Shield

Для начала работы с **Dr.Web Office Shield** необходимо выполнить следующие шаги:

1. Разместить устройство в помещении и подключить питание. При размещении устройства следует выбрать место, обеспечивающее наибольшую зону покрытия для точки доступа Wi-Fi, встроенной в устройство, если она будет использоваться.
2. С любого компьютера, подключенного к Интернет, зарегистрировать серийный номер, указанный в лицензионном сертификате, на сайте компании **«Доктор Веб»**: http://products.drweb.com/register.

   Отсчет срока действия лицензии начинается с момента регистрации серийного номера и получения ключевого файла. Полученные ключевые файлы необходимо разархивировать и сохранить на локальный диск компьютера или съемный накопитель USB.

   Если вы сохранили ключевые файлы на USB-накопитель, подключите его к любому USB-разъему устройства **Dr.Web Office Shield**.
3. Подключить устройство **Dr.Web Office Shield** к корпоративной локальной сети. Для этого следует выполнить следующие подключения:
   - К разъему **LAN1** подключается кабель локальной

сети (LAN);

- К разъему **LAN2** подключается кабель демилитаризованной зоны (DMZ), если она используется;
- К разъему **LAN3** подключается кабель провайдера услуг глобальной сети (WAN);

  Обратите внимание, что если **Dr.Web Office Shield** используется только в качестве внутреннего сервера централизованной антивирусной защиты локальной сети, обеспечивающего централизованную защиту рабочих станций и файловых серверов, то подключение его к сети WAN через **LAN3** не требуется.
- Разъем **LAN4** не используется.

Схема подключения кабелей к разъемам устройства указана на рисунке ниже.

Обратите внимание, что определение зон LAN и WAN зависит от способа включения **Dr.Web Office Shield** в сеть.

4. Включить устройство, нажав кнопку включения на лицевой панели устройства.
5. Произвести первоначальные настройки устройства через веб-интерфейс управления **Dr.Web Office Shield**, используя любой браузер, установленный на локальном компьютере.

Используйте адрес вида https://<IP adress>:10000/, где <IP address> – IP-адрес устройства.

Пароль по умолчанию для доступа к устройству — drweb.

Согласно настройкам по умолчанию, в зоне LAN **Dr.Web Office Shield** будет иметь IP-адрес 192.168.1.100.

В связи с этим обратите внимание, что после включения **Dr.Web Office Shield** будет доступен для настройки только в том случае, если в сети LAN используются сетевые адреса типа 192.168.1.xxx и в сети не занят адрес 192.168.1.100.

Если в сети используется другой диапазон адресов или IP-адрес 192.168.1.100 присвоен другому устройству, необходимо выполнить предварительную смену IP-адреса устройства в зоне LAN, подключившись к устройству через кросс-кабель.

При первом входе в систему рекомендуется сменить пароль, заданный по умолчанию.

Ознакомьтесь также с Рекомендациями по обеспечению безопасности.

Веб-интерфейс управления **Dr.Web Office Shield** поддерживается следующими версиями браузеров:

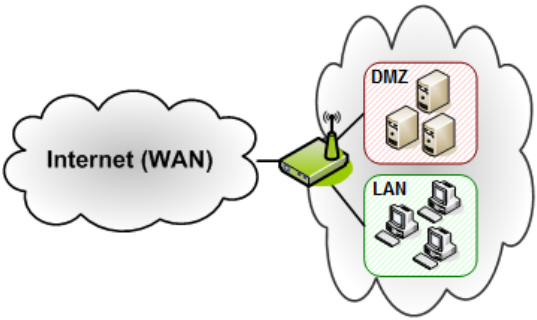
- **Mozilla Firefox** версии 3.5 и выше;
- **Internet Explorer** версии 7.0 и выше;
- **Google Chrome** версии 5 и выше.

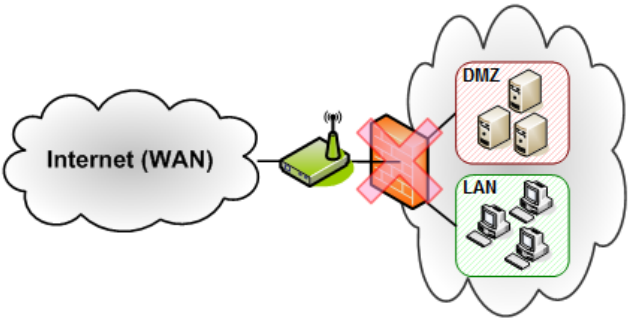
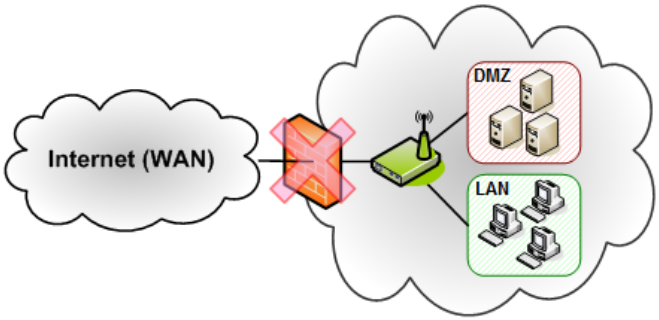
Способы включения Dr.Web Office Shield в сеть

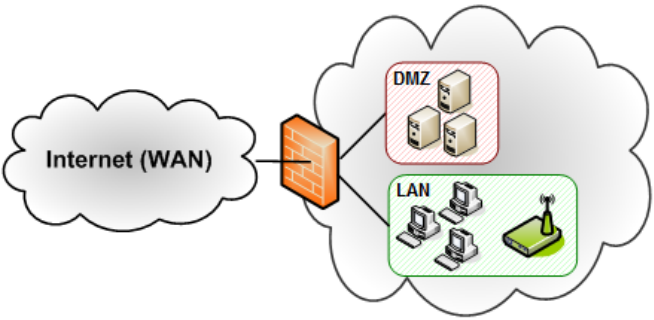
Dr.Web Office Shield может быть включен в состав сети в следующих основных режимах:

- В качестве **шлюза**, отделяющего локальную сеть и демилитаризованную зону, если она используется, от сети Интернет (рекомендованный режим).
- В качестве **внутреннего фильтра трафика** в составе локальной сети в дополнение к шлюзу, уже установленному в сети.
- В качестве **сервера централизованной антивирусной защиты LAN**, обеспечивающего централизованную защиту рабочих станций и файловых серверов.

Варианты включения **Dr.Web Office Shield** показаны в таблице.

№	Вариант подключения
1	**Включение Dr.Web Office Shield в качестве основного шлюза (Рекомендуемый вариант)**  • В разъем WAN подключается кабель, идущий от внешней сети (WAN); • В разъемы DMZ и LAN подключаются кабели сегмента демилитаризованной зоны и LAN соответственно
2	**Включение Dr.Web Office Shield в сеть перед существующим шлюзом**

№	Вариант подключения
	 • В разъем WAN подключается кабель, идущий от внешней сети (WAN); • В разъем LAN подключается кабель, подключаемый к разъему WAN используемого шлюза. • Разъем DMZ не используется (за разделение сети на зоны DMZ и LAN отвечает шлюз) Обратите внимание, что без специальной настройки маршрутизатора в этом случае клиенты, использующие Wi-Fi, могут оказаться отделенными от сети LAN.
3	**Включение Dr.Web Office Shield в сеть в дополнение к существующему шлюзу**  • В разъем WAN подключается кабель, идущий от разъема LAN (внутренней сети) шлюза. • В разъемы DMZ и LAN подключаются кабели сегмента демилитаризованной зоны и LAN соответственно.

№	Вариант подключения
	Обратите внимание, что без специальной настройки маршрутизации в данном случае может быть нарушена работа сервисов DNS и DHCP.
4	**Включение Dr.Web Office Shield в сеть в качестве сервера централизованной антивирусной защиты LAN**  • Через разъем LAN устройство подключается кабелем, идущим из сегмента LAN (внутренней сети). • Разъемы DMZ и WAN не используются. Обратите внимание, что на устройстве обязательно требуется задать корректные настройки подключения к LAN, а также обязательно включить и настроить службу DNS.

Использование **Dr.Web Office Shield** позволяет не использовать в сети другие шлюзы, поскольку устройство может выполнять функции шлюза (на рисунках зачеркнут шлюз, который можно отключить, если он присутствует в сети). Если помимо **Dr.Web Office Shield** в сети используются и другие шлюзы, при установке комплекса потребуется произвести также их настройку для обеспечения корректного прохождения трафика.

Обратите внимание, что если устройство используется только в качестве внутреннего сервера централизованной антивирусной защиты локальной сети, то ему не требуется подключение к WAN. Необходимо подключение к LAN в зоне сети, защищенной имеющимся шлюзом. В этом случае никаких изменений в настройки уже имеющегося шлюза (если он используется) вносить не потребуется (подробнее о настройке этого режима см. здесь).

Начальное конфигурирование с использованием кросс-кабеля

В случае возникновения проблем с доступом к устройству **Dr. Web Office Shield** по сети из-за конфликта IP-адресов в сети (если IP-адрес устройства не входит в диапазон IP-адресов сети или если присвоенный адрес занят другим устройством) имеется возможность подключиться к нему, используя кросс-кабель.

По умолчанию при первоначальных настройках в зоне LAN устройство имеет IP-адрес `192.168.1.100`.

Подключение к устройству **Dr.Web Office Shield** с использованием кросс-кабеля производится следующим образом:

1. Соедините используемый для настройки компьютер с **Dr. Web Office Shield** кросс-кабелем, подключив его на стороне устройства к разъему **LAN1**.
2. В случае необходимости задайте компьютеру, используемому для настройки устройства, новый IP-адрес.

В ОС Windows это выполняется следующим образом:

1. Открыть настройки сетевых подключений:
   - Windows XP: **Start** (**Пуск**) → **Control Panel** (**Панель управления**) → **Network Connections** (**Сетевые подключения**).
   - Windows 2000: **Start** (**Пуск**) → **Settings** (**Настройки**) → **Control Panel** (**Панель управления**) → **Network Connections** (**Сетевые подключения**).
   - Windows Vista/7: **Start** (**Пуск**) → **Control Panel** (**Панель управления**) → **Network and Internet** (**Сети и Интернет**) → **Network and Sharing Center** (**Центр управления сетями и общим доступом**) → **Change adapter settings** (**Настройка сетевого адаптера**).
2. Выбрать в открывшемся списке сетевых подключений используемую для подключения сетевую карту и, открыв по клику правой клавиши мышки меню, выбрать пункт **Properties** (**Свойства**).
3. В открывшемся окне выбрать из списка в верхней части окна пункт **Internet Protocol (TCP/IP)** (**Протокол Интернета (TCP/IP)**) и нажать **Properties** (**Свойства**).

   Примечание: Если в списке присутствуют настройки протокола Интернета версий 4 и 6, следует выбрать пункт **Internet Protocol Version 4** (**Протокол Интернета версия 4**).
4. В окне настроек сетевого адаптера на закладке **General** (**Основные**) отметить **Use the following IP adress** (**Использовать следующий IP-адрес**) и указать в поле **IP adress** (**IP-адрес**) новый адрес. Адрес следует указывать из диапазона `192.168.1.xxx`, например, `192.168.1.101`. (на компьютере и **Dr.Web Office Shield** последнее число в адресах не должно совпадать).
5. Задать **Маску подсети** (**Subnet mask**) по умолчанию – `255.255.255.0`.
6. Нажать кнопку **OK**.

3. Убедитесь, что подключение через кабель активно.

В ОС Windows это выполняется следующим образом:

В окне **Сетевые подключения** щелкнуть два раза по значку **Соединение по локальной сети**. Если настройка была проведена верно, то в поле **Состояние** будет надпись **Подключено**.

4. Для доступа к веб-интерфейсу **Dr.Web Office Shield** запустите браузер и введите в адресную строку адрес https://192.168.1.100:10000/. В первоначальном состоянии пароль доступа – **drweb**.
5. Задайте новые **Имя устройства** и **IP-адрес** на странице настройки сетевых подключений, а также смените пароль и задайте, при необходимости, другие настройки.
6. Выключите устройство и включите его в сеть штатным образом.
7. Верните сетевые настройки компьютера, использованного для настройки, в исходное состояние.

Дополнительные способы подключения к устройству см. также в разделе Доступ к настройке системы.

Задачи по настройке Dr.Web Office Shield

Здесь рассмотрены некоторые типовые ситуации, возникающие при использовании **Dr.Web Office Shield**.

1. Начало работы с Dr.Web Office Shield

Для начала работы необходимо:

- Зарегистрировать продукт с помощью лицензии.
- Сменить пароль, заданный по умолчанию.
- Проверить и установить (при необходимости) системное время.
- Проверить наличие обновлений.

2. Просмотр состояния системы

- Выполняется на странице **Главная → Состояние системы**.

3. Настройка DNS-сервера

- По умолчанию DNS-сервер, входящий в состав **Dr.Web Office Shield**, отключен.
- Включение и настройка DNS осуществляются на странице **Сеть → DNS**.

Если вы используете устройство только в качестве внутреннего сервера антивирусной защиты, вы обязательно должны включить и настроить DNS-сервер (подробнее см. здесь)

4. Настройка DHCP-сервера

- По умолчанию сервер DHCP, входящий в состав **Dr.Web Office Shield**, отключен.
- Включение и настройка DHCP осуществляется на странице **Сеть → DHCP**.

5. Настройка сетевых подключений и подключения по Wi-Fi

- Выполняется на странице **Сеть → Подключения**.

Если вы используете устройство только в качестве внутреннего сервера антивирусной защиты, вы должны отключить использование подключения WAN и корректно настроить параметры подключения к LAN (подробнее см. здесь)

6. Настройка компонентов защиты

- Управление настройками межсетевого экрана выполняется на странице **Безопасность → Firewall.**
- Включение и настройка **Веб-прокси** выполняется на странице **Безопасность → Веб-прокси.**
- Включение и настройка **Почтового прокси** выполняется на странице **Безопасность → Почтовый прокси.**
- Переход к **Центру управления Dr.Web** осуществляется на странице **Безопасность → Защита рабочих станций.**

В зависимости от приобретенной лицензии и загруженных ключей, некоторые компоненты защиты могут быть отключены и недоступны для настройки.

7. Обновление ПО Dr.Web Office Shield

- Наличие и доступность новых обновлений выводится в виде уведомления в верхней части любой страницы системы;
- Принудительная проверка наличия доступных обновлений и установка имеющихся обновлений осуществляются на странице **Система → Обновление ПО**.
- Настройка расписания проверки обновлений и действий системы при обнаружении новых пакетов для обновления задаются на странице **Система → Обновление ПО**.

- Перечень установленных пакетов ПО с указанием версий перечислен на странице **Система → Установленные пакеты**.

8. Устранение недоступности ресурсов по протоколу FTP

- Если при включенном веб-прокси у вас недоступны ресурсы по протоколу FTP, настройте использование активного режима подключения FTP у используемых FTP-клиентов.

9. Изменение языка веб-интерфейса

- Выполняется на странице **Общие настройки → Веб-интерфейс**.

10. Восстановление Dr.Web Office Shield при возникновении системных неполадок

- Сохранение и восстановление осуществляются на странице **Система → Сохранение и восстановление**.

11. Доступ к ОС Dr.Web Office Shield для нестандартной настройки или в случае сбоя

- Доступ к ОС **Dr.Web Office Shield** осуществляется через консоль.

При возникновении вопросов по использованию Dr.Web Office Shield, не рассмотренных в данном руководстве

- Обратитесь в службу технической поддержки компании **«Доктор Веб»**.

Обратите внимание, что службе технической поддержки для устранения возникших неисправностей может потребоваться удаленный доступ к вашему устройству. В этом случае вы должны быть готовы сообщить следующую информацию:

1. Имя устройства (доступно на странице настройки подключений);
2. IP-адрес устройства в зоне LAN, а также его IP-адрес в зоне WAN (со стороны Интернета), если не используется DHCP

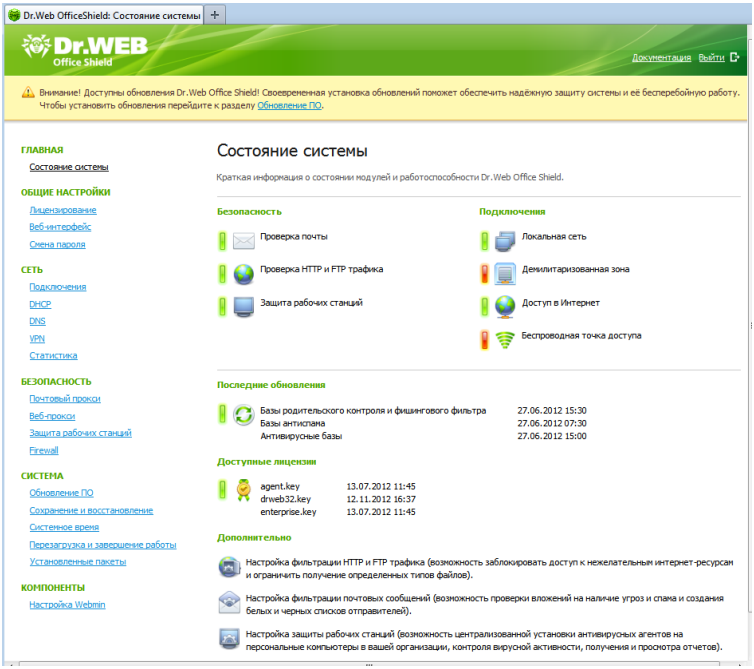
(доступно на странице настройки подключений);

3. Заданный вами пароль для входа в веб-интерфейс управления;
4. Дополнительно может потребоваться, чтобы вы включили службу VPN и сообщили имя и пароль заданной учетной записи PPP.

Управление и настройка Dr.Web Office Shield

Настройка программно-аппаратного комплекса **Dr.Web Office Shield** и управление его работой осуществляются через специально разработанный веб-интерфейс с любого компьютера, имеющего браузер и доступ в сегмент сети, в котором установлен комплекс **Dr.Web Office Shield**.

Внешний вид основной страницы веб-интерфейса управления приведен на рисунке ниже.



При запуске в разных браузерах во внешнем виде веб-интерфейса могут наблюдаться отличия от скриншотов, приведенных в данном руководстве. Все скриншоты для данного

документа сделаны с использованием браузера **Mozilla Firefox 12.0** при стандартных настройках.

В верхней части всех страниц интерфейса управления размещен заголовок продукта, а также ссылки **Документация** и **Выход**.

- Переход по ссылке **Документация** позволяет открыть в новом окне (или вкладке) браузера страницу документации по программному продукту **Dr.Web Office Shield**,
- Переход по ссылке **Выход** позволяет завершить сессию работы с веб-интерфейсом. После перехода по ссылке **Выход** для начала работы с веб-интерфейсом потребуется ввести пароль.

Также в верхней части страницы выводятся важные уведомления по работе программного комплекса, в частности, уведомления о наличии обновлений компонентов.

В левой части страницы располагается меню, предоставляющее доступ к просмотру и настройке функций комплекса **Dr.Web Office Shield**. Меню сгруппировано в следующие разделы:

- Главная — Просмотр общего состояния аппаратно-программного комплекса **Dr.Web Office Shield**;
- Общие настройки — Просмотр и настройка общих параметров функционирования, в частности – управление лицензиями;
- Сеть — Просмотр и настройка параметров сетевых подключений, управление VPN, службами DNS и DHCP;
- Безопасность — Просмотр и настройка параметров безопасности и антивирусной защиты компонентов сети;
- Система — Просмотр и настройка параметров работы встроенной ОС аппаратно-программного комплекса **Dr.Web Office Shield**, в частности, управление резервным копированием и восстановлением и обновлением программных компонентов АПК;
- Компоненты — Просмотр и настройка параметров аутентификации и доступа к управлению компонентами программного комплекса через встроенный веб-интерфейс Webmin.

По умолчанию после входа в систему и ввода пароля открывается страница просмотра общего состояния комплекса. После того как вы в первый раз зашли в систему, необходимо выполнить первоначальную настройку.

Просмотр состояния Dr.Web Office Shield

Состояние, в котором находится комплекс **Dr.Web Office Shield**, отображается на веб-странице **Главная → Состояние системы**.

На странице перечисляются:

- Состояние основных компонентов комплекса, обеспечивающих безопасность (**Проверка почты**, **Проверка HTTP- и FTP-трафика**, **Защита рабочих станций**);
- Состояние подключений к основным зонам сети (Локальная сеть, Демилитаризованная зона, Доступ в Интернет, Беспроводная точка доступа);
- Состояние и актуальность последних выполненных обновлений баз данных компонентов безопасности;
- Перечень и состояние лицензионных ключей. Для каждого имеющегося (загруженного) ключа выводится срок окончания его действия. Кроме того используется следующая цветовая индикация:
  - **Серый цвет** – файл ключа не загружен;
  - **Черный цвет** – файл ключа загружен, срок действия ключа не истек;
  - **Оранжевый цвет** – файл ключа загружен, срок действия ключа заканчивается менее чем через 14 дней;
  - **Красный цвет** – файл ключа загружен, но срок действия ключа закончился;

При отображении состояния компонентов комплекса

используются следующие обозначения:

 Компонент запущен и исправно функционирует

 Компонент не запущен или не функционирует вследствие ошибки

 Компонент не запущен, потому что отсутствует в поставке комплекса, или не активен соответствующий лицензионный ключ

Щелчок мышью по названию компонента открывает на экране страницу его настройки.

В нижней части перечислены дополнительные задачи по настройке функциональности комплекса:

- Настройка фильтрации HTTP- и FTP-трафика – переход к странице настройки **Dr.Web Веб-прокси**.
- Настройка фильтрации почтовых сообщений – переход к странице настройки **Dr.Web Почтовый прокси**.
- Настройка защиты рабочих станций – переход к странице настройки сервера **Dr.Web Enterprise Security Suite**.

Для перехода к соответствующей настройке следует щелкнуть мышью по названию нужной задачи.

Доступность компонентов, обеспечивающих безопасность, зависит от приобретенной лицензии. В случае если лицензия не полна, или соответствующие ключевые файлы не загружены, некоторые компоненты безопасности могут быть отключены и оказаться недоступными для настройки.

Первоначальные настройки

После того как вы в первый раз зашли в систему, необходимо:

- Сменить пароль, заданный по умолчанию.
- Задать настройки используемых сетевых подключений (LAN, WAN, Wi-Fi).
- Включить (если требуется) и настроить DNS, DHCP, VPN.
  - В случае если устройство **Dr.Web Office Shield** должно работать только в режиме сервера централизованной защиты локальной сети, ему требуются особые сетевые настройки и настройки DNS.
- Проверить и установить (при необходимости) системное время.
- Загрузить ключевые файлы.
- Настроить компоненты безопасности:
  - Выполнить настройку основных параметров **Почтового прокси** (если он доступен по приобретенной лицензии):
    - Включить использование компонентов **Антивирус** и **Антиспам** для проверки писем.
    - Задать **адрес почтового сервера** домена, на который будет пересылаться проверенная почта;
    - Указать **имя защищаемого домена** организации (часть `domain.com` в почтовых адресах вида `user@domain.com`);
    - Дополнительно рекомендуется задать **Перечень защищаемых сетей** в настройках ядра **Почтового прокси**.
    - Кроме того, следует модифицировать MX-запись DNS-сервера вашего домена так, чтобы она указывала на **Dr.Web Office Shield**, как на почтовый сервер домена (обратите внимание, что это действие выполняется не на устройстве).

- Включить использование **Веб-прокси** (если он доступен по приобретенной лицензии, он включается автоматически после загрузки ключа).
- Перейти к странице **Центра управления Dr.Web** централизованной антивирусной защитой для настройки **Антивирусной сети** организации (если использование **Dr.Web Enterprise Server** доступно по приобретенной лицензии).

- Ознакомьтесь также с Рекомендациями по обеспечению безопасности.

После выполнения вышеуказанной первоначальной настройки на странице просмотра состояния устройства все доступные по лицензии компоненты устройства должы отображаться как работающие в штатном режиме (отмечены индикаторами зеленого цвета).

Если для загрузки ключей на устройство вы использовали накопитель USB-flash, **не забудьте отсоединить накопитель** после загрузки ключей, поскольку при последующей перезагрузке устройства (если она потребуется, например, после обновления ПО), загрузка операционной системы **Dr.Web Office Shield** может быть остановлена из-за того, что устройство будет пытаться найти загрузчик операционной системы на вставленном съемном накопителе.

Загрузка лицензионных ключей

Для перехода к загрузке лицензионных ключей в разделе **Общие настройки** главного меню перейдите по ссылке **Лицензирование**.

В зависимости от приобретенной лицензии может использоваться от 1 до 3 файлов лицензионных ключей, которые поставляются пользователю в виде zip-архива:

- `drweb32.key` — лицензионный ключ **Dr.Web Office Shield**, определяющий права на использование компонентов защиты **Веб-прокси** и **Почтовый прокси**.
- Права пользователя на использование сервиса централизованной защиты рабочих станций регулируются при помощи пары ключевых файлов (ключевой файл для **Dr.Web Enterprise-Сервера** и ключевой файл для **Dr.Web Enterprise-Агентов** на каждой защищаемой рабочей станции):
  - `agent.key` — ключевой файл для **Dr.Web Enterprise-Агентов** на рабочих станциях защищаемой сети.
  - `enterprise.key` — ключевой файл для **Dr.Web Enterprise-Сервера**.

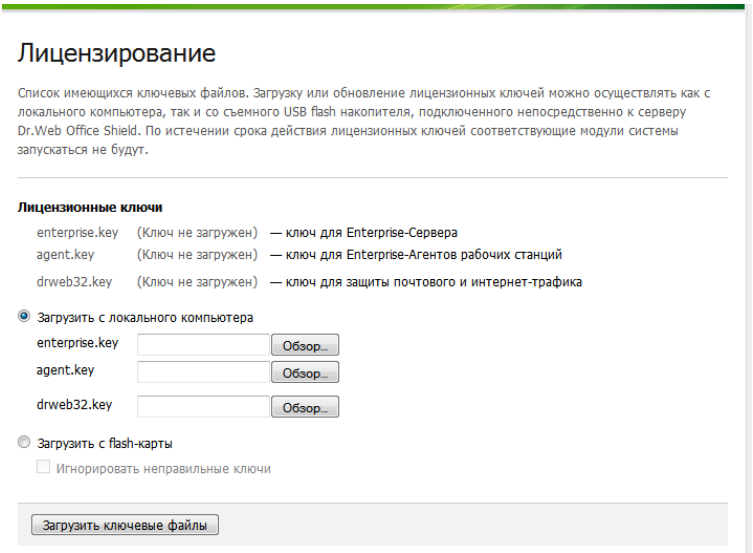
При отсутствии, недействительности или истечении срока действия лицензионных ключей соответствующие компоненты защиты сети и рабочих станций (**Enterprise Server Dr.Web**, **Веб-прокси** и **Почтовый прокси**) запускаться не будут.

На странице **Лицензирование** отображается перечень используемых лицензионных ключей. Если ключ уже был загружен, для него выводится срок окончания его действия. Кроме того используется следующая цветовая индикация:

- **Серый цвет** – файл ключа не загружен;
- **Черный цвет** – файл ключа загружен, срок действия ключа не истек;
- **Оранжевый цвет** – файл ключа загружен, срок действия ключа заканчивается менее чем через 14 дней;

- **Красный цвет** – файл ключа загружен, но срок действия ключа закончился, или ключ недействителен.

Вид страницы просмотра и загрузки лицензионных ключей приведен на рисунке ниже.



Для того чтобы зарегистрировать продукт, необходимо:

1. Приобрести лицензию;
2. Получить ключевой файл;
3. После того, как ключевые файлы были получены, их следует загрузить на устройство **Dr.Web Office Shield**. Для загрузки файлов лицензионных ключей (которые должны быть названы в соответствии с указанными названиями) выберите один из вариантов:
   - **Загрузить с локального компьютера**;
   - **Загрузить с flash-карты**.

При выборе варианта **Загрузить с локального компьютера** следует указать имя и путь к файлу ключа, расположенного на локальном компьютере (нажав кнопку **Обзор...** и указав файл в открывшемся окне выбора файла).

При выборе варианта **Загрузить с flash-карты** следует разместить ключевые файлы на съемном USB-накопителе, который подключить к любому USB-порту, расположенному на устройстве **Dr.Web Office Shield**. Обратите внимание, что файлы ключей должны быть размещены в корневом разделе накопителя и называться ожидаемыми именами (`drweb32.key`, `agent.key`, `enterprise.key`).

В случае если на flash-накопителе совместно расположены корректные ключи и ключи с истекшим сроком годности, следует включить флажок **Игнорировать неправильные ключи**. Это позволит загрузить на устройство только файлы корректных ключей, и проигнорировать некорректные ключи. В противном случае при наличии хотя бы одного некорректного ключа загрузка ключей потерпит неудачу.

4. После указания варианта загрузки ключей для их загрузки на сервер из указанного места следует нажать кнопку **Загрузить ключевые файлы**, после чего файлы ключей будут скопированы и сохранены на сервере **Dr.Web Office Shield**.

Для того чтобы продлить действие лицензии, необходимо:

1. Продлить лицензию;
2. Получить новые ключевые файлы;
3. Загрузить полученные ключи на устройство **Dr.Web Office Shield**.

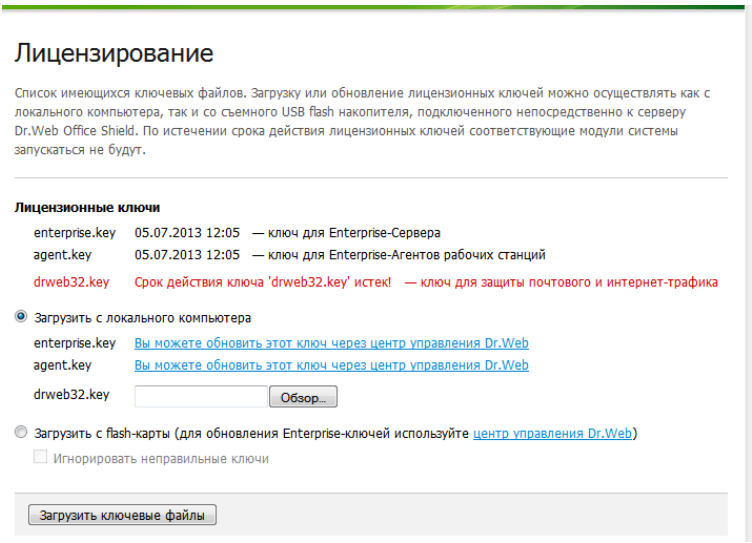
   Обратите внимание, что при продлении ключевые файлы, используемые для работы компонентов настроенной **Антивирусной сети Dr.Web** (`agent.key` и `enterprise.key` соответственно) на данной странице не загружаются. Для их загрузки на устройство **Dr.Web Office Shield** необходимо по соответствующей ссылке перейти на страницу **Центра управления Dr.Web**.

Для доступа к **Центру управления Dr.Web** вам, возможно, потребуется указать логин и пароль доступа.

Обратите внимание, что пароль доступа к **Dr.Web Office Shield** никак не связан с логином и паролем, используемым для доступа к **Центру управления Dr.Web**. Логин и пароль доступа к **Центру управления Dr.Web** задаются в **Центре управления Dr.Web**. По умолчанию (при заводских настройках устройства) в качестве пары логин/пароль задано `admin/root`.

Дополнительные сведения о работе с **Центром Управления Dr.Web** содержатся в Руководстве администратора **Антивирусной сети Dr.Web**, которое доступно по адресу: http://support.drweb.com/esuite/doc_ru.

Вид страницы просмотра и загрузки лицензионных ключей в режиме продления приведен на рисунке ниже.



Если для загрузки ключей на устройство вы использовали накопитель USB-flash, **не забудьте отсоединить накопитель** после загрузки ключей, поскольку при последующей перезагрузке устройства (если она потребуется, например, после обновления ПО), загрузка операционной системы **Dr.Web Office Shield** может быть остановлена из-за того, что устройство будет пытаться найти загрузчик операционной системы на вставленном съемном накопителе.

Настройка веб-интерфейса

Для настройки параметров веб-интерфейса **Dr.Web Office Shield** необходимо перейти по ссылке **Общие настройки → Веб-интерфейс**.

Доступна настройка следующих параметров веб-интерфейса:

- Язык веб-интерфейса. Для смены языка выберите нужный язык в выпадающем списке **Язык веб-интерфейса.**

Для применения указанных изменений нажмите кнопку **Применить и сохранить изменения.** Если необходимо отменить внесенные изменения и вернуть предыдущие сохраненные настройки, нажмите кнопку **Отменить изменения.**

Смена и восстановление пароля

Смена пароля

Для смены пароля в главном меню выберите раздел **Общие настройки → Смена пароля**.

Укажите новый пароль в поле **Новый пароль** и подтвердите его в поле **Повтор пароля**.

Для сохранения измененного пароля нажмите кнопку **Применить и сохранить изменения.** Если необходимо отменить сохранение пароля, нажмите кнопку **Отменить изменения.**

При первом входе в систему необходимо сменить пароль, заданный по умолчанию. По умолчанию в качестве пароля используется слово `drweb`.

Перед сменой пароля рекомендуется ознакомиться с Рекомендациями по обеспечению безопасности.

Восстановление пароля

Если пароль для доступа к веб-интерфейсу **Dr.Web Office Shield** был забыт или утрачен, то существует два способа восстановления пароля:

1. Если имеется активная сессия доступа к веб-интерфейсу, смените пароль, перейдя в раздел меню **Общие настройки → Смена пароля**.
2. Если активной сессии доступа к веб-интерфейсу не имеется, то необходимо выполнить восстановление образа системы на устройстве **Dr.Web Office Shield**.

Обратите внимание, что пароль доступа к **Dr.Web Office Shield** никак не связан с логином и паролем, используемым для доступа к **Центру управления Dr.Web**. Логин и пароль доступа к **Центру управления Dr.Web** задаются в **Центре управления Dr.Web**. По умолчанию (при заводских настройках устройства) в качестве пары логин/пароль задано `admin/root`.

Дополнительные сведения о работе с **Центром Управления Dr.Web** содержатся в Руководстве администратора **Антивирусной сети Dr.Web**, которое доступно по адресу: http://support.drweb.com/esuite/doc_ru.

Управление сетями

Веб-интерфейс **Dr.Web Office Shield** позволяет настроить подключение устройства к демилитаризованной зоне, локальной сети LAN и к глобальной сети WAN, настроить беспроводное подключение к сети LAN через Wi-Fi, а также использовать **Dr.Web Office Shield** как сервер DHCP и DNS (DNS-запросы будут перенаправляться на указанный DNS-сервер).

Дополнительно возможно подключить виртуальную частную сеть VPN и просмотреть статистику по использованию Интернета.

Доступ к управлению сетями и подключениями осуществляется по ссылкам, размещенным в разделе **Сеть** главного меню.

Раздел **Сеть** содержит следующие ссылки:

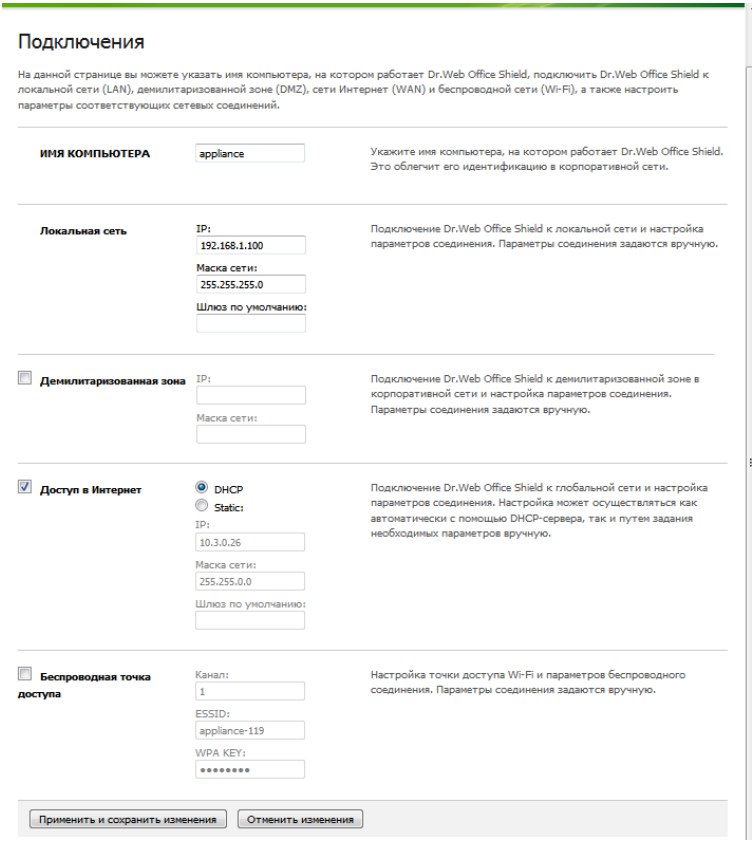
- Подключения — настроить подключение **Dr.Web Office Shield** к сетям WAN, DMZ, LAN и Wi-Fi;
- DHCP — настроить использование **Dr.Web Office Shield** в качестве DHCP-сервера;
- DNS — настроить использование **Dr.Web Office Shield** в качестве DNS-сервера;

- VPN — настроить персональную сеть VPN;
- Статистика — просмотр статистики по использованию Интернета.

Настройка подключений

Для перехода к странице настройки подключений следует перейти по ссылке **Подключения** в разделе **Сеть** главного меню веб-интерфейса **Dr.Web Office Shield**.

На странице **Подключения** отображены основные настройки подключения устройства **Dr.Web Office Shield** к основным сегментам сети (DMZ, LAN, WAN), а также настройки точки доступа Wi-Fi. Внешний вид страницы **Подключения** указан на рисунке ниже.



Имеется возможность задать следующие настройки:

Параметр	Описание
Имя компьютера	Имя, присвоенное устройству **Dr.Web Office Shield**. Используется для облегчения идентификации устройства в сети.
Локальная сеть	При подключении **Dr.Web Office Shield** к локальной сети требуется указать: • **IP-адрес** устройства в зоне LAN; • Используемую **маску сети**. • IP-адрес используемого **шлюза**.

Параметр	Описание
	Параметры **IP-адрес** и **маска** являются обязательными. Адрес **шлюза** указывается обязательно в том случае, если не используется подключение к сети WAN (например, если устройство работает только в качестве *внутреннего сервера антивирусной защиты*). Пожалуйста, обратите внимание, что если в сети LAN у вас используется сервер DHCP, IP-адрес устройства в зоне LAN должен быть вне диапазона IP-адресов, назначаемых DHCP-сервером (во избежание возможных конфликтов IP-адресов в сети LAN).
Демилитаризованная зона	Включает или выключает использование сегмента сети, подключенного к разъему DMZ (демилитаризованная зона). При включении подключения **Dr.Web Office Shield** к демилитаризованной зоне требуется указать: • **IP-адрес** устройства в зоне DMZ; • Используемую **маску сети**. Оба параметра являются обязательными.
Доступ в Интернет	Включает или выключает использование сегмента сети, подключенного к разъему WAN (как правило, выход в Интернет). При включении подключения **Dr.Web Office Shield** к WAN требуется указать режим назначения IP-адреса **Dr.Web Office Shield** в зоне Интернета. Допустимо использование двух режимов: • **DHCP** – IP-адрес устройства будет автоматически назначен DHCP-сервером сети; • **Static** – Устройство будет использовать **IP-адрес** и **маску сети**, указанные пользователем. В случае выбора режима **Static** обязательно требуется указать **IP-адрес**, **маску сети** и используемый **шлюз по умолчанию**. Обратите внимание, что если устройство

Параметр	Описание
	работает только в качестве *внутреннего сервера антивирусной защиты*, **Доступ в Интернет** следует отключить.
Беспроводная точка доступа	Включает или выключает использование встроенной в устройство **Dr.Web Office Shield** точки доступа Wi-Fi для предоставления беспроводного доступа к сети LAN. При включении беспроводной точки доступа требуется указать следующие параметры: • **Канал** – Номер используемого радиоканала. Требуется изменять только при наличии в зоне видимости нескольких сетей Wi-Fi; • **ESSID** – Идентификатор точки доступа, который будут отображать использующие ее устройства; • **WPA KEY** – Ключ (пароль) доступа, который потребуется ввести для подключения к этой точке. Требуется указать не менее 8 символов. В случае включения беспроводной точки доступа все параметры являются обязательными. При включении беспроводной точки доступа ознакомьтесь, пожалуйста, с Рекомендациями по обеспечению безопасности.

Для применения указанных изменений нажмите кнопку **Применить и сохранить изменения.** Если необходимо отменить внесенные изменения и вернуть предыдущие сохраненные настройки, нажмите кнопку **Отменить изменения.**

Процесс активации настроек может временно сделать вашу систему недоступной по сети и прервать доступ к серверу **Dr. Web Office Shield**.

Настройка DHCP

DHCP – это сервис централизованного управления сетевыми настройками компьютеров, входящих в локальную сеть. В первую очередь DHCP используется для распределения IP-адресов между компьютерами, составляющими локальную сеть.

Для перехода к странице настройки DHCP следует перейти по ссылке **DHCP** в разделе **Сеть** главного меню веб-интерфейса **Dr.Web Office Shield**.

На странице **DHCP** можно настроить **Dr.Web Office Shield** для использования в качестве DHCP-сервера для сети LAN, что позволит ему назначать IP-адреса клиентам локальной сети LAN.

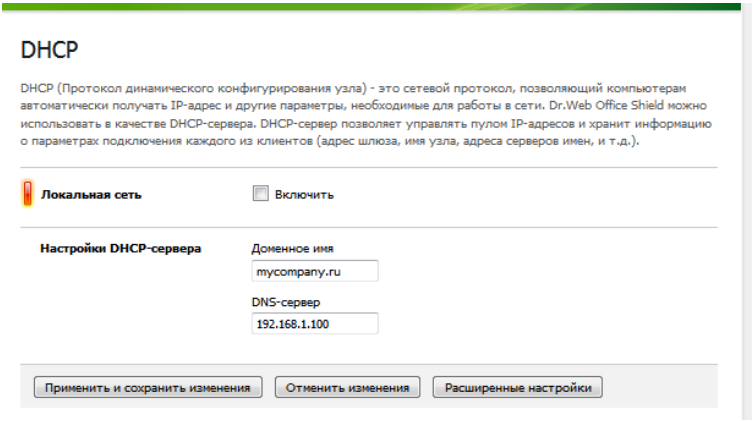
Если в сети уже имеется сервер DHCP, то подключение еще одного сервера может создать проблемы.

При открытии страницы отображаются упрощенные настройки DHCP:

- Флажок **Включить** позволяет включить или выключить использование **Dr.Web Office Shield** в качестве DHCP-сервера в сети LAN.
- При включении DHCP требуется указать параметры его работы:
  - Используемое **доменное имя**;
  - IP-адрес **DNS-сервера**, который DHCP-сервер **Dr.Web Office Shield** будет выдавать клиентам в локальной сети.

Обратите внимание, что по умолчанию в качестве IP-адреса DNS-сервера используется IP-адрес, присвоенный **Dr.Web Office Shield** в LAN. Это предполагает, что вы включили в устройстве сервис DNS. Если это не так, следует задать правильный IP-адрес используемого в сети DNS-сервера.

Внешний вид страницы упрощенных настроек изображен на рисунке ниже.



Для применения указанных изменений нажмите кнопку **Применить и сохранить изменения.** Если необходимо отменить внесенные изменения и вернуть предыдущие сохраненные настройки, нажмите кнопку **Отменить изменения.**

Для уточнения и изменения настроек DHCP нажмите кнопку **Расширенные настройки.**

Раздел **Расширенные настройки** позволяет задать следующие параметры:

- Подсети и разделяемые сети;
- Узлы и группы узлов.

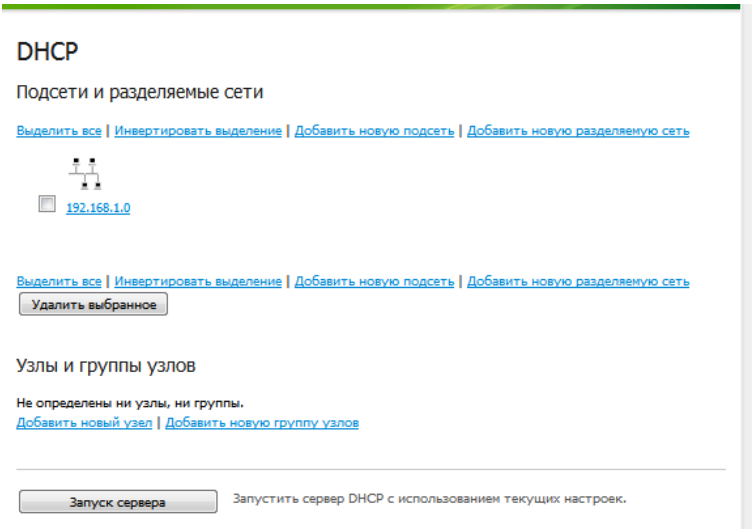
Подсети и разделяемые сети

Управление подсетями и разделяемыми сетями выполняется на странице расширенных настроек DHCP.

Для настройки подсетей и разделяемых сетей

- Выберите в главном меню в разделе **Сеть** пункт **DHCP**;
- Нажмите кнопку **Расширенные настройки**.

Вид страницы расширенных настроек DHCP приведен на рисунке ниже.



Дополнительно на данной странице можно осуществить запуск и остановку сервера DHCP, нажав соответствующую кнопку в нижней части страницы.

Подсети

Для простейшей конфигурации сервера DHCP необходимо создать подсеть для выдачи IP-адресов клиентам одной локальной сети. По умолчанию в качестве единственной

подсети используется вся зона LAN. Перечень заданных для сервера подсетей и разделяемых сетей выводится в разделе **Подсети и разделяемые сети.**

Добавление новых подсетей

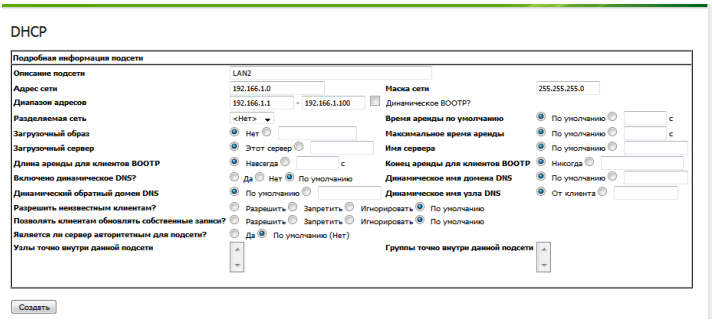
Чтобы добавить новую подсеть:

1. Кликните по ссылке **Добавить новую подсеть** в разделе **Подсети и разделяемые сети**. После этого откроется страница добавления и настройки DHCP-параметров новой подсети.
2. В поле **Описание подсети** введите описание подсети (не обязательно);
3. Введите сетевой адрес в поле **Адрес сети**. Адрес должен принадлежать сети LAN, к которой непосредственно подключен **Dr.Web Office Shield**.
4. Введите маску сети в поле **Маска сети**.
5. Введите начальный и конечный адрес диапазона IP-адресов для назначения клиентам в поля **Диапазон адресов**. Размер диапазона следует задавать таким образом, чтобы в нем содержалось IP-адресов не меньше, чем имеется клиентов в данной подсети.
6. Для включения данной подсети в разделяемую сеть выберите разделяемую сеть в выпадающем списке **Разделяемая сеть** (если необходимо).
7. Выберите срок аренды IP-адресов для клиентов. Срок аренды – это интервал времени, в течение которого компьютер может использовать IP-адрес, назначенный сервером DHCP.
   - выберите **Время аренды по умолчанию** (**По умолчанию**, или указав срок аренды в секундах);
   - выберите **Максимальное время аренды** (**По умолчанию**, или указав срок аренды в секундах).

   Настройка максимального времени аренды позволит запретить клиентам запрашивать срок аренды IP-адресе на период времени, больший, чем указано для данного параметра.
8. Остальные параметры подсети на данной странице рекомендуется оставить по умолчанию.

9. Нажмите кнопку **Создать**, чтобы добавить новую подсеть в конфигурацию DHCP-сервера.

Вид страницы добавления новой подсети приведен на рисунке ниже.



Редактирование подсетей

Для редактирования параметров подсети нажмите на название или изображение подсети в списке **Подсети и разделяемые сети**, после чего на экране откроется страница редактирования параметров подсети, аналогичная странице добавления новой подсети. Дополнительно на данной странице можно внести следующие изменения в подсеть:

- Настроить параметры DHCP-клиента,
- Просмотреть список адресованных адресов,
- Добавить узел или группу узлов внутри подсети
- Добавить или изменить пул адресов.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**.

Удаление подсетей

Для удаления подсети выделите ее, активировав флажок возле названия и изображение подсети в списке **Подсети и разделяемые сети**. При необходимости можно выделить несколько подсетей, активировав соответствующие флажки. Дополнительные возможности выделения:

- Щелчок по ссылке **Выделить все** выделяет все подсети в списке,
- Щелчок по ссылке **Инвертировать выделение** инвертирует выделение, делая не выбранные элементы списка выбранными, и наоборот.

Для удаления выбранных подсетей необходимо нажать кнопку **Удалить выбранное**.

Удаление подсетей – необратимая операция. В случае если удаленная подсеть потребуется в дальнейшем, ее придется создать и настроить заново.

Разделяемые сети

Разделяемая сеть — это группа подсетей, которые логически разделяют одну LAN. Если внутри одной LAN имеется несколько IP-сетей, то конфигурация DHCP-сервера должна быть помещена внутри разделяемой сети. В противном случае сервер может работать некорректно или сообщать об ошибках при запуске. Не следует использовать подсети с различными LAN внутри одной разделяемой подсети.

Добавление новых разделяемых подсетей

Чтобы добавить новую разделяемую сеть:

1. Кликните по ссылке **Добавить новую разделяемую сеть** в разделе **Подсети и разделяемые сети**. После этого откроется страница добавления и настройки параметров новой разделяемой сети.
2. Введите имя сети в поле **Название сети**.
3. Выберите срок аренды IP-адресов для клиентов.
   - выберите **Время аренды по умолчанию** (**По умолчанию**, или указав срок аренды в секундах);
   - выберите **Максимальное время аренды** (**По умолчанию**, или указав срок аренды в секундах).

   Настройка максимального времени аренды позволит запретить клиентам запрашивать срок аренды IP-адресе на период времени, больший, чем указано для данного параметра.
4. Выберите в списке существующих подсетей сети, подлежащие включению в данную разделяемую сеть.

Необходимо выбрать хотя бы одну подсеть, т.к. разделяемая сеть не может быть пустой.

5. Нажмите кнопку **Создать**, чтобы добавить новую разделяемую сеть в конфигурацию DHCP-сервера.

Редактировать разделяемую сеть

Для редактирования параметров разделяемой сети нажмите на название или изображение сети в списке **Подсети и разделяемые сети**, после чего на экране откроется страница редактирования параметров сети, аналогичная странице добавления новой разделяемой сети. Дополнительно на данной странице можно внести следующие изменения в разделяемую сеть:

- Настроить параметры DHCP-клиента,
- Добавить узел или группу узлов внутри подсети
- Добавить или изменить пул адресов.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**.

Удаление разделяемых сетей

Выполняется аналогично удалению подсетей. Для удаления необходимо отметить разделяемые сети, подлежащие удалению, и нажать кнопку **Удалить выбранное**.

Удаление разделяемых сетей – необратимая операция. В случае если удаленная разделяемая сеть потребуется в дальнейшем, ее придется создать и настроить заново.

Узлы и группы узлов

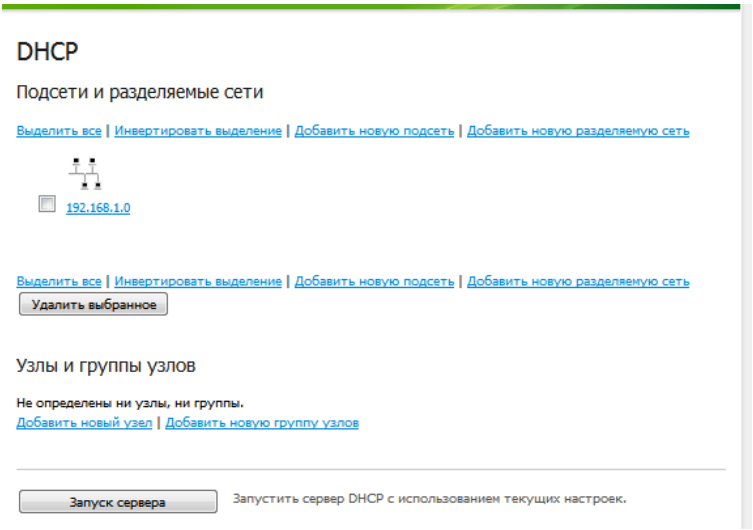
Для назначения IP-адреса на определенный узел необходимо добавить этот узел в конфигурацию DHCP-сервера. Также здесь можно настроить параметры клиента для узла сети, например адреса DNS-сервера или маршрутизатор по умолчанию.

Управление узлами и группами выполняется на странице расширенных настроек DHCP.

Для настройки узлов и групп узлов

- Выберите в главном меню в разделе **Сеть** пункт **DHCP**;
- Нажмите кнопку **Расширенные настройки**.

Вид страницы расширенных настроек DHCP приведен на рисунке ниже.



Добавление новых узлов

Чтобы добавить в сеть новый узел, выполните следующие действия:

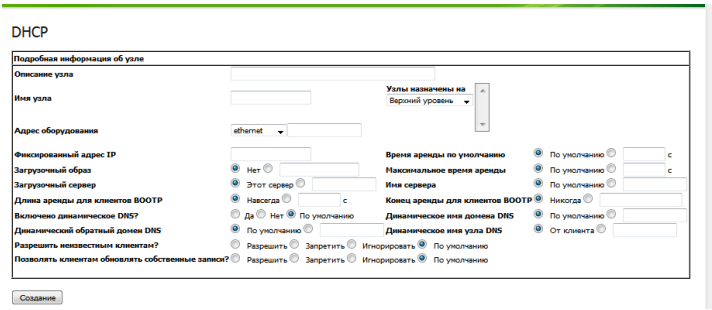
1. Нажмите ссылку **Добавить новый узел** в разделе **Узлы и группы узлов**. При этом на экране откроется страница редактирования параметров узла.
2. Введите **Описание узла** и его имя узла в поле **Имя узла** (необязательные параметры).
3. Выберите тип сети для узла из выпадающего списка **Адрес оборудования** и укажите в поле справа от типа адреса 48-разрядный (6 октетов) MAC-адрес, который

разделен на четыре части.

> Сервер определяет хосты с помощью MAC-адреса (аппаратный адрес устройства, присоединенного к сетевой среде). Для того, чтобы узнать MAC-адрес сетевого устройства, используйте следующие команды:
> - **ОС Linux** — `ifconfig -a`,
> - **ОС Windows** — `ipconfig`.

4. Введите IP-адрес для текущего клиента в поле **Фиксированный адрес IP**.
5. Выберите назначение узла в выпадающем списке **Назначение узлов**. Для назначения узла подсети и наследования параметров клиента выберите в списке пункт "Подсеть".
6. Остальные настройки узла рекомендуется оставить настроенными по умолчанию.
7. Нажмите кнопку **Создать**, чтобы добавить новый узел в конфигурацию DHCP-сервера.

Вид страницы добавления нового узла приведен на рисунке ниже.



Редактирование узлов

Для редактирования параметров узла нажмите на название или изображение узла в списке **Узлы и группы узлов**, после чего на экране откроется страница редактирования параметров узла, аналогичная странице добавления нового узла.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**.

Удаление узлов

Для удаления узла выделите его, активировав флажок возле названия и изображения узла в списке **Узлы и группы узлов**. При необходимости можно выделить несколько узлов, активировав соответствующие флажки. Дополнительные возможности выделения:

- Щелчок по ссылке **Выделить все** выделяет все узлы и группы в списке,
- Щелчок по ссылке **Инвертировать выделение** инвертирует выделение, делая не выбранные элементы списка выбранными, и наоборот.

Для удаления выбранных узлов необходимо нажать кнопку **Удалить выбранное**.

Удаление узлов – необратимая операция. В случае если удаленный узел потребуется в дальнейшем, его придется создать и настроить заново.

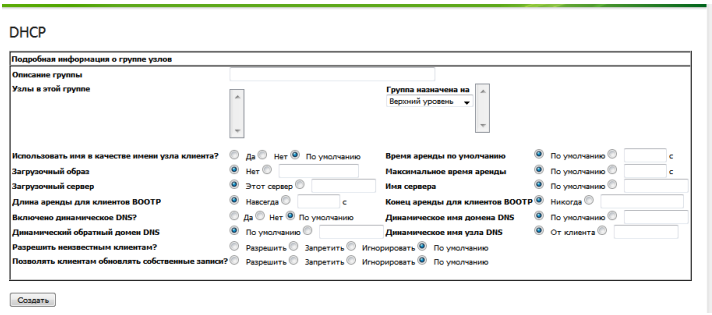
Добавление новых групп узлов

Чтобы добавить в сеть новую группу узлов, выполните следующие действия:

1. Нажмите ссылку **Добавить новую группу узлов** в разделе **Узлы и группы узлов**. При этом на экране откроется страница редактирования параметров группы узлов.
2. Введите **Описание группы** узлов (необязательный параметр).
3. В списке **Узлы в этой группе** выделите узлы, входящие в создаваемую группу. Если узлов в списке нет, то предварительно создайте их (см. выше).
4. Укажите время аренды IP-адресов для узлов в группе (по умолчанию, или задайте его в секундах).
5. Выберите назначение группы узлов в выпадающем списке **Группа назначена на**.
6. Остальные настройки группы узла рекомендуется оставить настроенными по умолчанию.
7. Нажмите кнопку **Создать**, чтобы добавить новую группу

узлов в конфигурацию DHCP-сервера.

Вид страницы добавления новой группы узлов приведен на рисунке ниже.



Редактирование групп узлов

Для редактирования параметров группы узлов нажмите на название или изображение группы узлов в списке **Узлы и группы узлов**, после чего на экране откроется страница редактирования параметров группы узлов, аналогичная странице добавления новой группы узлов.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**.

Удаление группы узлов

Удаление групп узлов выполняется аналогично удалению узлов. Для удаления групп узлов необходимо отметить их в списке **Узлы и группы узлов** и нажать кнопку **Удалить выбранное**.

Удаление групп узлов – необратимая операция. В случае если удаленная группа узлов потребуется в дальнейшем, ее придется создать и настроить заново.

Настройка DNS

Dr.Web Office Shield может быть использован как сервер имен DNS (сервер, содержащий часть базы данных DNS, используемой для доступа к именам компьютеров в интернет-домене) для отправки DNS-запросов для внешних серверов DNS, находящихся за пределами вашей сети. Использование сервера имен DNS позволяет преобразовывать внешние имена доменов (такие, например, как `drweb.com`) в IP-адреса и позволяет улучшить эффективность преобразования имен для компьютеров вашей сети.

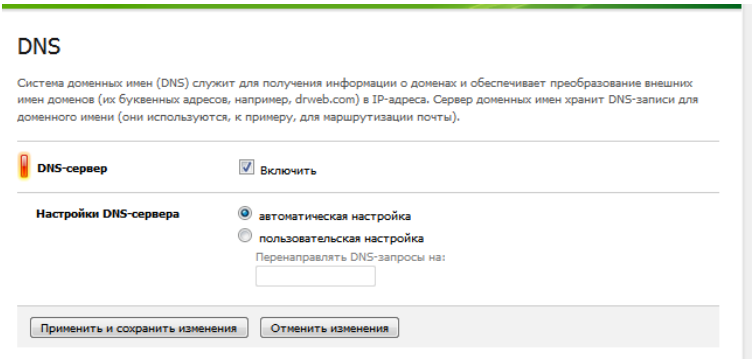
В **Dr.Web Office Shield** используется **BIND** (Berkeley Internet Name Domain) — открытая и наиболее распространенная реализация DNS-сервера.

Для перехода к странице настройки DNS следует перейти по ссылке **DNS** в разделе **Сеть** главного меню веб-интерфейса **Dr.Web Office Shield**.

На странице настройки DNS доступны следующие настройки DNS-сервера:

- Флажок **Включить** позволяет включить или выключить использование **Dr.Web Office Shield** в качестве DNS-сервера в сети LAN.
- При включении DNS требуется указать используемую настройку его работы:
  - При **автоматической настройке** **Dr.Web Office Shield** будет пытаться использовать адрес DNS-сервера, указанный в настройках ОС (в файле `resolv.conf`). Если этот файл не существует или пуст, то будет использован адрес DNS-сервера локальной машины (т. е. **Dr.Web Office Shield**);
  - При **пользовательской настройке** DNS следует за дать IP-адрес DNS-сервера, на который будут перенаправляться DNS-запросы клиентов.

Внешний вид страницы настроек DNS изображен на рисунке ниже.



Если вы используете устройство **Dr.Web Office Shield** только в режиме внутреннего сервера антивирусной защиты (при отключенном WAN), следует обязательно **включить** DNS-сервер в режиме **пользовательской настройки**, указав **IP-адрес DNS-сервера**, на который будут перенаправляться DNS-запросы клиентов!

В противном случае не сможет корректно работать встроенный в устройство сервер централизованной защиты антивирусной сети **Dr.Web Enterprise Server**.

Для применения указанных изменений нажмите кнопку **Применить и сохранить изменения.** Если необходимо отменить внесенные изменения и вернуть предыдущие сохраненные настройки, нажмите кнопку **Отменить изменения.**

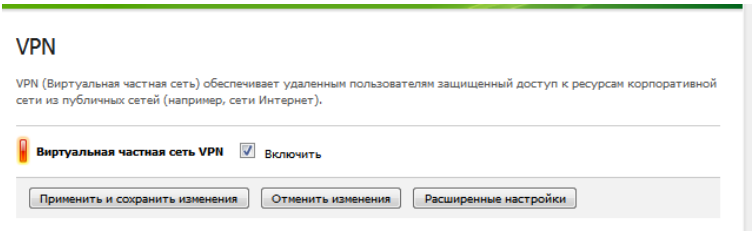
Настройка VPN

Под VPN понимается виртуальная частная сеть, то есть подсеть корпоративной сети, которая обеспечивает безопасный вход в сеть удаленных пользователей.

Для перехода к странице настройки VPN следует перейти по ссылке **VPN** в разделе **Сеть** главного меню веб-интерфейса **Dr.**

Web Office Shield. На главной странице можно подключить или отключить VPN при помощи флажка **Включить**.

Вид страницы включения VPN показан на рисунке ниже.



По умолчанию для VPN выделена сеть диапазона `192.168.3.0/24`.

Пользователь по умолчанию — `vpn_user`.

Пароль по умолчанию — `drweb`.

Пользователь по умолчанию может подключаться к сети с любого IP-адреса.

Для применения указанных изменений нажмите кнопку **Применить и сохранить изменения.** Если необходимо отменить внесенные изменения и вернуть предыдущие сохраненные настройки, нажмите кнопку **Отменить изменения.**

Для перехода к дополнительным настройкам VPN нажмите кнопку **Расширенные настройки.**

Раздел **Расширенные настройки** позволяет задать следующие параметры:

- Опции PPTP-сервера — сервера протокола PPTP (Point-to-point tunneling protocol), обеспечивающего создание защищенных соединений.
- Учетные записи PPP — управление учетными записями пользователей, имеющих удаленный доступ к сети.
- Активные соединения — просмотр активных VPN-соединений и управление ими.

Обратите внимание, что по умолчанию служба VPN при поставке устройства **отключена**. Однако ее можно использовать для удаленного доступа к устройству, к примеру, со стороны службы технической поддержки компании **«Доктор Веб»** по вашему запросу.

Поэтому в настройках VPN по умолчанию присутствует учетная запись пользователя `vpn_user`. В случае если службе поддержки для решения проблем с устройством потребуется удаленный доступ через VPN, вам достаточно будет только включить флажок, разрешающий **Виртуальную частную сеть VPN**.

Подробнее об обращении в службу технической поддержки см. в разделе Техническая поддержка.

Перед использованием VPN ознакомьтесь, пожалуйста, с Рекомендациями по обеспечению безопасности.

Настройки PPTP-сервера

PPTP-серверы – это узлы присоединения к сети, которые поддерживают протокол PPTP и способны принимать запросы обслуживания для VPN из других узлов сети (удаленных и локальных). В состав **Dr.Web Office Shield** входит сервер PPTP.

Управление настройками PPTP-сервера выполняется на странице расширенных настроек VPN.

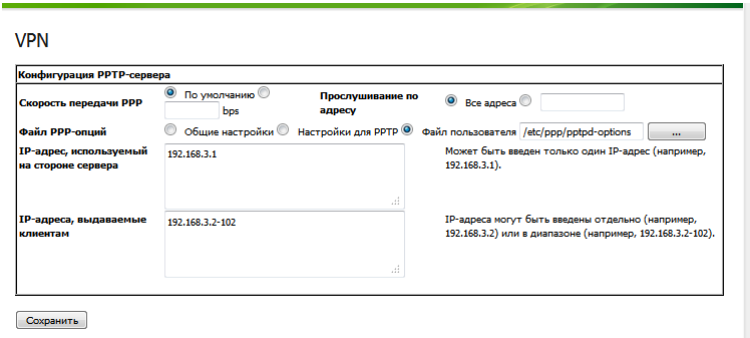
Управление настройками PPTP-сервера

- Выберите в главном меню в разделе **Сеть** пункт **VPN**;
- Нажмите кнопку **Расширенные настройки**.

Вид страницы расширенных настроек VPN приведен на рисунке ниже.

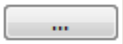
Дополнительно на данной странице можно осуществить запуск и остановку сервера PPTP, нажав соответствующую кнопку в нижней части страницы.

Для настроек PPTP-сервера перейдите по ссылке **Опции PPTP-сервера**. При этом на экране откроется страница настройки параметров PPTP-сервера, приведенная на рисунке ниже.



На странице доступны следующие настройки сервера:

Параметр	Описание
Скорость передачи PPP	Выбор скорости передачи информации по протоколу PPP. Имеется возможность указать следующие режимы: • **По умолчанию** – в этом случае скорость

Параметр	Описание
	будет определяться системой (рекомендуется); • Вручную, указав собственное значение скорости передачи (bps).
Прослушивание по адресу	Указание IP-адресов интерфейсов, на которые которых будут приниматься VPN-соединения. Имеется возможность указать следующие режимы: • **Все адреса** – соединения будут приниматься на все интерфейсы; • Указанный IP-адрес – Соединения будут приниматься только на интерфейс, имеющий указанный IP-адрес.
Файл PPP-опций	Указание файла, в котором будут храниться дополнительные настройки PPTP. Доступны следующие пункты: • **Общие настройки** – настройки будут храниться в общем конфигурационном файле (по умолчанию). • **Настройки для PPTP** – настройки будут храниться в конфигурационном файле PPTP. • **Файл пользователя** – настройки будут храниться в конфигурационном файле, указанном пользователем (файл должен находиться в файловой системе сервера **Dr. Web Office Shield**). При выборе этого пункта следует указать путь к файлу, для чего можно воспользоваться кнопкой  . В этом случае на экране откроется окно обзора файловой системы. В нем следует выбрать имя нужного файла и нажать кнопку **OK**.
IP-адрес, используемый на стороне сервера	Указывается IP-адрес, используемый сервером PPTP. Этот адрес должен отличаться от IP-адресов, выделенных клиентам VPN. Параметр является обязательным
Клиентские IP-адреса	Указывается перечень IP-адресов клиентов VPN. Адреса указываются через запятую. Могут быть указаны диапазоны IP-адресов (младший и

Параметр	Описание
	старший адрес диапазона разделяются дефисом). Например: Запись `192.168.3.2-102` задает диапазон адресов от `192.168.3.2` до `192.168.3.102` включительно. Необходимо указать не менее одного клиентского адреса.

Для сохранения указанных изменений нажмите кнопку **Сохранить**.

Учетные записи PPP

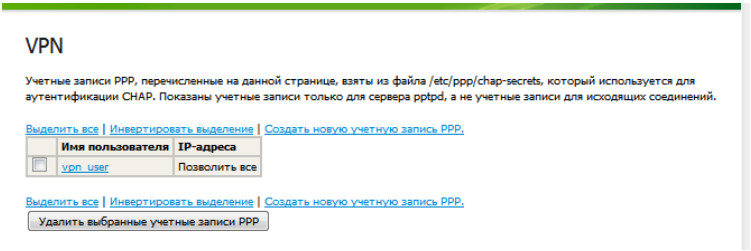
Учетные записи протокола PPP используются для обеспечения подключения внешних пользователей к локальной сети через VPN. Просмотр и управление учетными записями протокола PPP выполняется на странице расширенных настроек VPN.

Перед изменением учетных записей PPP ознакомьтесь, пожалуйста, с Рекомендациями по обеспечению безопасности.

Управление учетными записями PPP

- Выберите в главном меню в разделе **Сеть** пункт **VPN**;
- Нажмите кнопку **Расширенные настройки**.

Для просмотра и управления учетными записями протокола PPP перейдите по ссылке **Учетные записи PPP**. При этом на экране откроется страница настройки параметров протокола PPP, приведенная на рисунке ниже.



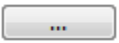
Набор учетных записей PPP по умолчанию

По умолчанию в **Dr.Web Office Shield** для PPP-соединений в рамках VPN уже имеется настроенная учетная запись пользователя. Эта учетная запись имеет следующие параметры:

- **Имя пользователя (логин)**: `vpn_user`;
- **Пароль**: `drweb`;
- **Действительные адреса**: все.

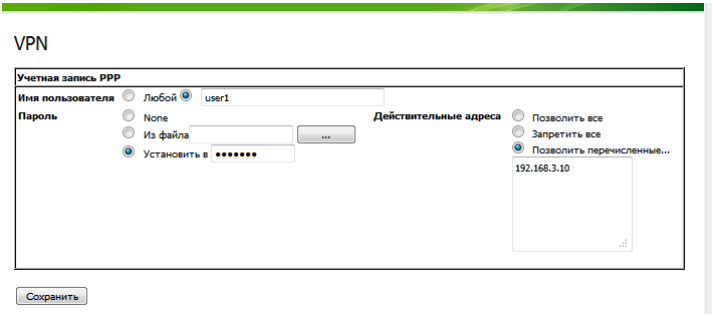
Добавление новой учетной записи PPP

Чтобы добавить новую учетную запись:

1. Кликните по ссылке **Создать новую учетную запись PPP**. После этого откроется страница добавления и настройки параметров новой учетной записи PPP.
2. В поле **Пароль** выберите требуемый переключатель, определяющий способ определения пароля:
   - **None** – пароль не используется, пользователю не потребуется вводить пароль;
   - **Из файла** – в текстовом поле справа требуется указать путь к файлу, содержащему пароль (файл должен находиться в файловой системе сервера **Dr.Web Office Shield**). Для выбора файла можно воспользоваться кнопкой  . В этом случае на экране откроется окно обзора файловой системы. В нем следует выбрать имя нужного файла и нажать кнопку **ОК**.
   - **Установить в** – в текстовое поле справа следует ввести используемый пользователем пароль.

3. В поле **Действительные адреса** следует указать, с каких адресов пользователю будет разрешен доступ в сеть. Выберите требуемый переключатель:
   - **Позволить все** – пользователю будет разрешено заходить в сеть и авторизоваться с любого IP-адреса;
   - **Запретить все** – пользователь не сможет зайти в сеть и авторизоваться ни с одного IP-адреса;
   - **Позволить перечисленные** – пользователь сможет зайти в сеть и авторизоваться, только если он будет заходить с хоста, имеющего IP-адрес, попадающий в указанный список адресов (адреса перечисляются через запятую, в этом режиме должно быть указано не менее одного IP-адреса);
4. Нажмите кнопку **Сохранить**, чтобы добавить новую учетную запись PPP в конфигурацию сервера.

Вид страницы добавления новой учетной записи приведен на рисунке ниже.



Редактирование учетных записей PPP

Для редактирования учетной записи нажмите на название учетной записи в списке учетных записей, после чего на экране откроется страница редактирования учетной записи, аналогичная странице добавления новой учетной записи.

Чтобы применить внесенные в учетную запись изменения, нажмите кнопку **Сохранить**.

Удаление учетных записей PPP

Для удаления учетной записи PPP выделите её, активировав флажок возле названия учетной записи в списке учетных записей. При необходимости можно выделить несколько учетных записей, активировав соответствующие флажки. Дополнительные возможности выделения:

- Щелчок по ссылке **Выделить все** выделяет все учетные записи в списке,
- Щелчок по ссылке **Инвертировать выделение** инвертирует выделение, делая не выбранные элементы списка выбранными, и наоборот.

Для удаления выбранных учетных записей необходимо нажать кнопку **Удалить выбранные учетные записи PPP**.

Удаление учетных записей – необратимая операция. В случае если удаленная учетная запись PPP потребуется в дальнейшем, ее придется создать и настроить заново.

Активные соединения

На странице **Активные соединения** можно просмотреть текущие активные соединения PPP, если они имеются.

Просмотр активных соединений PPP

- Выберите в главном меню в разделе **Сеть** пункт **VPN**;
- Нажмите кнопку **Расширенные настройки**.

Для просмотра активных соединений протокола PPP перейдите по ссылке **Активные соединения**. При этом на экране откроется страница просмотра списка активных соединений.

Статистика

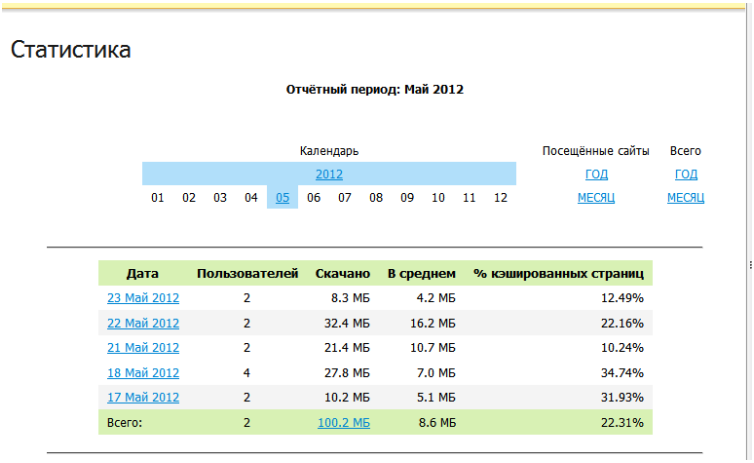
На этой странице можно просмотреть статистику обращения пользователей локальной сети к Интернет (по протоколам HTTP и FTP) через прокси-сервер **Dr.Web Office Shield**. Статистика извлекается из журналов регистрации прокси-сервера **Squid**. В статистике отражаются действия пользователей (количество загруженной и отправленной информации) в течение выбранного периода времени.

Обратите внимание на следующие особенности работы модуля статистики:

- FTP-трафик всех клиентов локальной сети в статистике учитывается и отображается только как суммарный трафик клиента с IP-адресом `127.0.0.1`.
- При отключении **Веб-прокси** (или его недоступности при истечении или отсутствии лицензионного ключа) сбор статистики обращений пользователей к Интернет не ведется.
- Если в локальной сети используется DHCP, то идентификация клиентов не гарантируется, поскольку один и тот же IP-адрес может в разные моменты времени принадлежать разным клиентам.

Для перехода к странице просмотра статистики использования Интернет следует перейти по ссылке **Статистика** в разделе **Сеть** главного меню веб-интерфейса **Dr.Web Office Shield**.

Вид страницы просмотра статистики приведен на рисунке ниже.


Статистика

Отчётный период: Май 2012

Календарь

2012

01 02 03 04 05 06 07 08 09 10 11 12

Посещённые сайты: ГОД, МЕСЯЦ

Всего: ГОД, МЕСЯЦ

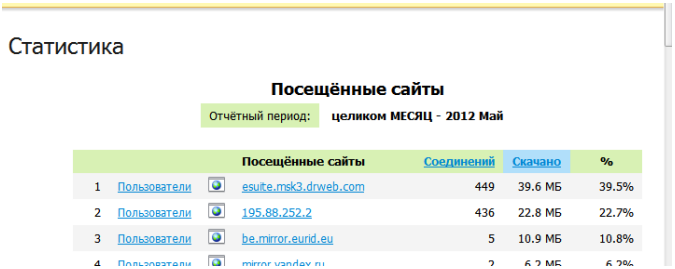
Дата	Пользователей	Скачано	В среднем	% кэшированных страниц
23 Май 2012	2	8.3 МБ	4.2 МБ	12.49%
22 Май 2012	2	32.4 МБ	16.2 МБ	22.16%
21 Май 2012	2	21.4 МБ	10.7 МБ	10.24%
18 Май 2012	4	27.8 МБ	7.0 МБ	34.74%
17 Май 2012	2	10.2 МБ	5.1 МБ	31.93%
Всего:	2	100.2 МБ	8.6 МБ	22.31%

Главное меню статистики состоит из следующих разделов:

- **Календарь** – позволяет выбрать год и месяц для просмотра статистики посещения сайтов.
- **Посещенные сайты** – отражение статистики посещения сайтов за выбранный в календаре период:
  - В статистических данных отображаются:
    - Имена пользователей;
    - Названия посещенных сайтов;
    - Количества подключений к сайтам;
    - Количество загруженных байтов;
    - Кэш-попадания.
  - Имеются следующие возможности управления:
    - Выбор периода просмотра статистики (за весь год или только за месяц, выбранные в календаре);
    - Сортировка статистики по соединениям или количеству загруженных байтов по убыванию. Для сортировки статистики нажмите на название соответствующего столбца.

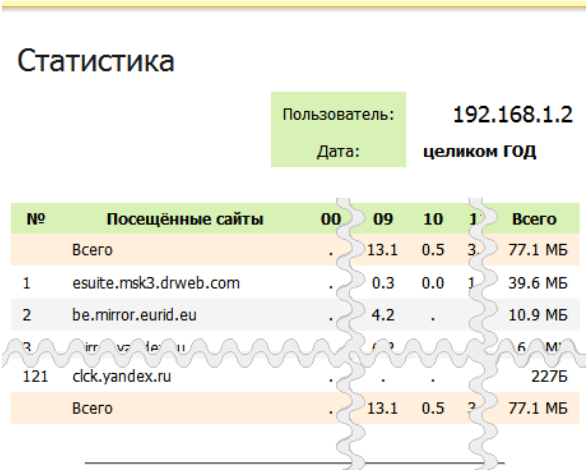
- Доступ к дополнительной статистике по некоторому пользователю. Для этого нажмите на имя пользователя.
- Переход на посещенный пользователем сайт. Для этого нажмите на адрес сайта.
- Занесение сайта в черный список. Для этого нажмите на иконку  рядом с адресом сайта.

Вид страницы просмотра статистики посещенных сайтов показан на рисунке ниже.



- **Всего** – отражение статистики активности пользователей за выбранный в календаре период:
  - В статистических данных отображаются:
    - Время соединения;
    - IP-адрес пользователя;
    - Количество соединений;
    - Количество загруженных байтов;
    - Среднее количество байтов.
  - Имеются следующие возможности управления:
    - Выбор периода просмотра статистики (за весь год или только за месяц, выбранные в календаре);
    - Доступ к дополнительной статистике по некоторому пользователю. Для этого нажмите на IP-адрес пользователя.

- Доступ к временному графику активности пользователя по посещению сайтов. Для этого нажмите на пиктограмму  рядом с IP-адресом пользователя. Во временном графике активности отображается активность пользователя по посещению различных сайтов (выраженная в количестве загруженных с сайта байт), разбитая по часам. Вид страницы временного графика активности пользователя (с сокращениями):

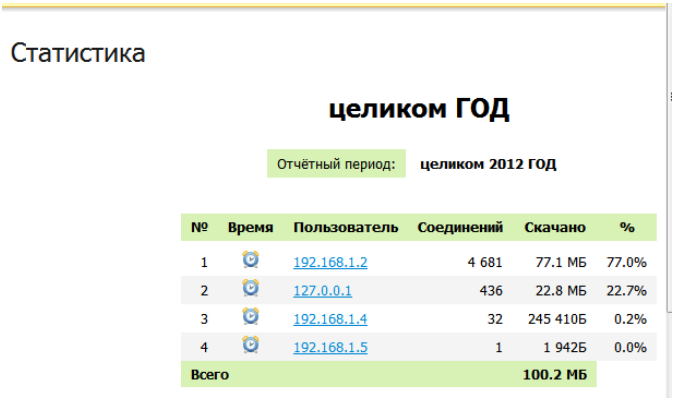


Статистика

Пользователь:	192.168.1.2
Дата:	целиком ГОД

№	Посещённые сайты	00	09	10	1	Всего
	Всего	.	13.1	0.5	3	77.1 МБ
1	esuite.msk3.drweb.com	.	0.3	0.0	1	39.6 МБ
2	be.mirror.eurid.eu	.	4.2	.		10.9 МБ
3	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	6 М
121	clck.yandex.ru	.	.	.		227Б
	Всего	.	13.1	0.5	3	77.1 МБ

Вид страницы просмотра статистики активности пользователей показан на рисунке ниже.


Статистика

целиком ГОД

Отчётный период: целиком 2012 ГОД

№	Время	Пользователь	Соединений	Скачано	%
1		192.168.1.2	4 681	77.1 МБ	77.0%
2		127.0.0.1	436	22.8 МБ	22.7%
3		192.168.1.4	32	245 410Б	0.2%
4		192.168.1.5	1	1 942Б	0.0%
Всего				100.2 МБ	

В статистических таблицах используются следующие пиктограммы:

- Просмотр временного (почасового) графика активности пользователя;
- Просмотр графика (гистограммы) объема закачанных с сайта байт;
- Блокирование сайта и занесение его в черный список (пользователям будет запрещено посещать данный сайт);

Управление безопасностью

Веб-интерфейс управления **Dr.Web Office Shield** позволяет настроить безопасность в локальной сети. Комплекс **Dr.Web Office Shield** обеспечивает следующие аспекты безопасности:

- экранирование сетей от атак снаружи (firewall);
- анализ веб-трафика и корпоративной почты на вирусы,
- управление комплексной антивирусной защитой рабочих станций локальной сети.

Доступ к управлению настройками безопасности локальной сети обеспечивают пункты главного меню, сгруппированные в разделе **Безопасность**.

Раздел **Безопасность** главного меню содержит следующие пункты:

- Почтовый прокси – доступ к настройке **Dr.Web Почтовый прокси**, обеспечивающему безопасность почтового трафика пользователей.
- Веб-прокси – доступ к настройке **Dr.Web Веб-прокси**, обеспечивающему безопасность веб-трафика.
- Защита рабочих станций – доступ к управлению **Антивирусной сетью Dr.Web** и работой **Dr.Web Enterprise Server**, обеспечивающему централизованную защиту рабочих станций локальной сети.
- Межсетевой экран (firewall) – доступ к настройке параметров сетевого экрана, обеспечивающего безопасность сетевых соединений и предотвращающего сетевые атаки извне.

Вкладки меню **Безопасность** могут быть отличны от представленных в данном руководстве.

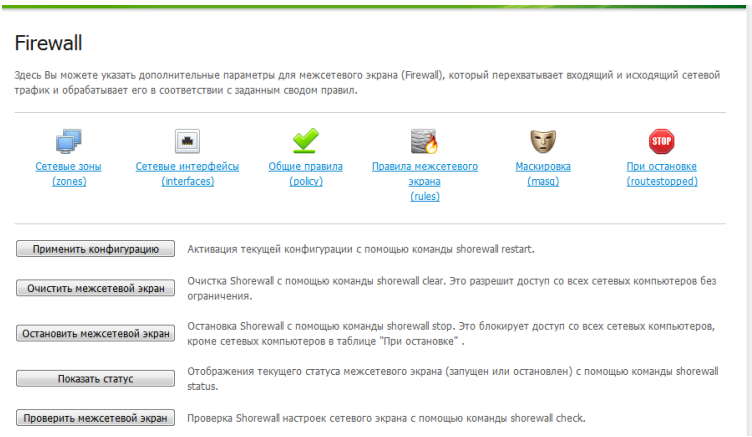
Настройки безопасности зависят от потребностей вашей компании и типа приобретенной лицензии, поэтому некоторые настройки могут отсутствовать.

Межсетевой экран (firewall)

Межсетевой экран (firewall) предназначен для перехватывания потоков входящего и исходящего сетевого трафика и обработки его в соответствии с заданными правилами (например, разрешение прохождения, запрет или изменение маршрута). Межсетевой экран позволяет скрыть компьютеры, расположенные в зоне LAN, от узлов, находящихся в зоне WAN, и предотвратить возможность сетевых атак на локальные компьютеры из внешних сетей.

Доступ к странице управления параметрами межсетевого экрана осуществляется выбором пункта главного меню **Безопасность** → **Firewall**. Вид страницы управления

параметрами межсетевого экрана приведен на рисунке ниже.



В качестве межсетевого экрана в **Dr.Web Office Shield** используется программное обеспечение **Shorewall**.

Настройки для межсетевого экрана

- Сетевые зоны (zones) – задание сетей, доступных с системы. Перечень сетевых зон не влияет на межсетевой экран, он только содержит названия зон и их описания.
- Сетевые интерфейсы (interfaces) – отображение и настройка параметров работы сетевых интерфейсов системы.
- Общие правила (policy) – настройка правил обработки трафика между различными зонами межсетевого экрана, применяемых экраном по умолчанию. Правила могут быть отменены для некоторых хостов или типов трафика на вкладке **Правила межсетевого экрана**.
- Правила межсетевого экрана (rules) – настройка исключений для правил по умолчанию для некоторых видов трафика, источников или назначений. Выбранное действие будет применяться к пакетам, удовлетворяющим заданным критериям.

- Маскировка (masq) – настройка трансляций IP-адресов для трафика между некоторой сетью и отдельным интерфейсом.
- При остановке (routestopped) – настройка перечня хостов или сетей, которые будут доступны при остановке межсетевого экрана (по умолчанию при остановке межсетевого экрана включается запрет доступа со всех хостов).

Управление межсетевым экраном

Межсетевой экран Shorewall запускается автоматически при включении **Dr.Web Office Shield**.

- Для активации текущей конфигурации межсетевого экрана нажмите кнопку **Применить конфигурацию**.
- Для очистки настроек межсетевого экрана (чтобы разрешить доступ со всех хостов без ограничения) нажмите кнопку **Очистить межсетевой экран**.
- Для остановки межсетевого экрана (чтобы заблокировать доступ со всех хостов, кроме хостов перечисленных в перечне **При остановке**) нажмите кнопку **Остановить межсетевой экран**.
- Для отображения текущего статуса межсетевого экрана (запущен или остановлен) нажмите кнопку **Показать статус**.
- Для проверки настроек межсетевого экрана нажмите кнопку **Проверить межсетевой экран**.

Настройка сетевых зон

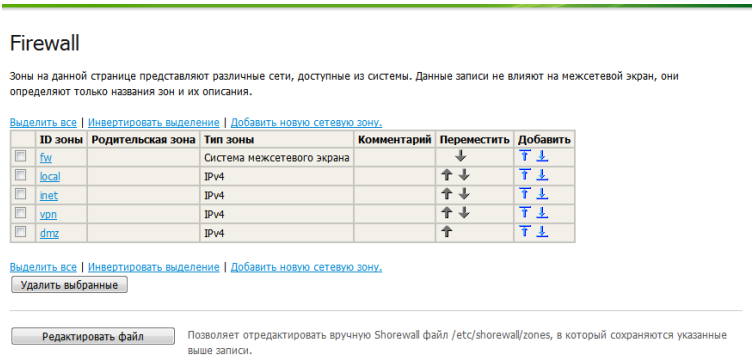
Сетевые зоны представляют различные сети, доступные с системы. Записи о сетевых зонах не влияют на работу межсетевого экрана, а используются для определения названия зон и их описания.

Управление перечнем сетевых зон выполняется на странице настройки сетевых зон.

Настройка сетевых зон

- Перейдите по ссылке **Firewall** в разделе **Безопасность** главного меню,
- Нажмите ссылку **Сетевые зоны (zones)**.

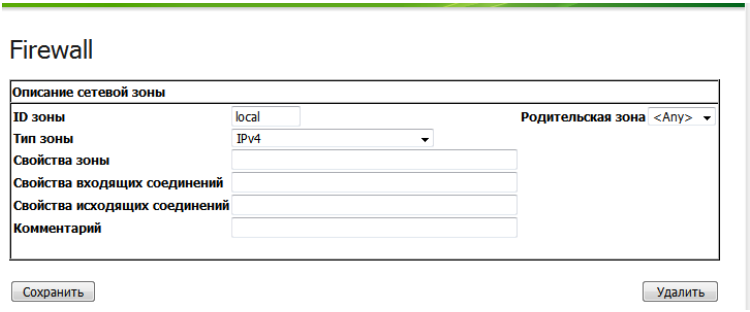
Вид страницы перечня сетевых зон приведен на рисунке ниже.



Добавление новой сетевой зоны

1. Нажмите ссылку **Добавить новую сетевую зону**. На экране откроется страница добавления новой сетевой зоны.
2. Задайте следующие параметры сетевой зоны:
   - Введите идентификатор зоны в поле **ID зоны**;
   - Выберите **Тип зоны** (IPv4, IPsec или Система межсетевого экрана) из выпадающего списка;
   - Укажите **родительскую зону** для данной зоны (из уже имеющихся). Если данная зона не имеет родительской, выберите в списке пункт `<Any>`.
   - Остальные параметры являются необязательными и могут быть оставлены без изменения.
3. Нажмите кнопку **Сохранить**.

Вид страницы добавления новой сетевой зоны показан на рисунке ниже.



Примечания:

1. Стандартно (но не обязательно) для обозначения разных зон сети применяются следующие идентификаторы:

ID	Описание зоны
`lan, local`	Локальная сеть (LAN)
`inet, internet, wan`	Интернет, глобальная (внешняя) сеть WAN
`dmz`	Демилитаризованная зона
`vpn`	Виртуальная частная сеть (VPN)
`fw`	Система межсетевого экрана

2. Используются следующие типы зон:

Тип зоны	Описание
`IPv4`	Обычная IP-сеть, использующая транспортный протокол и адресацию IP (версия 4). Используется для любой зоны по умолчанию
`IPsec`	IP-сеть, использующая шифрование (secured). Обычно используется для зоны VPN
`Система межсетевого экрана`	Только зона межсетевого экрана. Обычно имеется только одна зона данного типа

3. Для корректной работы **Dr.Web Office Shield** необходимо наличие не меньше трех зон (для LAN, WAN и межсетевого экрана). По умолчанию в **Dr.Web Office Shield** настроены зоны LAN, WAN, DMZ, VPN и межсетевого экрана, как показано на рисунке "Вид страницы перечня сетевых зон".

Управление списком сетевых зон

При помощи пиктограмм, размещенных в списке сетевых зон, можно управлять порядком следования зон в списке:

 Перемещение сетевой зоны на одну позицию в списке наверх

 Перемещение сетевой зоны на одну позицию в списке вниз

 Добавление в список новой сетевой зоны на позицию выше текущей

 Добавление в список новой сетевой зоны на позицию ниже текущей

Редактирование сетевых зон

Для редактирования сетевой зоны нажмите на идентификатор сетевой зоны в списке, после чего на экране откроется страница редактирования параметров сетевой зоны, аналогичная странице добавления новой сетевой зоны.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**. Чтобы удалить зону, нажмите кнопку **Удалить**.

Удаление сетевых зон

Для удаления сетевой зоны выделите ее в списке, активировав флажок в строке списка возле идентификатора зоны. При необходимости можно выделить несколько сетевых зон, активировав соответствующие флажки. Дополнительные возможности выделения:

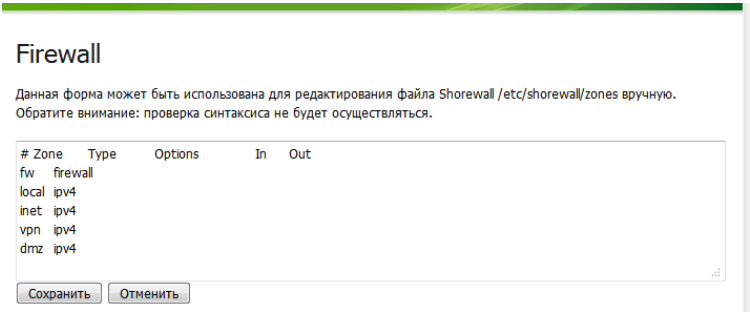
- Щелчок по ссылке **Выделить все** выделяет все сетевые зоны в списке,
- Щелчок по ссылке **Инвертировать выделение** инвертирует выделение, делая не выбранные элементы списка выбранными, и наоборот.

Для удаления выбранных сетевых зон необходимо нажать кнопку **Удалить выбранное**.

Удаление сетевых зон – необратимая операция. В случае если удаленная сетевая зона потребуется в дальнейшем, ее придется создать и настроить заново.

Ручная правка файла сетевых зон Shorewall

Имеется возможность отредактировать файл Shorewall, хранящий список сетевых зон. Для редактирования вручную файла Shorewall, расположенного в `/etc/shorewall/`, нажмите **Редактировать файл вручную**. После этого на экране откроется страница редактирования содержимого файла, показанная на рисунке ниже.



Введите перечень зон в текстовое поле в формате, используемом Shorewall (одна строка – одна зона, поля разделяются пробелом или табуляцией).

Нажатие кнопки **Сохранить** сохраняет внесенные изменения в файл зон, а нажатие кнопки **Отменить** позволяет отказаться от внесения изменений в файл.

Обратите внимание, что при редактировании файла зон Shorewall вручную не производится проверка синтаксиса и корректности введенного текста. Неправильное заполнение файла может привести к сбросу списка зон Shorewall.

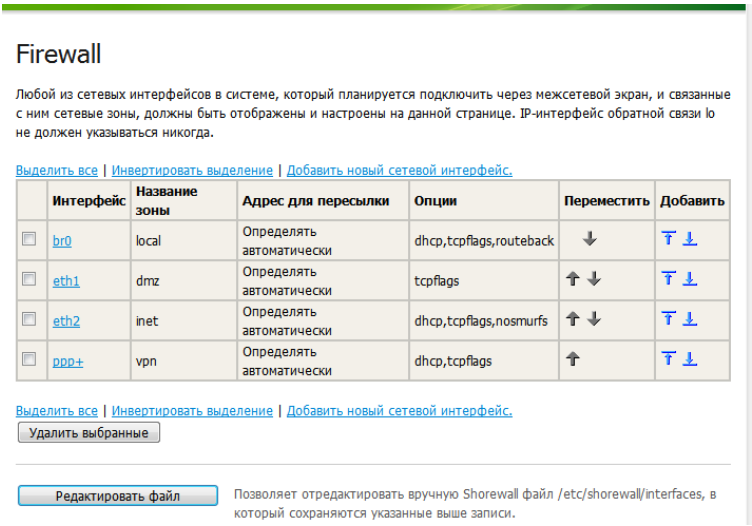
Настройка сетевых интерфейсов

На этой странице отображается список сетевых интерфейсов, имеющихся в комплексе **Dr.Web Office Shield**, и их назначение сетевым зонам. Трафик всех интерфейсов, перечисленных в в списке, будет обрабатываться межсетевым экраном Shorewall с использованием правил по умолчанию или дополнительных правил маршрутизации.

Настройка сетевых интерфейсов

- Перейдите по ссылке **Firewall** в разделе **Безопасность** главного меню,
- Нажмите ссылку **Сетевые интерфейсы (interfaces)**.

Вид страницы перечня сетевых интерфейсов приведен на рисунке ниже.



Конфигурация интерфейсов по умолчанию

По умолчанию в **Dr.Web Office Shield** выполнена следующая настройка сетевых интерфейсов и привязка к сетевым зонам:

Интерфейс	Назначение	Параметры
`eth0`	Подключение локальной сети (LAN) *Напрямую не используется*	–
`eth1`	Подключение демилитаризованной зоны (DMZ)	Зона: **dmz** (DMZ) Адрес: Определять автоматически Прочие параметры: `tcpflags`
`eth2`	Подключение зоны глобальной сети (Интернета, WAN)	Зона: **inet** (WAN) Адрес: Определять автоматически Прочие параметры: `dhcp`, `tcpflags`, `nosmurfs`
`wlan0`	Подключение сети Wi-Fi *Напрямую не используется*	–
`ppp+`	Подключение PPP (для организации VPN)	Зона: **vpn** (VPN) Адрес: Определять автоматически Прочие параметры: `dhcp`, `tcpflags`
`br0`	Мост, объединяющий интерфейсы локальной сети `eth0` и сети Wi-Fi `wlan0`	Зона: **local** (LAN + Wi-Fi) Адрес: Определять автоматически Прочие параметры: `dhcp`, `tcpflags`, `routeback`

Добавление нового сетевого интерфейса

1. Нажмите ссылку **Добавить новый сетевой интерфейс**. На экране откроется страница добавления нового сетевого интерфейса.
2. Задайте следующие параметры интерфейса:
   - Введите идентификатор интерфейса в поле **Интерфейс**;
   - Укажите **Название зоны**, связанной с этим интерфейсом, из выпадающего списка;
   - Укажите **Адрес для пересылки** (рекомендуется оставить вариант **Определять автоматически**).
   - Укажите, при необходимости, дополнительные параметры сетевого интерфейса, включив соответствующие флажки:

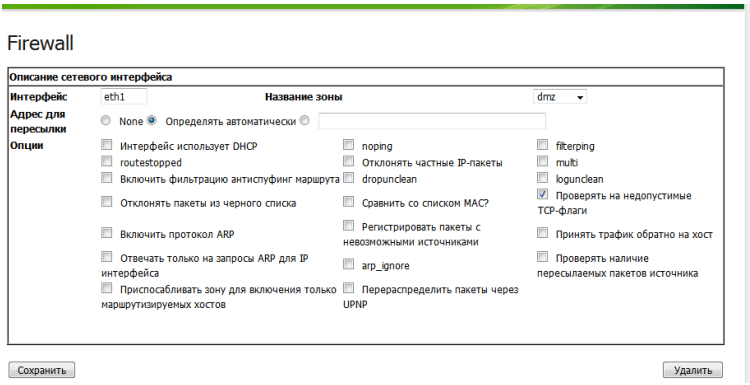
Параметр	Описание
Интерфейс использует DHCP	Этот интерфейс используется DHCP (в сетевой зоне, связанной с этим интерфейсом, используется DHCP)
Игнорировать ICMP-запросы	Интерфейс не будет отвечать на ICMP-запросы (ping)
Проверять ICMP-запросы	Поступающие ICMP-запросы будут проверяться, и обрабатываться будут только корректные
Использовать, когда Shorewall отключен	Интерфейс (и его подсеть) будет доступен при остановке межсетевого экрана
Отклонять частные IP-пакеты	Интерфейс будет отклонять частные IP-пакеты
Разрешить multicast	Будет разрешено использование этого интерфейса для работы в режиме multicast
Включить фильтрацию антиспуфинг маршрута	Разрешить для интерфейса фильтрацию пакетов с целью предотвращения спуфинг-атак (подмена IP-адреса отправителя в IP-пакетах). Пакеты с подмененными IP-адресом отправителя будут отбрасываться

Параметр	Описание
Не обрабатывать некорректные пакеты	Поступающие некорректные пакеты будут отбрасываться
Регистрировать некорректные пакеты	Поступающие некорректные пакеты будут регистрироваться в журнале
Проверять на недопустимые TCP-флаги	Будут отбрасываться пакеты с неправильным сочетанием флагов протокола TCP
Включить протокол ARP	Включить прием и обработку интерфейсом ARP-запросов (важно, если интерфейс обеспечивает работу PPP с Proxy ARP).
Регистрировать пакеты с невозможными источниками	Записывать в журнал появление IP-пакетов с невозможным адресом отправителя
Принять трафик обратно на хост	Обязать принимать весь трафик, являющийся ответным на запросы, прошедшие через этот интерфейс, на этот же интерфейс
Отвечать только на запросы ARP для IP интерфейса	Отвечать на запросы ARP, только если они об IP-адресах, находящихся в сетевой зоне, подключенной к этому интерфейсу
Принимать ARP-запросы только от локальных адресов	Принимать запросы ARP только если они исходят из сетевой зоны, подключенной к этому интерфейсу
Проверять наличие пересылаемых пакетов источника	Отклонять пакеты с широковещательным адресом отправителя
Приспосабливать зону для включения	Автоматическое изменение состава сетевой зоны таким образом, чтобы в нее входили только хосты,

Параметр	Описание
только маршрутизируемых хостов	маршрутизируемые через этот интерфейс
Перераспределить пакеты через UPNP	Использовать UPNP для распределения пакетов

3. Нажмите кнопку **Сохранить**.

Вид страницы добавления нового сетевого интерфейса показан на рисунке ниже.



Управление списком сетевых интерфейсов

При помощи пиктограмм, размещенных в списке сетевых интерфейсов, можно управлять порядком их следования в списке:

- Перемещение сетевого интерфейса на одну позицию в списке наверх
- Перемещение сетевого интерфейса на одну позицию в списке вниз
- Добавление в список нового сетевого интерфейса на позицию выше текущего
- Добавление в список нового сетевого интерфейса на позицию ниже текущего

Редактирование сетевых интерфейсов

Для редактирования сетевого интерфейса нажмите на его название в списке, после чего на экране откроется страница редактирования параметров сетевого интерфейса, аналогичная странице добавления нового сетевого интерфейса.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**. Чтобы удалить интерфейс, нажмите кнопку **Удалить**.

Удаление сетевых интерфейсов

Для удаления сетевого интерфейса выделите его в списке, активировав флажок в строке списка возле названия интерфейса. При необходимости можно выделить несколько сетевых интерфейсов, активировав соответствующие флажки. Дополнительные возможности выделения:

- Щелчок по ссылке **Выделить все** выделяет все сетевые интерфейсы в списке,
- Щелчок по ссылке **Инвертировать выделение** инвертирует выделение, делая не выбранные элементы списка выбранными, и наоборот.

Для удаления выбранных сетевых интерфейсов необходимо нажать кнопку **Удалить выбранное**.

Удаление сетевых интерфейсов – необратимая операция. В случае если удаленный интерфейс потребуется в дальнейшем, его придется создать и настроить заново.

Ручная правка файла сетевых интерфейсов Shorewall

Имеется возможность отредактировать файл Shorewall, хранящий список сетевых интерфейсов. Для редактирования вручную файла Shorewall, расположенного в `/etc/shorewall/`, нажмите **Редактировать файл вручную**. После этого на экране откроется страница редактирования содержимого файла. Введите перечень интерфейсов в текстовое поле в формате, используемом Shorewall (одна строка – один интерфейс, поля разделяются пробелом или табуляцией).

Нажатие кнопки **Сохранить** сохраняет внесенные изменения в файл интерфейсов, а нажатие кнопки **Отменить** позволяет отказаться от внесения изменений в файл.

Обратите внимание, что при редактировании файла интерфейсов Shorewall вручную не производится проверка синтаксиса и корректности введенного текста. Неправильное заполнение файла может привести к сбросу списка интерфейсов Shorewall.

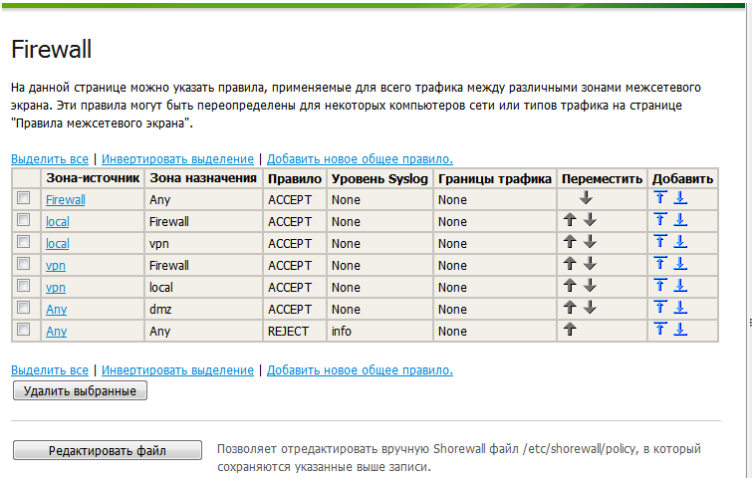
Задание общих правил

Имеется возможность настроить действия (общие правила), которые межсетевой экран будет использовать по умолчанию для трафика между различными зонами межсетевого экрана. Для некоторых хостов или типов трафика общие правила могут быть заменены на специфические правила маршрутизации на странице Правила межсетевого экрана.

Настройка правил по умолчанию

- Перейдите по ссылке **Firewall** в разделе **Безопасность** главного меню,
- Нажмите ссылку **Общие правила (policy)**.

Вид страницы перечня общих правил приведен на рисунке ниже.



На странице просмотра перечня общих правил для каждого правила выводятся следующие сведения:

- **Зона-источник** – Из какой зоны следует трафик.
- **Зона назначения** – В какую зону следует трафик.
- **Правило** – Действие, применяемое к трафику данного направления.
- **Уровень Syslog** – Уровень важности, используемый при записи о срабатывании данного правила в системный журнал.
- **Границы трафика** – Границы разрешенной интенсивности трафика по данному маршруту.

При помощи пиктограмм, размещенных в списке, можно управлять порядком следования правил в списке:

Перемещение правила на одну позицию в списке наверх

Перемещение правила на одну позицию в списке вниз

Добавление в список нового правила на позицию выше

текущего

Добавление в список нового правила на позицию ниже текущего

Список правил просматривается межсетевым экраном сверху вниз до первого подходящего правила. Поэтому наиболее общие правила (типа Any → Any) должны находиться ниже специфических правил.

По умолчанию в межсетевом экране **Dr.Web Office Shield** настроены следующие общие правила:

- Разрешается трафик из зоны firewall во все сетевые зоны.
- Разрешается трафик из зоны LAN в зоны firewall и VPN.
- Разрешается трафик из зоны VPN в зоны LAN и firewall.
- Разрешается трафик из любой зоны в зону DMZ.
- Трафик из любой зоны в любую, не попавший под ранее перечисленные правила, отклоняется, о чем делается запись в системном журнале.

Добавление нового общего правила

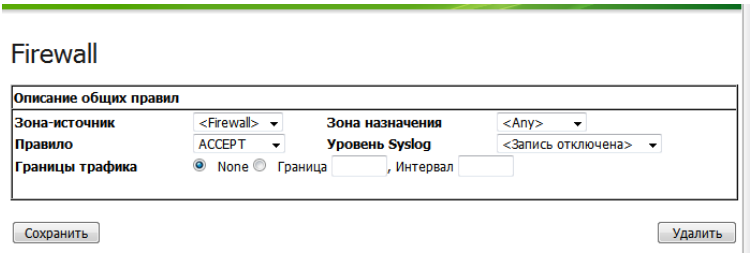
1. Нажмите ссылку **Добавить новое общее правило**. На экране откроется страница добавления нового правила.
2. Задайте следующие параметры правила:
   - Выберите зону–источник трафика из выпадающего списка **Зона-источник** и зону назначения трафика из выпадающего списка **Зона назначения** (<Firewall> означает зону межсетевого экрана, а <Any> – любую зону).
   - Укажите **Правило**, применяемое к трафику этого маршрута. Доступен следующий перечень действий:

Параметр	Описание
ACCEPT	Пропустить трафик по маршруту
REJECT	Отклонить пакеты
DROP	Удалить пакеты
CONTINUE	Не принимать никакого решения, продолжить просматривать список правил

- Укажите, требуется ли вносить в системный журнал запись о срабатывании правила, выбрав из списка **Уровень Syslog** уровень важности события (выбор пункта <Запись отключена> отключает фиксацию срабатывания правила в журнале).
- Укажите, следует ли учитывать интенсивность трафика по маршруту, выбрав соответствующий переключатель в поле границы трафика. При выборе None интенсивность трафика не учитывается, в противном случае необходимо указать границу и интервал интенсивности для срабатывания правила.

3. Нажмите кнопку **Сохранить**.

Вид страницы добавления нового сетевого интерфейса показан на рисунке ниже.



Редактирование общих правил

Для редактирования общего правила нажмите на его зону-источник в списке, после чего на экране откроется страница редактирования правила, аналогичная странице добавления нового правила.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**. Чтобы удалить общее правило, нажмите кнопку **Удалить**.

Удаление общих правил

Для удаления общего правила выделите его в списке, активировав флажок в строке списка возле его зоны-источника. При необходимости можно выделить несколько правил, активировав соответствующие флажки. Дополнительные возможности выделения:

- Щелчок по ссылке **Выделить все** выделяет все правила в списке,
- Щелчок по ссылке **Инвертировать выделение** инвертирует выделение, делая не выбранные элементы списка выбранными, и наоборот.

Для удаления выбранных правил необходимо нажать кнопку **Удалить выбранное**.

Удаление общих правил – необратимая операция. В случае если удаленное правило потребуется в дальнейшем, его придется создать и настроить заново.

Ручная правка файла общих правил Shorewall

Имеется возможность отредактировать файл Shorewall, хранящий список общих правил. Для редактирования вручную файла Shorewall, расположенного в `/etc/shorewall/`, нажмите **Редактировать файл вручную**. После этого на экране откроется страница редактирования содержимого файла. Введите список правил в текстовое поле в формате, используемом Shorewall (одна строка – одно правило, поля разделяются пробелом или табуляцией).

Нажатие кнопки **Сохранить** сохраняет внесенные изменения в файл общих правил, а нажатие кнопки **Отменить** позволяет отказаться от внесения изменений в файл.

Обратите внимание, что при редактировании файла общих правил Shorewall вручную не производится проверка синтаксиса и корректности введенного текста. Неправильное заполнение файла может привести к сбросу списка общих правил Shorewall.

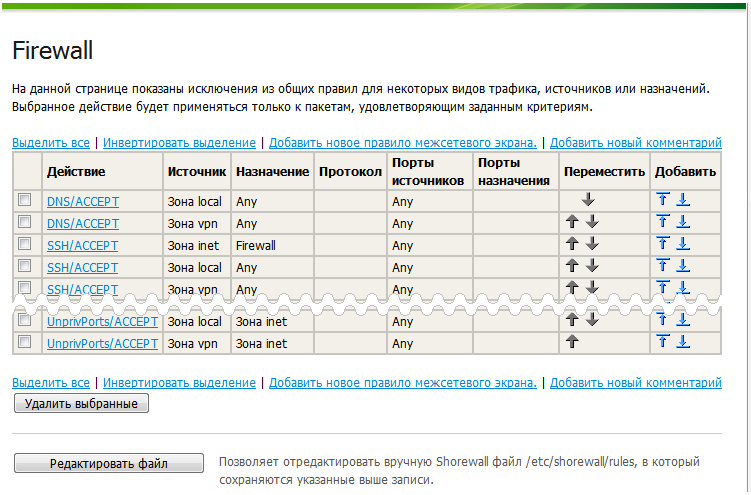
Задание правил межсетевого экрана

Имеется возможность настроить правила, которые межсетевой экран Shorewall будет применять в конкретных случаях вместо общих правил.

Настройка правил межсетевого экрана

- Перейдите по ссылке **Firewall** в разделе **Безопасность** главного меню,
- Нажмите ссылку **Правила межсетевого экрана (rules)**.

Вид страницы перечня правил межсетевого экрана (фрагмент) приведен на рисунке ниже.



На странице просмотра перечня исключающих правил межсетевого экрана для каждого правила выводятся следующие сведения:

- **Действие** – Действие, которое будет выполнено при срабатывании правила (вида <тип трафика>/<действие>).
- **Источник** – Зона, из которой следует трафик.
- **Назначение** – Зона, в которую следует трафик.
- **Протокол** – Используемый протокол (TCP, UDP, ICMP). Если протокол не указан, то он не учитывается в правиле.
- **Порты источников** – Номера портов, с которых должен исходить трафик (если не указаны, то в правиле не анализируется и не учитывается).

- **Порты назначения** – Номера портов, на которые должен идти трафик (если не указаны, то в правиле не анализируется и не учитывается).

При помощи пиктограмм, размещенных в списке, можно управлять порядком следования правил в списке:

- Перемещение правила на одну позицию в списке наверх
- Перемещение правила на одну позицию в списке вниз
- Добавление в список нового правила на позицию выше текущего
- Добавление в список нового правила на позицию ниже текущего

Список правил просматривается межсетевым экраном сверху вниз до первого подходящего правила. Поэтому наиболее общие правила (типа Any → Any) должны находиться в списке ниже специфических правил.

Рекомендуемый набор правил межсетевого экрана

Для обеспечения корректной работы комплекса **Dr.Web Office Shield** рекомендуется иметь следующий базовый набор правил:

Правило	Направления	Комментарий
DNS/ACCEPT	LAN → Any VPN → Any	Разрешение DNS-запросов из зон LAN и VPN в любую зону для корректной работы DNS и DHCP
SSH/ACCEPT	LAN → Any VPN → Any WAN → Firewall	Разрешить прохождение трафика SSH (удаленной консоли безопасного доступа). Минимально требуется разрешение доступа только к зоне Firewall (подключение к консоли ОС **Dr.Web Office Shield**)

Правило	Направления	Комментарий
		Обратите внимание, что прохождения трафика SSH рекомендуется оставить разрешенным, поскольку это может пригодиться для удаленного доступа к устройству в случае возникновения проблем.
Ping/ACCEPT	LAN → Any VPN → Any	Разрешение прохождения ICMP-запросов (требуется для определения доступности хостов по сети)
NTP/Accept	LAN → Any VPN → Any	Разрешение прохождения запросов к серверам времени (для синхронизации системного времени)
Auth/ACCEPT	LAN → Any VPN → Any Any → Firewall	Разрешение прохождения запросов авторизации
PPTP/ACCEPT	Any → Any	Разрешение пропуска PPTP (для организации VPN)
HTTP/ACCEPT	LAN → Any VPN → Any	Доступ к WWW-ресурсам Интернет по протоколу HTTP
SMTP/ACCEPT	LAN → Firewall VPN → Firewall WAN → Firewall	Доступ к серверам электронной почты по протоколу SMTP Обратите внимание, что данные правила запрещают сквозное прохождение SMTP через **Dr.Web Office Shield**, поскольку сообщения направляются на **Почтовый прокси Dr.Web**
HTTPS/ACCEPT	LAN → Any VPN → Any	Доступ к Интернет через защищенные соединения
SMTPS/ACCEPT	Any → Any	Разрешать пропуск электронной почты через защищенные соединения

Правило	Направления	Комментарий
SMB/ACCEPT	LAN → Firewall VPN → Firewall	Доступ к файловуму серверу **Dr.Web Office Shield**, хранящему документацию в электронном виде
REDIRECT **Порт 80 → 3128**	LAN → Any VPN → Any	Перенаправление запросов к WWW-ресурсам (протокол HTTP) на внутренний прокси-сервер **squid3** для проверки через **Веб-Прокси Dr.Web**
REDIRECT **Порт ftp → 2121** **ftpdata → 2121**	LAN → Any VPN → Any	Перенаправление запросов к FTP-ресурсам на внутренний прокси-сервер **frox** для проверки через **Веб-Прокси Dr.Web**

Перечисленные правила входят в заводские настройки устройства, удалять или изменять их без необходимости не рекомендуется. Например, удаление указанных здесь правил **REDIRECT** приведет к тому, что работа **Веб-прокси** будет заблокирована. Кроме того, данные правила автоматически модифицируются устройством при включении и отключении **Веб-прокси**.

Добавление нового правила межсетевого экрана

1. Нажмите ссылку **Добавить новое правило межсетевого экрана**. На экране откроется страница добавления нового правила.
2. Задайте следующие параметры правила:
   - Выберите **Действие**, которое необходимо выполнить межсетевому экрану. В качестве действия может быть выбрано непосредственное действие межсетевого экрана (такое, как ACCEPT, DNAT, DROP и т.п) которое нужно применить к трафику, или макродействие, которое определяет тип трафика (в перечне макродействий содержатся типы трафика основных прикладных протоколов, таких, как ICQ, SSH, FTP и т.п.)

- В случае если в списке **Действие** было выбрано макродействие, необходимо выбрать, какое действие необходимо совершить межсетевому экрану с трафиком данного вида. Совершаемое действие в этом случае выбирается из выпадающего списка **Параметр макродействия**.

  Межсетевой экран может выполнять следующие действия с трафиком:

Параметр	Описание
ACCEPT	Пропустить пакеты по маршруту (с возможным применением к ним нижележащих правил DNAT или REDIRECT)
ACCEPT+	Только пропустить пакеты по маршруту, не применяя к ним нижележащих правил DNAT или REDIRECT, если они заданы
CONTINUE	Перейти к поиску следующего правила
DNAT	Генерация для пакетов разрешающего правила ACCEPT, применение к ним процедуры DNAT (трансляции адресов/портов)
DNAT-	Применение к пакетам процедуры DNAT без использования разрешающего правила ACCEPT
DROP	Уничтожить пакеты без ответа
LOG	Вывести запись о транзакции в системный журнал и продолжить поиск правила
NONAT	Не применять правил DNAT или REDIRECT
QUEUE	Оставление пакетов в очереди для обработки дополнительными приложениями
REDIRECT	Генерация для пакетов разрешающего правила ACCEPT, перенаправление пакетов на указанные хост/порт (или локально на другой порт) для обработки
REDIRECT-	Аналогично REDIRECT, но без генерации разрешающего правила ACCEPT
REJECT	Отвергнуть пакеты и разорвать соединение
SAME	Аналогично DNAT, только не переопредляется порт

Параметр	Описание
SAME-	Аналогично DNAT-, только не переопредляется порт

- Укажите, требуется ли вносить в системный журнал запись о срабатывании правила, выбрав из списка **Уровень Syslog** уровень важности события (выбор пункта <Не записывать> отключает фиксацию срабатывания правила в журнале).
- Укажите зону-источник, из которой должен исходить трафик, чтобы к нему применялось это правило, выбрав ее из выпадающего списка **Зона источника**. Пункт списка <Any> указывает, что правило будет применено к трафику, поступающему из любой зоны. В случае отсутствия в списке необходимой зоны следует выбрать в списке пункт 'Другое...' и ввести название зоны (или ее сетевой адрес) в поле справа от списка.
- Аналогичным образом следует указать **Зону назначения или порт**. При необходимости указания порта следует выбрать в списке пункт "Другое..." и указать номер порта в поле справа.
- Для ограничения перечня компьютеров в зоне-источнике и/или зоне назначения, к которым применяется данное правило, следует установить соответствующий флажок **Только компьютеры в зоне с адресами** и перечислить в поле справа их IP-адреса через запятую или диапазоном.
- Выберите тип используемого протокола (TCP, UDP или ICMP) из выпадающего списка **Протокол**. Если тип протокола не важен, следует выбрать пункт списка <Any>.
- В полях **Порты источников** и **Порты назначения** указываются порты, с которых и на которые следует трафик. Если номера портов не должны учитываться, следует выбрать переключатели **Any**. В противном случае номера портов указываются через запятую или диапазонами (через дефис). Вместо номера порта может быть использовано имя сервиса, стандартно предоставляемое на данном порте (например, вместо номера 80 может быть указано название сервиса – www).

Обратите внимание на следующие особенности настройки правил:

1. Если в списке **Действие** было выбрано макродействие, определяющее некоторый стандартный прикладной протокол (ICQ, SSH и т. п.), то параметры **Протокол** и **Порты назначения** рекомендуется установить в значения Any, поскольку любой стандартный прикладной протокол определяет тип транспорта и порт назначения.
2. При использовании действия типа REDIRECT или DNAT следует обязательно указывать:
   - В поле **Порты назначения** – исходный порт, на который клиенты отправляют пакеты (например, порт www или 80 для HTTP).
   - В поле **Зона назначения или порт** зону и порт, на который будут перенаправлены пакеты.

- Если в качестве действия с трафиком выбраны переадресация REDIRECT или DNAT, требуется указать **Исходный адрес назначения для DNAT или REDIRECT.** В противном случае следует выбрать переключатель **None.**
- Если необходимо выполнить ограничение количества и интенсивности подключений данного маршрута, необходимо указать величину ограничения в поле ввода справа в поле **Представление ограничение скорости.** Ограничение интенсивности запросов задается выражением:

  ```
  rate/{sec|min}[:burst]
  ```

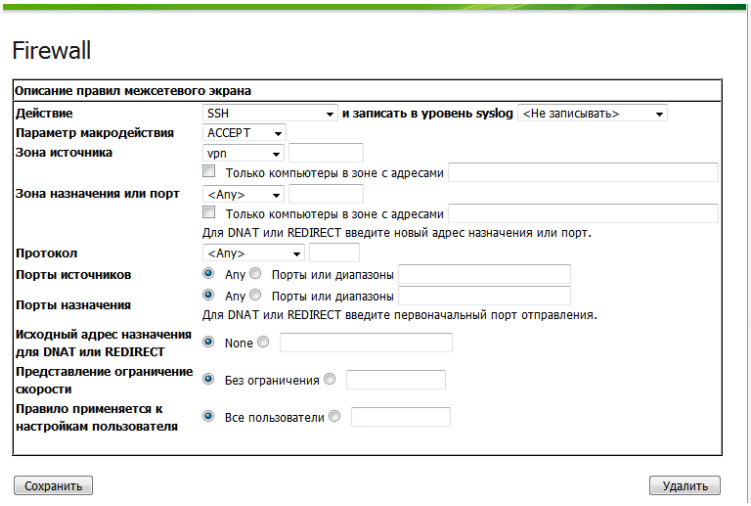
  где `rate` – допустимое количество соединений в интервал времени, `sec`, `min` - единицы измерения интервала времени, а `burst` - максимально допустимая (пиковая) частота запросов. Например, запись `10/sec:20` означает разрешение от 10 до 20 подключений в секунду.

  Если интенсивность подключений ограничивать не надо, выберите переключатель **Без ограничения.**

- В поле **Правило применяется к настройкам пользователя** всегда должен быть включен переключатель **Все пользователи**.

3. Нажмите кнопку **Сохранить.**

Вид страницы добавления нового правила межсетевого экрана показан на рисунке ниже.



Редактирование правил межсетевого экрана

Для редактирования правила нажмите на его действие в списке, после чего на экране откроется страница редактирования правила, аналогичная странице добавления нового правила.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**. Чтобы удалить правило межсетевого экрана, нажмите кнопку **Удалить**.

Удаление правил межсетевого экрана

Для удаления правила межсетевого экрана выделите его в списке, активировав флажок в строке списка. При необходимости можно выделить несколько правил, активировав соответствующие флажки. Дополнительные возможности выделения:

- Щелчок по ссылке **Выделить все** выделяет все правила в списке,
- Щелчок по ссылке **Инвертировать выделение** инвертирует выделение, делая не выбранные элементы списка выбранными, и наоборот.

Для удаления выбранных правил необходимо нажать кнопку **Удалить выбранное**.

Удаление правил межсетевого экрана – необратимая операция. В случае если удаленное правило потребуется в дальнейшем, его придется создать и настроить заново.

Ручная правка файла правил межсетевого экрана Shorewall

Имеется возможность отредактировать файл Shorewall, хранящий список правил межсетевого экрана. Для редактирования вручную файла Shorewall, расположенного в `/etc/shorewall/`, нажмите **Редактировать файл вручную**. После этого на экране откроется страница редактирования содержимого файла. Введите список правил в текстовое поле в формате, используемом Shorewall (одна строка – одно правило, поля разделяются пробелом или табуляцией).

Нажатие кнопки **Сохранить** сохраняет внесенные изменения в файл правил межсетевого экрана, а нажатие кнопки **Отменить** позволяет отказаться от внесения изменений в файл.

Обратите внимание, что при редактировании файла правил межсетевого экрана Shorewall вручную не производится проверка синтаксиса и корректности введенного текста. Неправильное заполнение файла может привести к сбросу списка правил межсетевого экрана Shorewall.

Управление маскировкой

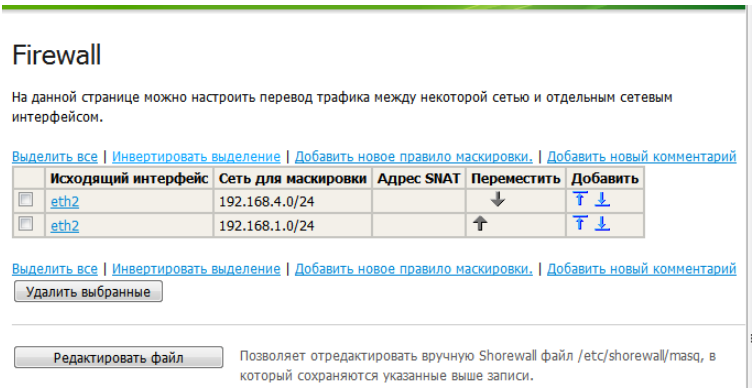
На этой странице можно настроить правила маскировки (маскарадинга), т.е. трансляцию сетевых адресов, при которой

в пакетах, проходящих через интерфейс, адрес отправителя подставляется динамически, в зависимости от назначенного интерфейсу адреса.

Управление маскировкой

- Перейдите по ссылке **Firewall** в разделе **Безопасность** главного меню,
- Нажмите ссылку **Маскировка (masq)**.

Вид страницы правил маскировки приведен на рисунке ниже.



На странице просмотра перечня правил маскировки для каждого правила выводятся следующие сведения:

- **Исходящий интерфейс** – На какой интерфейс (и в какую сеть через него) следует трафик.
- **Сеть для маскировки** – Сетевой адрес (в формате CIDR) или имя зоны сети, описывающие перечень маскируемых адресов.
- **Адрес SNAT** – Используемый адрес для SNAT (если пусто – не используется).

При помощи пиктограмм, размещенных в списке, можно управлять порядком следования правил в списке:

Перемещение правила маскировки на одну позицию в

списке наверх

- Перемещение правила маскировки на одну позицию в списке вниз
- Добавление в список нового правила маскировки на позицию выше текущего
- Добавление в список нового правила маскировки на позицию ниже текущего

Щелчок по ссылке **Добавить новый комментарий** позволяет добавить в список правил маскировки строку комментария.

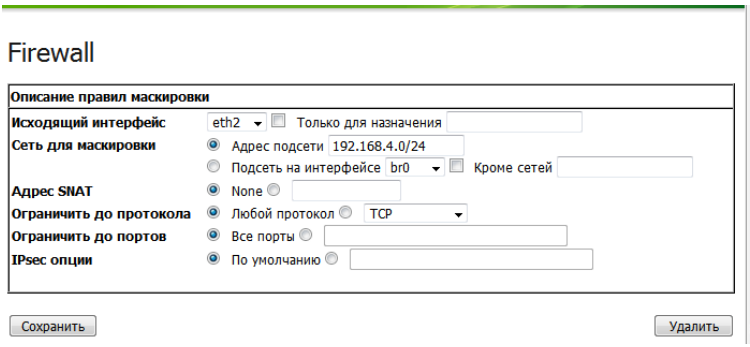
Добавление нового правила маскировки

1. Нажмите ссылку **Добавить новое правило маскировки**. На экране откроется страница добавления нового правила маскировки.
2. Задайте следующие параметры правила маскировки:
   - Выберите **Исходящий интерфейс** из выпадающего списка.
   - Если требуется подвергать маскировке не все пакеты, следующие через указанный исходящий интерфейс, а только те, которые отправляются на известный перечень хостов, то следует включить флажок **Только для назначения** и указать в поле справа от него IP-адреса хостов, при направлении к которым IP-пакеты будут подвергаться маскировке. IP-адреса перечисляются через запятую.
   - В поле **Сеть для маскировки** укажите способ определения IP-адресов, подлежащих маскировке. В случае выбора переключателя **Адрес подсети** следует указать сетевой адрес в формате CIDR, описывающий диапазон IP-адресов, маскировка которых требуется. В случае если выбрать переключатель **Подсеть на интерфейсе**, маскировка будет выполняться для пакетов, следующих из всех сетевых зон, закрепленных за этим интерфейсом. Для этого из выпадающего списка следует выбрать название сетевого интерфейса. При необходимости можно исключить из этого списка сетевые диапазоны, включив флажок **Кроме сетей**, и задав (через запятую) адреса сетей, пакеты из которых маскироваться не будут.

- В поле **Адрес SNAT** укажите режим использования SNAT. Если SNAT не используется, установите переключатель в **None**. В противном случае выберите переключатель справа и в поле ввода укажите адрес, используемый для SNAT на данном интерфейсе.
- Определите, для каких протоколов будет применяться маскировка, выбрав соответствующую опцию в поле **Ограничить до протокола**. Если преобразование должно выполняться для любого протокола, активируйте переключатель **Любой протокол**. В случае необходимости использовать преобразование только для конкретного протокола, следует включить переключатель сбоку от выпадающего списка и выбрать в списке протокол, для которого будет применяться преобразование адресов.
- Определите, для каких портов будет применяться маскировка, выбрав соответствующую опцию в поле **Ограничить до портов**. Если преобразование должно выполняться для любого порта, активируйте переключатель **Все порты**. В случае необходимости использовать преобразование только для конкретного набора портов, следует включить переключатель сбоку от поля ввода и ввести в поле перечень портов (через запятую), для которого будет применяться преобразование адресов.
- Если используется защищенный транспорт IPsec, а поле **Ipsec опции** определяются параметры, которые будут использованы при маскировке. Рекомендуется оставить включенным переключатель **По умолчанию**. При необходимости задания особых опций следует включить переключатель сбоку от поля ввода и ввести в поле требуемые опции. Опции вводятся в виде пар '`опция=значение`', разделенных запятой.

3. Нажмите кнопку **Сохранить**.

Вид страницы добавления нового сетевого интерфейса показан на рисунке ниже.



Редактирование правил маскировки

Для редактирования правила маскировки нажмите на его исходящий интерфейс в списке, после чего на экране откроется страница редактирования правила маскировки, аналогичная странице добавления нового правила маскировки.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**. Чтобы удалить правило маскировки, нажмите кнопку **Удалить**.

Удаление правил маскировки

Для удаления правила маскировки выделите его в списке, активировав флажок в строке списка возле его исходящего интерфейса. При необходимости можно выделить несколько правил, активировав соответствующие флажки. Дополнительные возможности выделения:

- Щелчок по ссылке **Выделить все** выделяет все правила маскировки в списке,
- Щелчок по ссылке **Инвертировать выделение** инвертирует выделение, делая не выбранные элементы списка выбранными, и наоборот.

Для удаления выбранных правил необходимо нажать кнопку **Удалить выбранное**.

Удаление правил маскировки – необратимая операция. В случае если удаленное правило маскировки потребуется в дальнейшем, его придется создать и настроить заново.

Ручная правка файла правил маскировки Shorewall

Имеется возможность отредактировать файл Shorewall, хранящий список правил маскировки. Для редактирования вручную файла Shorewall, расположенного в `/etc/shorewall/`, нажмите **Редактировать файл вручную**. После этого на экране откроется страница редактирования содержимого файла. Введите список правил маскировки в текстовое поле в формате, используемом Shorewall (одна строка – одно правило, поля разделяются пробелом или табуляцией).

Нажатие кнопки **Сохранить** сохраняет внесенные изменения в файл правил маскировки, а нажатие кнопки **Отменить** позволяет отказаться от внесения изменений в файл.

Обратите внимание, что при редактировании файла правил маскировки Shorewall вручную не производится проверка синтаксиса и корректности введенного текста. Неправильное заполнение файла может привести к сбросу списка правил маскировки Shorewall.

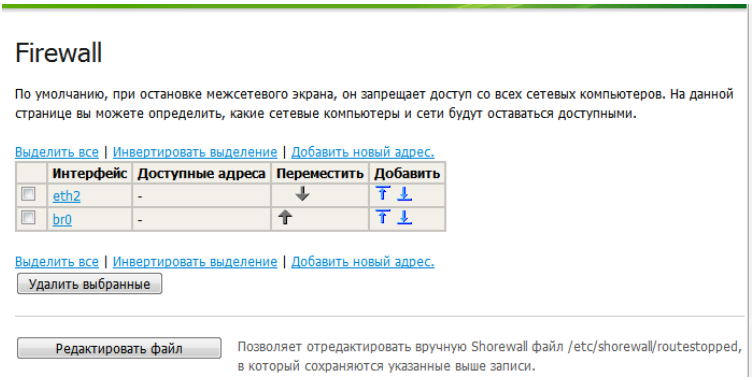
Настройка доступа при остановке firewall

На этой странице можно настроить правила, разрешающие прохождение трафика через сетевые интерфейсы **Dr.Web Office Shield** в том случае, когда межсетевой экран будет остановлен. По умолчанию при остановке межсетевого экрана всякое прохождение трафика между разными сетями через экран запрещается. Чтобы не парализовать работу сети, рекомендуется добавить правила, регламентирующие доступность интерфейсов при остановке межсетевого экрана.

Управление доступом при остановке межсетевого экрана

- Перейдите по ссылке **Firewall** в разделе **Безопасность** главного меню,
- Нажмите ссылку **При остановке (routestopped)**.

Вид страницы правил доступа при остановке межсетевого экрана приведен на рисунке ниже.



На странице просмотра перечня для каждого правила выводятся следующие сведения:

- **Интерфейс** – Для какого интерфейса разрешается доступ.
- **Доступные адреса** – Перечень адресов, обращение к которым разрешено. Если не указано, то обращение разрешено ко всем адресам.

При помощи пиктограмм, размещенных в списке, можно управлять порядком следования правил в списке:

- Перемещение правила доступа на одну позицию в списке наверх
- Перемещение правила доступа на одну позицию в списке вниз
- Добавление в список нового правила доступа на позицию выше текущего

 Добавление в список нового правила доступа на позицию ниже текущего

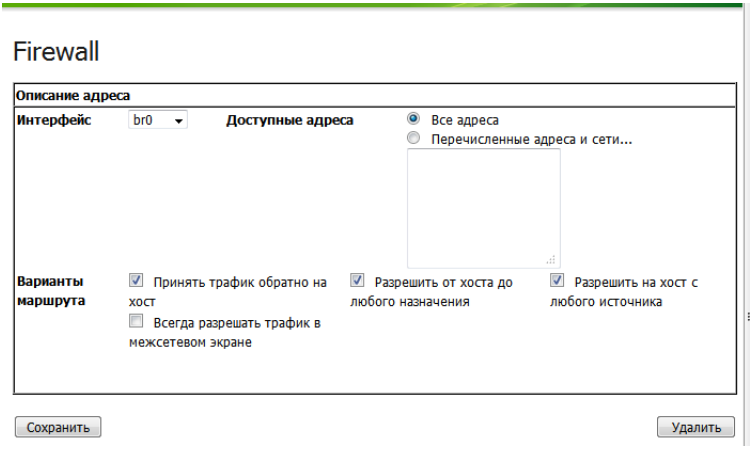
Добавление нового правила доступа

1. Нажмите ссылку **Добавить новый адрес**. На экране откроется страница добавления нового правила доступа.
2. Задайте следующие параметры правила доступа:
   - Выберите из выпадающего списка **Интерфейс**, для которого создается разрешающее правило.
   - Укажите перечень разрешенных для доступа IP-адресов и/или сетей. Выбор переключателя **Все адреса** разрешает доступ к любому адресу, а переключателя **Перечисленные адреса и сети...** – только к тем адресам, которые перечислены в списке ниже. Разрешенные адреса в списке перечисляются через запятую, сети указываются в формате CIDR.
   - При помощи дополнительных опций в разделе **Варианты маршрута** укажите параметры разрешения на доступ. Имеется возможность задать следующие опции:

Параметр	Описание
Принять трафик обратно на хост	Ответ на исходящие запросы к удаленному хосту должен возвращаться через этот же интерфейс
Разрешить от хоста до любого назначения	Разрешить внешний исходящий трафик через этот интерфейс
Разрешить на хост с любого источника	Разрешить внешний входящий трафик на этот интерфейс
Всегда разрешать трафик в межсетевом экране	Всегда разрешать трафик, направленный в зону firewall

3. Нажмите кнопку **Сохранить**.

Вид страницы добавления нового правила доступа показан на рисунке ниже.



Редактирование правил доступа

Для редактирования правила доступа нажмите на его интерфейс в списке, после чего на экране откроется страница редактирования правила доступа, аналогичная странице добавления нового правила доступа.

Чтобы применить внесенные изменения, нажмите кнопку **Сохранить**. Чтобы удалить правило доступа, нажмите кнопку **Удалить**.

Удаление правил доступа

Для удаления правила маскировки выделите его в списке, активировав флажок в строке списка возле его интерфейса. При необходимости можно выделить несколько правил, активировав соответствующие флажки. Дополнительные возможности выделения:

- Щелчок по ссылке **Выделить все** выделяет все правила доступа в списке,
- Щелчок по ссылке **Инвертировать выделение** инвертирует выделение, делая не выбранные элементы списка выбранными, и наоборот.

Для удаления выбранных правил необходимо нажать кнопку **Удалить выбранное**.

Удаление правил доступа – необратимая операция. В случае если удаленное правило доступа потребуется в дальнейшем, его придется создать и настроить заново.

Ручная правка файла правил доступа Shorewall

Имеется возможность отредактировать файл Shorewall, хранящий список правил доступа. Для редактирования вручную файла Shorewall, расположенного в `/etc/shorewall/`, нажмите **Редактировать файл вручную**. После этого на экране откроется страница редактирования содержимого файла. Введите список правил доступа в текстовое поле в формате, используемом Shorewall (одна строка – одно правило, поля разделяются пробелом или табуляцией).

Нажатие кнопки **Сохранить** сохраняет внесенные изменения в файл правил доступа, а нажатие кнопки **Отменить** позволяет отказаться от внесения изменений в файл.

Обратите внимание, что при редактировании файла правил доступа Shorewall вручную не производится проверка синтаксиса и корректности введенного текста. Неправильное заполнение файла может привести к сбросу списка правил доступа Shorewall.

Почтовый прокси Dr.Web

Dr.Web Почтовый прокси, входящий в состав **Dr.Web Office Shield**, предназначен для проверки сообщений электронной почты, поступающей на почтовый сервер организации. Сообщения электронной почты проверяются на наличие в них следующих угроз:

- Присутствие во вложениях (файлах, прикрепленных к письму) вирусов и другого вредоносного программного обеспечения, способного нести угрозы безопасности и сохранности информации;

- Присутствие признаков спама – навязчивой рассылки коммерческой, политической и иной рекламы или иной информации лицам, не выражавшим желания их получать.

Для того, чтобы **Dr.Web Почтовый прокси** мог проверять почту, необходимо наличие почтового сервера, обрабатывающего электронную почту организации (или только защищаемого домена). Почтовую систему необходимо настроить таким образом, чтобы вся почта, поступающая на почтовый сервер по протоколам SMTP/LMTP, предварительно поступала для проверки на **Dr.Web Почтовый прокси**. Письма, прошедшие проверку на вирусы и спам, пересылаются почтовым прокси на почтовый сервер для доставки получателям.

Обратите внимание, что сообщения, передаваемые по защищенному протоколу SMTPS (и вообще, весь трафик, следующий через защищенные соединения SSL/TLS) не проверяются.

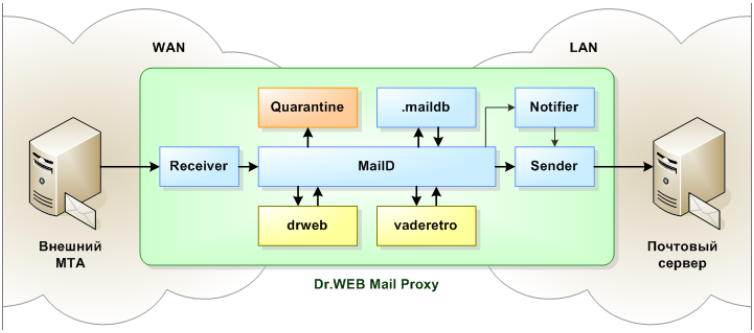
Структура Почтового прокси Dr.Web

Почтовый прокси состоит из следующих модулей:

Модуль	Назначение
Receiver	Принимает входящие сообщения электронной почты от почтовых серверов для проверки, используя протокол SMTP/LMTP
MailD	Модуль, управляющий проверкой сообщений, принятых модулем **Receiver**
Sender	Модуль, отправляющий исходящие сообщения электронной почты (сообщения, прошедшие проверку или уведомления о результатах обработки сообщений) на почтовые сервера, используя протокол SMTP/LMTP
Notifier	Модуль, формирующий уведомления об результатах обработки полученных сообщений, а также отчеты и передающий их на доставку модулю **Sender**
Quarantine	Специальный каталог, используемый для хранения подозрительных или инфицированных сообщений электронной почты
.maildb	База данных, хранящая полученные сообщения электронной почты в процессе их проверки

Модуль	Назначение
drweb	Модуль антивирусной проверки содержимого поступающих сообщений электронной почты
vaderetro	Модуль анализа поступающих сообщений электронной почты на спам

Структура почтового прокси, а также типовое включение его в сеть в составе **Dr.Web Office Shield** изображены на рисунке ниже.



В типовом варианте использования **Dr.Web Почтовый прокси** в составе **Dr.Web Office Shield** в качестве сервера-источника сообщений для проверки использует внешний почтовый релей (MTA), с которого принимается почта, следующая в защищаемый домен. Сообщения, прошедшие проверку, а также уведомления об обработке сообщений (и обнаруженных угрозах) и отчеты передаются для дальнейшей доставки почтовому серверу домена (как правило, он располагается в сетевой зоне LAN относительно **Dr.Web Office Shield**). Исходящая из домена почта по умолчанию не проверяется. Проходящие через **Почтовый прокси** сообщения проверяются с использованием всех модулей анализа.

Вирусные базы и правила распознавания спама, используемые модулями Антивируса **drweb** и Антиспама **vaderetro**, регулярно обновляются автоматически, что позволяет сохранять стабильно высокое качество фильтрации почтовых сообщений. Автоматическое обновление баз и правил выполняет встроенный модуль **drweb-updater** согласно расписанию, заданному в планировщике **cron** операционной

системы **Dr.Web Office Shield**.

В случае истечения срока действия ключа, разрешающего работу **Почтового прокси Dr.Web**, останавливается прохождение почты (SMTP-трафика) через устройство.

- Для продолжения работы **Почтового прокси Dr.Web** необходимо приобрести новый ключ.
- Для обработки почты без участия **Dr.Web Office Shield** необходимо изменить сетевые почтовые настройки домена.

Алгоритм обработки почтовых сообщений

1. Компонент **Receiver** принимает сообщение, поступившее от сервера-источника по протоколу SMTP/LMTP, и передает его для обработки модулю **MailD**.
2. **MailD** – основной компонент (ядро) системы обработки почты. Он производит сохранение писем в базе данных **.maildb**, MIME-разбор сообщений и передачу их на обработку подключаемым модулям анализа в соответствии с порядком проверки, заданным в настройках.
3. Результаты проверки сообщения отправляются либо компоненту **Receiver** (если существует такая возможность – например, еще не истекло время ожидания результата проверки), либо компоненту **Sender**.
4. В случае если письма не проходят проверку, они отправляются в каталог карантина (**Quarantine**), а сервер-получатель получает вместо них отчеты об обнаружении вируса (или иной угрозе). В противном случае письма передаются компоненту **Sender** для доставки серверу-получателю.
5. Компонент **Sender** отвечает за отправление писем на сервер-получатель по протоколу SMTP/LMTP.
6. Компонент **Notifier** формирует и отправляет отчеты о результатах обработки сообщений, получаемых в процессе работы комплекса. Запрос на отправку отчетов могут отправлять как модули анализа (например, при обнаружении вируса), так и другие компоненты системы. Например, компонент **MailD** может посылать запрос на создание общего отчета со статистикой работы всех подключенных

модулей анализа, а компонент **Sender** может посылать запрос на формирование отчета о невозможности отправить письмо. Отчеты могут рассылаться как отправителям и получателям писем, так и администратору системы.

Настройка почтового прокси для Dr.Web Office Shield

Доступ к настройке **Dr.Web Почтовый прокси** производится в разделе **Безопасность → Почтовый прокси** главного меню. На странице настроек почтового прокси доступно три вкладки:

- На вкладке Основные настройки можно включить или выключить основные виды защиты (от вирусов и спама), а также указать параметры подключения к почтовому серверу и имя защищаемого домена (или нескольких доменов, перечислив их через запятую).
- На вкладке Карантин имеется возможность просмотра списка писем, попавших в карантин. Имеется фильтр поиска писем в карантине по таким критериям, как:
  - Имя компонента, поместившего письмо в карантин.
  - Причина попадания письма в карантин.
  - Тема письма.
  - Отправитель или получатель письма.
  - Дата получения письма.
- На вкладке Расширенные настройки представлены дополнительные параметры, управляющие работой почтового прокси.

Сетевые настройки почтового прокси для Dr. Web Office Shield

Для корректной работы **Dr.Web Почтовый прокси** необходимо внести изменения в конфигурацию сети. Сетевые настройки, обеспечивающие корректную работу почты, рассматриваются в разделе Сетевые настройки почты.

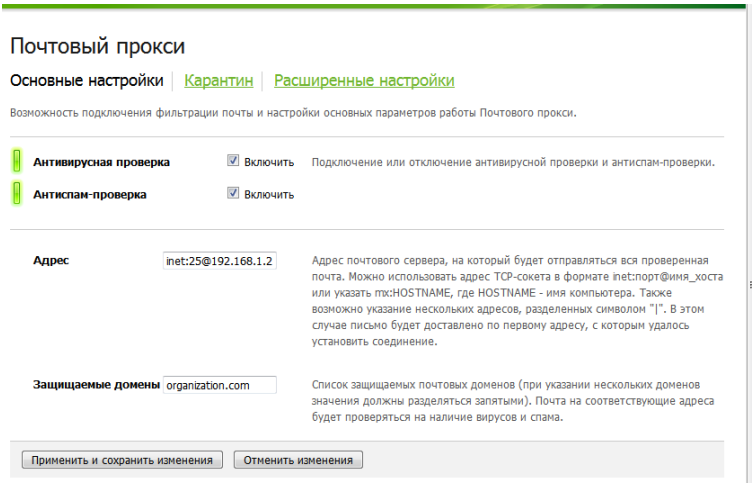
Основные настройки

На вкладке **Основные настройки** выполняется простейшая настройка работы **Почтового прокси**.

Для доступа к странице основных настроек необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния комплекса;
- На странице настроек **Почтового прокси** активировать вкладку **Основные настройки.**

Вид страницы основных настроек **Почтового прокси** показан на рисунке ниже.



Основные настройки

На странице основных настроек **Почтового прокси** доступны следующие настройки:

- Подключение и отключение компонентов **антивирусной проверки** и **антиспам-проверки.** Работа каждого из этих компонентов может быть включена или выключена по

отдельности активацией или деактивацией соответствующего флажка.

Не рекомендуется отключать компоненты **Антивируса** и **Антиспама**, т.к. в этом случае почтовый трафик и компьютеры получателей писем в локальной сети не будут защищены от вируса и спама.

Обратите внимание, что отключение компонентов антивирусной защиты не отключает сам **Почтовый прокси Dr.Web**, поскольку он используется в качестве почтового сервера домена с точки зрения внешних почтовых серверов. В этом случае письма, получаемые **Почтовым прокси**, передаются им почтовому серверу домена без проверки.

Если вам требуется выключить использование **Почтового прокси** в качестве почтового сервера домена, см. раздел Сетевые настройки почты.

- **Адрес** для отправки сообщений. В этом поле указывается адрес почтового сервера, на который отправляются проверенные прокси сообщения, а также уведомления о статусе обработки сообщений. Адрес почтового сервера может быть задан в следующих форматах:

Формат	Описание
inet:<port>@<host>	Указывается адрес сокета приема со стороны почтового сервера, где: • **<port>** – прослушиваемый почтовым сервером порт (обычно – 25, стандартный порт для протокола SMTP) • **<host>** – хост, на котором расположен почтовый сервер. Может быть указан IP-адрес или имя хоста. Например: `inet:25@192.168.12.3`, `inet:25@mail.company.com`
mx:имя_хоста	MX-запись почтового сервера Например: `mx:mail.company.com`

Возможно указание адресов нескольких серверов, разделенных символом "|", тогда письмо будет доставлено первому серверу в списке, с которым удалось установить

соединение.

- Список **защищаемых доменов**. В этом поле указываются (через запятую) названия доменов. **Почтовый прокси** будет проверять только письма, направляемые в указанные домены. Письма, направляемые в другие домены, будут пропускаться без проверки. По умолчанию здесь рекомендуется указать название своего домена. В этом случае будут проверяться только письма, поступающие на почтовые ящики домена.

Для применения указанных изменений нажмите кнопку **Применить и сохранить изменения.** Если необходимо отменить внесенные изменения и вернуть предыдущие сохраненные настройки, нажмите кнопку **Отменить изменения.**

Обратите внимание, что для правильной работы **Почтового прокси** с почтовыми сообщениями домена обязательно следует указать не только перечень **Защищаемых доменов**, но и перечень **Защищаемых сетей** (он задается на странице настроек Ядра). При этом перечень **Защищаемых сетей** должен содержать все IP-адреса всех почтовых серверов, через которые будет идти почтовый трафик внутри **Защищаемых доменов**.

Карантин

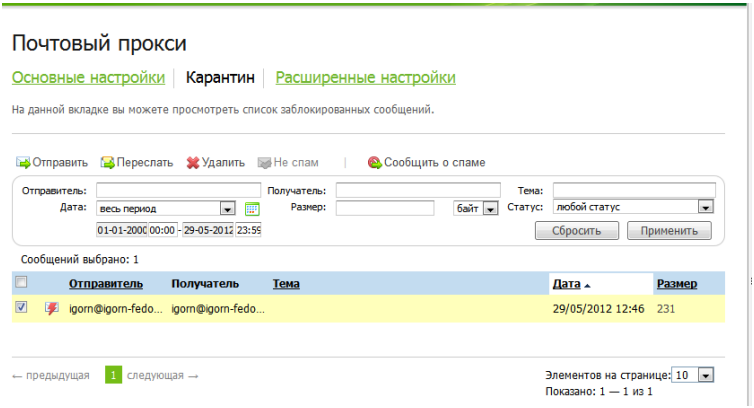
Карантин – это специальный каталог, содержащий письма, доставка которых получателю была заблокирована компонентами **Антивирус** (**drweb**) или **Антиспам** (**vaderetro**).

Для просмотра писем, помещенных **Почтовым прокси Dr.Web** в карантин, необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния комплекса;
- На странице настроек **Почтового прокси** активировать

вкладку **Карантин**.

Вид страницы просмотра карантина показан на рисунке ниже.



В верхней части страницы расположена панель инструментов, позволяющая выполнять некоторые действия с письмами, выделенными в списке писем. Под панелью инструментов располагается панель фильтрации, позволяющая определить, какие письма будут отображаться в списке.

Просмотр списка писем

В списке писем для каждого письма выводится:

- Статус письма в карантине (угроза, спам, соответствие запрещающему правилу, ошибка);
- Отправитель письма;
- Получатель письма;
- Тема сообщения;
- Дата приема сообщения;
- Размер сообщения в байтах.

Имеется возможность отсортировать письма в списке, нажав на название соответствующего столбца в заголовке списка. При этом сообщения будут отсортированы по возрастанию значений в столбце. Повторный щелчок по этому же столбцу сортирует письма в противоположном порядке. Текущий столбец, задающий порядок сортировки, отмечается стрелкой,

направление которой указывает направление сортировки.

Под списком писем в нижней части страницы можно указать, по скольку писем будет выводиться на одной странице списка, если под текущие критерии поиска подпадает большое количество писем. Для этого выберите соответствующее значение в выпадающем списке **Элементов на странице**. При наличии более чем одной страницы списка переключение между страницами списка осуществляется щелчком по номеру нужной страницы, или с использованием ссылок **предыдущая** и **следующая**, расположенными под списком.

Фильтрация списка писем

На панели фильтра, расположенной над списком писем, можно задавать критерии поиска писем. В этом случае в списке будут выведены только те письма, которые удовлетворяют всем критериям, заданным на панели фильтра. На панели фильтра можно задать следующие критерии:

- Отправитель – строка, которая должна содержаться в адресе отправителя письма;
- Получатель – строка, которая должна содержаться в адресе получателя письма;
- Тема – строка, которая должна содержаться в теме письма;
- Дата – диапазон дат, в который должна попасть дата получения письма. Даты можно указать непосредственно, заполнив соответствующие поля формы, или выбрав их из календаря. Также из выпадающего списка можно выбрать типовые диапазоны (текущий день, месяц, год);
- Размер – наименьший допустимый размер письма (в байтах, килобайтах или мегабайтах). Письма с размером меньше указанного в список не попадут.
- Статус – письма с каким статусом (угроза, спам, соответствие правилу, ошибка) должны быть выведены в списке. Пункт "любой статус" позволяет не учитывать статус письма.

Для применения условий фильтрации, заданных на панели, следует нажать кнопку **Применить**. Нажатие кнопки **Сброс** позволяет сбросить все критерии поиска.

Работа с письмами

С письмами, попавшими в карантин, можно совершить следующие действия:

- **Ознакомиться с содержимым письма** (просмотреть его) или только с его заголовками. Чтобы просмотреть письмо, следует щелкнуть мышью по любому полю письма (отправитель, получатель, тема, дата) в строке списка. Текст письма откроется на этой же странице на месте списка писем. Чтобы вернуться к списку писем, нажмите кнопку **Закрыть письмо**.
- **Отправить письмо получателю**. Если вы уверены, что письмо отправлено в карантин по ошибке, то можно отправить его получателю. Для этого нужно выделить его в списке, включив флажок в строке списка слева, и нажать кнопку **Отправить** на панели инструментов. При этом на экране появится окно предупреждения, в котором требуется подтвердить отправку получателю, или отказаться от нее. Можно отправить получателям несколько писем, предварительно выделив их в списке.
- **Переслать письмо по другому адресу в качестве вложения**. Чтобы отправить одно или более писем другому адресату в качестве вложений, следует выделить их в списке, включив соответствующие флажки, и нажать на панели инструментов кнопку **Переслать**. После этого на экране откроется окно, в котором необходимо ввести адрес получателя, тему и текст письма. Выделенные в списке письма будут прикреплены к этому письму как вложения. После заполнения полей письма следует нажать кнопку **Переслать**. Чтобы отказаться от пересылки, нажмите кнопку **Отмена**.
- **Удалить письмо из карантина**. Для удаления писем их следует выделить в списке, включив флажки, нажать на панели инструментов кнопку **Удалить**, и подтвердить удаление выбранных писем в появившемся окне. Обратите внимание, что операция удаления писем является необратимой, т.е. восстановить удаленное письмо невозможно.
- **Отметить письмо, как не спам**. Если письмо ошибочно попало в карантин как спам, то чтобы снять с него пометку "Спам" и доставки его получателю, выделите письмо (одно

или несколько) в списке, и нажмите на панели инструментов кнопку **Не спам**. Это действие применимо только к письмам со статусом "Спам".

Сообщение о спаме

Если вы получаете спам-сообщения, которые Антиспам-модуль **Почтового прокси Dr.Web** ошибочно пропускает, принимая за обычную корреспонденцию, то на данной странице вы можете послать сообщение о спаме. Для этого:

- Сохраните образец спам-письма в своей локальной почтовой программе, как файл (обычно это файл с расширением .eml).
- На странице карантина нажмите кнопку **Сообщить о спаме** на панели инструментов.
- В появившемся окне укажите путь к файлу письма, сохраненному на локальной машине, нажав кнопку **Обзор...**
- Для отправки письма с образцом спама на анализ нажмите кнопку **Сообщить о спаме**. Для отмены отправки нажмите кнопку **Отмена**.

Расширенные настройки

Разделы расширенных настроек

Расширенные настройки **Почтового прокси Dr.Web** предоставляют следующие разделы по управлению работой почтового прокси:

- Карантин – настройка работы карантина, в частности, времени хранения в нем писем.
- Ядро – настройка работы **MailD** – ядра **Почтового прокси Dr.Web**, в частности, задание защищаемых сетей и доменов и т.п.
- Отчеты – настройка отправки отчетов с результатами обработки сообщений.
- Прием почты – задание параметров получения сообщений и действия, применимые к входящей почте, настройки для SMTP.

- Отправка почты – задание параметров отправки и маршрутизации сообщений, определение действий для застрявших писем и т.п
- Антивирус – настройка компонента проверки писем на вирусы.
- Антиспам – настройка компонента проверки писем на наличие признаков спама.

Для доступа к расширенным настройкам **Почтового прокси Dr. Web** необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния комплекса;
- На странице настроек **Почтового прокси** активировать вкладку **Расширенные настройки.**

Переход к нужному разделу расширенных настроек осуществляется выбором нужной вкладки на странице **Расширенные настройки.**

Общие принципы редактирования расширенных настроек

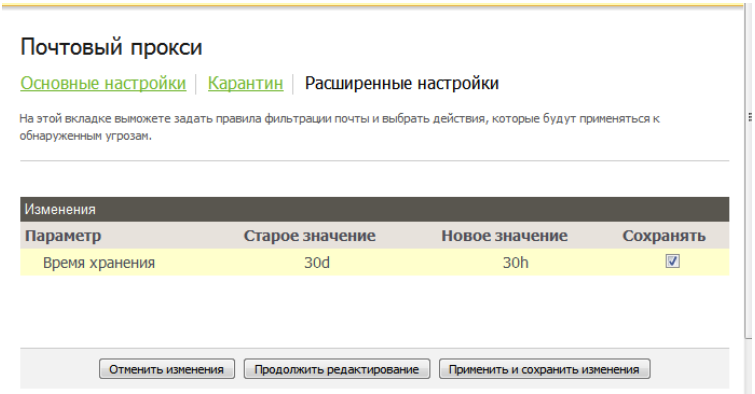
На каждой странице редактирования расширенных настроек все параметры выводятся в виде таблицы, причем одна строка таблицы соответствует ровно одному параметру. В правой части строки выводится краткое описание параметра и ссылка **подробнее.** При нажатии на эту ссылку краткое описание параметра разворачивается в более подробное.

При задании расширенных настроек значение каждого параметра либо выбирается из выпадающего списка, либо вводится в соответствующее поле ввода. Если параметр может иметь более одного значения, то перечень заданных значений выводится в виде списка. При задании и изменении значений параметров рядом с полями значений доступны пиктограммы, нажатие на которые выполняет действия, приведенные в таблице:

	Установка значения параметра по умолчанию
	Отмена изменения значения параметра и возврат к предыдущему значению
	Удаление значения из списка значений параметра (только если параметр может принимать более 1 значения)
	Добавление нового значения в список значений параметра (только если параметр может принимать более 1 значения)
	Перемещение значения в списке на более приоритетную позицию (только если параметр может принимать более 1 значения)
	Перемещение значения в списке на менее приоритетную позицию (только если параметр может принимать более 1 значения)

Просмотр и сохранение внесенных изменений

Для того чтобы просмотреть все внесенные в настройку изменения, нажмите кнопку **Предпросмотр** внизу страницы редактирования параметров. На появившейся странице вы можете выбрать те изменения, которые желаете сохранить, отметив соответствующую ячейку. Вид страницы просмотра внесенных изменений показан на рисунке ниже.



Если вы хотите внести дополнительные изменения, вы можете вернуться к предыдущей странице, нажав на кнопку

Продолжить редактирование. Если вы хотите отменить изменения, то нажмите кнопку **Отменить изменения.** Если сделанные изменения вас устраивают, нажмите на кнопку **Применить и сохранить изменения.**

Настройка карантина

Для доступа к настройкам карантина **Почтового прокси Dr. Web** необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния комплекса;
- На странице настроек **Почтового прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Карантин**.

Параметры работы карантина

На данной вкладке имеется возможность задания следующих параметров работы карантина:

Параметр	Описание
Время хранения	Задает время хранения сообщений, попавших в карантин. По истечению этого срока сообщения безвозвратно удаляются из карантина. Чтобы задать параметр, необходимо ввести в поле ввода числовое значение (целое неотрицательное число) и выбрать из выпадающего списка единицу измерения времени (часов, дней и т.п.).

Параметр	Описание
	При задании значения 0 сообщения будут храниться в карантине бесконечно долго. Данный режим не рекомендуется, поскольку это может привести к тому, что на файловой системе устройства **Dr.Web Office Shield** закончится место. Значение параметра по умолчанию: **24 часа**.
Максимальный размер сообщений	Максимальный суммарный размер сообщений (считается только размер тела сообщения, а не сообщение целиком, совместно с заголовками), которые могут храниться в карантине. При превышении данного объема забракованные в процессе проверки письма перестанут добавляться в карантин, а будут сразу безвозвратно удаляться. Чтобы задать параметр, необходимо ввести в поле ввода числовое значение (целое неотрицательное число) и выбрать из выпадающего списка единицу измерения объема (байты, килобайты, мегабайты). При задании значения 0 размер карантина ограничен только объемом свободного места на разделе файловой системы. Значение параметра по умолчанию: **0**.
Максимальное количество сообщений	Максимальное количество сообщений, которые могут храниться в карантине. При превышении данного количества забракованные в процессе проверки письма перестанут добавляться в карантин, а будут сразу безвозвратно удаляться. Чтобы задать параметр, необходимо ввести в поле ввода числовое значение (целое неотрицательное число). При задании значения 0 размер карантина ограничен только объемом свободного места на разделе файловой системы. Значение параметра по умолчанию: **0**.

Если задано несколько ограничений на хранение сообщений в карантине, то при работе с карантином все они применяются одновременно.

Настройка параметров ядра

Для доступа к настройкам параметров работы ядра **Почтового прокси Dr.Web** необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния комплекса;
- На странице настроек **Почтового прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Ядро**.

Основные параметры работы ядра

На данной вкладке имеется возможность задать следующие основные параметры работы ядра почтового прокси:

Параметр	Описание
Защищаемые сети	Задает список защищаемых сетей, не менее одной. Сетью считается непрерывный диапазон IP-адресов, задаваемый в формате CIDR (IP/MASK, например, `192.168.10.0/8`). **Почтовый прокси** будет принимать исходящие письма для отправки только в том случае, если они поступают с узлов, входящих в защищаемые сети. Чтобы добавить в список новую защищаемую сеть, укажите ее IP-диапазон в поле ввода, и нажмите пиктограмму  . Удаление сети из списка производится нажатием пиктограммы  в списке возле адреса сети.

Параметр	Описание
	Значение параметра по умолчанию: **127.0.0.0/8**
Защищаемые домены	Задает список защищаемых доменов, не менее одного. Управление списком защищаемых доменов производится аналогично списку защищаемых сетей. В качестве защищаемого домена может быть добавлено само название домена (например, `organization.com`) или регулярное выражение, которому должно соответствовать название защищаемого домена. Для добавления регулярного выражения необходимо в выпадающем списке **Префикс** выбрать значение "регулярное выражение", и указать в поле ввода выражение. Значение параметра по умолчанию: пустой список доменов
Включать поддомены	Определяет, следует ли считать защищаемыми не только домены, указанные в списке **Защищаемые домены**, но и любые их поддомены. Значение параметра выбирается из выпадающего списка. Если выбран пункт "Нет", то защищаемыми будут только домены, указанные в списке защищаемых доменов. Если выбран пункт "Да", то защищаемыми будут все поддомены любого домена, указанного в списке защищаемых доменов. Значение параметра по умолчанию: **Да**
Адрес перенаправления	Адрес почтового ящика, на который будут отправляться письма, для которых сработает действие "REDIRECT" (перенаправление другому получателю). В поле редактирования необходимо указать почтовый адрес в формате `user@domain`. Значение по умолчанию: **root@localhost**

Параметр	Описание
Лицензионные ограничения	Выбираются действия, которые следует совершить с письмом, в случае, если оно не было проверено вследствие лицензионных ограничений на работу антивирусного или антиспам-модуля. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Перечень доступных действий: • **пропустить** – пропустить письмо к получателю; • **отклонить без уведомления** – отклонить письмо без уведомления получателя; • **отклонить** – отклонить письмо и уведомить получателя; • **временная ошибка** – уведомить отправителя, что письмо временно не может быть доставлено. В качестве дополнительных действий можно выбрать следующее: • **карантин** – поместить письмо в карантин; • **перенаправить** – перенаправить письмо на другой адрес (требуется ввести в поле ввода адрес получателя). Можно указать несколько адресов, разделяя их символом '|'; • **информировать** – выслать отчет о найденных в письме угрозах (обработка письма не прекращается); • **добавить заголовок** – добавить к письму дополнительный заголовок. Заголовок задается в виде [ИМЯ:] ЗНАЧЕНИЕ, где: ○ ИМЯ – название заголовка (по умолчанию, если не указано, `X-DrWeb-MailD`), ○ ЗНАЧЕНИЕ – значение заголовка.

Параметр	Описание
	При использовании в заголовке символа ';', а также символов '(' и ')' их необходимо экранировать, поставив перед ними трижды символ обратного слэша '\' (например: `X-Additional-Header: LicenseRestricted\\\;`); • **добавить счет** – добавить к значению Счета сообщения* указанное значение. Добавляемое значение - это указанное целое число (может быть отрицательным). Основное действие выбирается из выпадающего списка **Основное действие**, а дополнительные действия добавляются в список **Дополнительные действия** нажатием на иконку  . Значение параметра по умолчанию: • Обязательное действие: **пропустить** • Дополнительные действия: нет
Ошибки обработки	Выбираются действия, которые следует совершить с письмом, в случае если возникли ошибки его обработки. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Перечень доступных действий аналогичен действиям, доступным в параметре **Лицензионные ограничения**. Значение параметра по умолчанию: • Обязательное действие: **временная ошибка** • Дополнительные действия: **информировать**
Максимальный счет	Пороговое значение Счета, которое может быть присвоено сообщению. Если Счет сообщения превысит величину, указанную в этом параметре, то для него выполнятся действия, заданные параметром **Превышение максимального счета**.

Параметр	Описание
	Для задания параметра необходимо ввести целое число из диапазона [-10000, 10000]. Чем больше величина Счета сообщения, тем более подозрительным считается сообщение (на наличие вирусов и/или спама). Значение параметра по умолчанию: **10000**
Превышение максимального счета	Выбираются действия, которые следует совершить с письмом, в случае если его Счет превышает значение **Максимального счета**. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Перечень доступных действий аналогичен действиям, доступным в параметре **Лицензионные ограничения**. Значение параметра по умолчанию: • Обязательное действие: **пропустить** • Дополнительные действия: нет

Обратите внимание, что для правильной работы **Почтового прокси** с почтовыми сообщениями домена обязательно следует указать не только перечень **Защищаемых доменов** (который задается, в том числе, и на странице основных настроек), но и перечень **Защищаемых сетей**. При этом перечень Защищаемых сетей должен содержать все IP-адреса всех почтовых серверов, через которые будет идти почтовый трафик внутри **Защищаемых доменов**.

Дополнительные параметры работы ядра

Для задания дополнительных настроек ядра следует щелкнуть по строке заголовка **Дополнительные**, расположенной в нижней части страницы, под секцией основных настроек. После этого на экране развернется секция настройки дополнительных настроек ядра. В этой секции можно задать следующие параметры работы ядра **Почтового прокси:**

Параметр	Описание
Использовать настраиваемые сообщения	Определяет, следует ли использовать перечень настраиваемых сообщений (их перечень дается в этом же разделе ниже) для формирования ответных сообщений отправителю сообщения при возникновении ошибок их приема или обработки. Значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Ответ на пустое From	Текст сообщения, высылаемого отправителю сообщения в ответ на попытку передать сообщение с пустым полем `From`: Текст вводится в текстовое поле. Текст, содержащий пробелы, должен быть заключён в кавычки. Значение параметра по умолчанию: пусто
Ответ на ошибки обработки	Текст сообщения, высылаемого при возникновении ошибки, если в качестве дополнительного действия было выбрано **информировать**. Текст вводится в текстовое поле. Текст, содержащий пробелы, должен быть заключён в кавычки. Значение параметра по умолчанию: пусто
Ответ на превышение максимального счета	Текст сообщения, высылаемого при возникновении превышения максимального Счета, если в качестве дополнительного действия было выбрано **информировать**. Текст вводится в текстовое поле. Текст, содержащий пробелы, должен быть заключён в кавычки. Значение параметра по умолчанию: пусто

Параметр	Описание
Максимальное число MIME-частей	Максимально допустимое число частей (MIME part) в сообщении. Если установлено в 0, число частей сообщения не ограничивается. В случае если число частей во входящем сообщении превысит указанное число, возникает ошибка обработки письма, и с ним будут выполнены действия, указанные в параметре **Ошибка обработки**. Значение параметра (целое неотрицательное число) вводится в текстовое поле. Значение параметра по умолчанию: **1000**
Максимальная вложенность MIME-частей	Максимально допустимая глубина вложенности частей (MIME part) в сообщении. Если установлено в 0, глубина вложенности частей сообщения не ограничивается. В случае если глубина вложенности частей во входящем сообщении превысит указанное число, возникает ошибка обработки письма, и с ним будут выполнены действия, указанные в параметре **Ошибка обработки**. Значение параметра (целое неотрицательное число) вводится в текстовое поле. Значение параметра по умолчанию: **100**

* Счет сообщения – это числовая оценка (целое число из диапазона [-10000, 10000]), присваиваемая сообщению, которая показывает степень его подозрительности. Чем Счет сообщения больше, тем оно подозрительнее с точки зрения системы проверки почты.

Управление отчетами

Для доступа к управлению отчетами **Почтового прокси Dr. Web** необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния

комплекса;

- На странице настроек **Почтового прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Отчеты**.

Основные параметры отчетов

На данной вкладке имеется возможность задать следующие основные параметры работы почтового прокси с отчетами:

Параметр	Описание
Отсылка отчетов	Параметр указывает, будут ли отсылаться отчеты о работе **Почтового прокси**. Имеются два значения "Да" и "Нет". Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Да**
Время отправки отчетов	Параметр задает периодичность отправки отчетов (если она включена). Имеются следующие возможные значения: Ежедневно, Еженедельно, Ежемесячно. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Ежедневно**
Адреса	Перечень адресов e-mail, на которые следует отправлять письма с отчетами (если отсылка отчетов включена). Если требуется отправлять отчеты на несколько адресов, они указываются через запятую. Если ни одного адреса на указано, отчеты будут отправляться на адрес, указанный в параметре **Адрес администратора**. Перечень адресов вводится в текстовое поле. Значение параметра по умолчанию: пусто

Параметр	Описание
Количество записей в списке часто блокируемых объектов	Количество объектов, включаемых в список наиболее часто блокируемых объектов и адресов, с которых присылается наибольшее количество блокируемых объектов. При значении 0 списки не создаются. При значении -1 размер списков не ограничен. Количество записей (целое число) вводится в текстовое поле. Значение параметра по умолчанию: **20**
Максимальное время хранения	Задает время хранения статистики обработки сообщений, используемой для формирования отчетов, в базе данных. Чтобы задать параметр, необходимо ввести в поле ввода числовое значение (целое неотрицательное число) и выбрать из выпадающего списка единицу измерения времени (секунд, минут, часов, дней). При задании значения 0 статистика будут храниться в базе данных бесконечно долго. Значение параметра по умолчанию: **31 день**.
Адрес администратора	Адрес e-mail, считающийся адресом администратора системы. Если не указаны адреса для доставки отчетов (в поле **Адреса**) то отчеты будут отправляться на этот адрес. При необходимости здесь можно указать несколько адресов через запятую. Адрес (или список адресов) вводится в текстовое поле. Значение параметра по умолчанию: **root@localhost**
Адрес фильтра	Адрес отправителя, который будет указан в поле From: сообщений со статистикой. Адрес вводится в текстовое поле. Значение параметра по умолчанию: **root@localhost**

Параметр	Описание
Языки отчетов	Список языков, на которых будут сформированы рассылаемые отчеты. Должно быть указано не менее одного языка. Перечень и количество языков, доступных для формирования отчетов, зависит от конфигурации **Почтового прокси**. Чтобы задать параметр, необходимо добавить в список языки, которые будут использованы для формирования отчетов. Значение параметра по умолчанию: **ru** (русский язык)

Дополнительные параметры отчетов

На данной вкладке имеется возможность задания следующих дополнительных параметров отчетов:

Параметр	Описание
Уровень подробности протоколирования обработчика правил	Уровень подробности ведения протокола обработчика правил. Чем выше уровень подробности, тем подробнее будут записи в протоколе обработчика правил. Могут быть использованы следующие уровни подробности протоколирования: • **quiet** – не выводить сообщений вообще ("тихий" уровень); • **error** – выводить только сообщения об ошибках; • **alert** – выводить сообщения об ошибках и предупреждения; • **info** – выводить сообщения об ошибках, предупреждения и информационные сообщения; • **debug** – выводить все сообщения (отладочный режим). Чтобы задать параметр, необходимо выбрать нужное значение из выпадающего списка. Значение параметра по умолчанию: **alert**

Настройка приема почты

Для доступа к управлению настройками приема почты **Почтовым прокси Dr.Web** необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния комплекса;
- На странице настроек **Почтового прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Прием почты**.

Основные параметры приема почты

На данной вкладке имеется возможность задания следующих основных параметров приема почты:

Параметр	Описание
Адрес	Список сокетов (не менее одного), используемых для приема входящих сообщений. Адрес сокета имеет вид `inet:<port>@<host>`, где: • **<port>** – прослушиваемый порт (обычно - 25, стандартный порт для протокола SMTP) • **<host>** – IP-адрес сетевого интерфейса. через который принимаются сообщения. Если интерфейс может быть любым, указывается 0.0.0.0. Для добавления сокета в список необходимо ввести адрес в поле редактирования и нажать пиктограмму  . Удаление сокета из списка производится нажатием на пиктограмму  возле сокета в списке. Значение параметра по умолчанию: **inet:25@0.0.0.0**

Параметр	Описание
Ошибки обработки	Выбирается действие, которое следует совершить с письмом, в случае если возникли ошибки его приема. Требуется указать основное действие. Перечень доступных действий: • **отклонить без уведомления** – отклонить письмо без уведомления получателя; • **отклонить** – отклонить письмо и уведомить получателя; • **временная ошибка** – уведомить отправителя, что письмо временно не может быть доставлено. Для задания параметра необходимо выбрать нужное действие из выпадающего списка. Значение параметра по умолчанию: **временная ошибка**

Параметры протокола SMTP

В разделе основных настроек приема почты имеется подраздел настройки параметров протокола SMTP, который по умолчанию свернут. При его разворачивании в этом подразделе имеется возможность задания следующих параметров:

Параметр	Описание
Защищаемые адреса	Список защищаемых адресов, который используется в **ограничении получателя** `reject_unknown_rcpts`. Позволяет отбрасывать неверных получателей и (при использовании фильтра `anti_dha` в **Reputation IP Filter**) эффективно бороться с DHA-атаками. В список могут быть добавлены как непосредственно защищаемые адреса (в формате user@domain), так и регулярные выражения, которые будут описывать группы защищаемых адресов.

Параметр	Описание
	Для добавления адреса или регулярного выражения в список необходимо ввести его в поле редактирования, выбрать тип из выпадающего списка (другое значение или регулярное выражение) и нажать пиктограмму  . Удаление адреса из списка производится нажатием на пиктограмму  возле адреса в списке. Значение параметра по умолчанию: пустой список Рекомендуется задавать этот параметр вместе с ограничением получателя `reject_unknown_rcpts` и использовать совместно с фильтром `anti_dha` (см. ниже)
Приветствие	Строка текстового приветствия, посылаемого компонентом **Receiver** **Почтового прокси** подключившемуся SMTP-клиенту при начале сессии. В строке могут использоваться следующие плейсхолдеры: • **%host%** – Значение **`Hostname`** из настроек **Dr.Web Office Shield**; • **%ver%** – версия компонента **Receiver**. Для задания параметра необходимо ввести текст приветствия в текстовое поле. Значение параметра по умолчанию: **%host% Dr.Web SMTP receiver v%ver% ready**
Максимальное количество получателей	Максимальное количество получателей (адресатов) для принимаемого письма. При превышении этого числа прием письма отвергается. Если этот параметр равен **0**, то ограничений на количество получателей нет. Если IP-адрес клиента, с которого было установлено данное соединение, отмечен как trusted, то данное ограничение не проверяется. В поле редактирования необходимо указать целое неотрицательное число.

Параметр	Описание
	Значение параметра по умолчанию: **100**
Максимальное количество подключений	Максимально разрешенное количество SMTP-подключений с одного IP-адреса. При превышении этого числа очередное подключение отвергается. Если этот параметр равен **0**, то ограничений на количество подключений нет. В поле редактирования необходимо указать целое неотрицательное число. Значение параметра по умолчанию: **20**
Максимальное количество сообщений на сессию	Максимально разрешенное количество сообщений, принимаемых от одного клиента за одну SMTP-сессию. При превышении этого числа очередное сообщение отвергается. Если этот параметр равен **0**, то ограничений на количество принимаемых сообщений за сессию нет. В поле редактирования необходимо указать целое неотрицательное число. Значение параметра по умолчанию: **20**
Максимальное количество заголовков Received	Максимально разрешенное количество заголовков Received в сообщениях, принимаемых от клиентов. При превышении этого числа сообщение отвергается. Если этот параметр равен **0**, то ограничений на количество заголовков Received нет. В поле редактирования необходимо указать целое неотрицательное число. Значение параметра по умолчанию: **100**
Максимальное количество ошибок на сессию	Максимально разрешенное количество ошибок в течение одной SMTP-сессий. При превышении этого числа сессия завершается. Если этот параметр равен **0**, то ограничений на количество ошибок за сессию нет.

Параметр	Описание
	Пожалуйста, обратите внимание, что если заданы другие ограничения (например, на **Максимальное количество получателей** не равно 0), то крайне нежелательно указывать для данного параметра значение 0. В поле редактирования необходимо указать целое неотрицательное число. Значение параметра по умолчанию: **10**
Максимальный размер сообщения	Максимально разрешенный размер сообщения, принимаемого от клиента. При превышении этого числа сообщение отвергается. Если этот параметр равен **0**, то ограничений на размер сообщений нет. В поле редактирования необходимо указать целое неотрицательное число, а в выпадающем списке выбрать единицы измерения параметра (байты, килобайты, мегабайты). Значение параметра по умолчанию: **10 МБ**
Почтовые домены	Список доменов, которым разрешена пересылка почты. При указании обычного списка доменов, для которых **Почтовый прокси** будет являться почтовым релеем, их поддомены не учитываются, т.е. почта, приходящая от их поддоменов, пересылаться не будет. Для задания поддоменов возможно использование регулярного выражения (например, regex:.*.domain.com - будет разрешена пересылка для всех поддоменов domain.com). Для добавления почтового домена или регулярного выражения в список необходимо ввести его в поле редактирования, выбрать тип из выпадающего списка (другое значение или регулярное выражение) и нажать пиктограмму  . Удаление домена из списка производится нажатием на пиктограмму  возле адреса в списке.

Параметр	Описание
	Значение параметра по умолчанию: пустой список
Ограничения сессии*	Список проверок, выполняемых непосредственно после установления соединения с клиентом. Возможно использование следующих проверок: • **trust_protected_network** – Если IP-адрес клиента находится в списке, определенном значением параметра **Защищаемые сети** (задается в параметрах Ядра), то адрес помечается как доверенный (trusted). • **mark_trust** – Пометить IP-адрес клиента как доверенный (trusted). Если есть еще ограничения после данного, то они будут пропущены. • **sleep** – Приостановить SMTP-соединение на заданное время (в секундах). Требуется указать время приостановки (целое число, не меньшее 1). • **tempfail** – Вернуть клиенту временную ошибку (с кодом 4*). • **reject** – Вернуть клиенту постоянную ошибку (с кодом 5*). • **reject_black_domains** – Проверка, находится ли IP-адрес клиента в **Черном списке доменов**, для чего производится PTR-запрос. При совпадении сессия закрывается. • **reject_black_networks** – Если IP-адрес клиента находится в **Черном списке сетей**, сессия закрывается. • **reject_dnsbl** – Проверка, находится ли IP-адрес клиента в черных списках серверов DNSBL, указанных в параметре **Серверы DNSBL**, для чего производится PTR-запрос. При совпадении сессия закрывается.

Параметр	Описание
	• **trust_white_domains** – Проверка, находится ли IP-адрес в **Белом списке доменов**, для чего производится PTR-запрос. При совпадении адрес помечается как доверенный. • **trust_white_networks** – Если IP-адрес клиента находится в **Белом списке сетей**, то адрес помечается как доверенный (trusted). • **trust_protected_domains** – проверка, находится ли IP-адрес клиента в списке, определенном значением параметра **Защищаемые домены** (задается в параметрах Ядра). Проверка осуществляется посредством двойного DNS-запроса. Сначала производится PTR-запрос и проверяется, находится ли полученное имя хоста в списке **Защищаемые домены**. Если этот домен есть в списке, производится A-запрос и проверяется, находится ли IP-адрес соединения в полученном списке адресов. При совпадении адрес клиента помечается как доверенный (trusted). Для добавления ограничения в список необходимо щелкнуть по его названию. Удаление ограничения из списка производится нажатием на пиктограмму возле ограничения в списке. Значение параметра по умолчанию: **trust_white_networks**
Ограничения HELO/EHLO	Список проверок, выполняемых на этапе идентификации клиента SMTP-сессии (HELO/EHLO). Возможно использование следующих проверок: • **mark_trust** – Пометить IP-адрес клиента как доверенный (trusted). Если есть еще ограничения после данного, то они будут пропущены.

Параметр	Описание
	• **sleep** – Приостановить SMTP-соединение на заданное время (в секундах). Требуется указать время приостановки (целое число, не меньшее 1). • **tempfail** – Вернуть клиенту временную ошибку (с кодом 4*). • **reject** – Вернуть клиенту постоянную ошибку (с кодом 5*). • **reject_unknown_hostname** – Если имя хоста клиента не имеет ни DNS-записи "A", ни DNS-записи "MX", то прием сообщений от клиента блокируется. • **reject_diff_ip** – Если IP-адрес клиента не совпадает ни с одним из IP-адресов, определенных для указанного в EHLO/HELO доменного имени, то прием сообщений от клиента блокируется Для добавления ограничения в список необходимо щелкнуть по его названию. Удаление ограничения из списка производится нажатием на пиктограмму  возле ограничения в списке. Значение параметра по умолчанию: пустой список
Ограничения отправителя	Список проверок, выполняемых на этапе идентификации отправителей письма (FROM). Возможно использование следующих проверок: • **mark_trust** – Пометить IP-адрес клиента как доверенный (trusted). Если есть еще ограничения после данного, то они будут пропущены. • **sleep** – Приостановить SMTP-соединение на заданное время (в секундах). Требуется указать время приостановки (целое число, не меньшее 1). • **tempfail** – Вернуть клиенту временную ошибку (с кодом 4*).

Параметр	Описание
	• **reject** – Вернуть клиенту постоянную ошибку (с кодом 5*). • **reject_unknown_domain** – Если имя хоста клиента не имеет ни DNS-записи "A", ни DNS-записи "MX", то прием сообщений от клиента блокируется. Для добавления ограничения в список необходимо щелкнуть по его названию. Удаление ограничения из списка производится нажатием на пиктограмму  возле ограничения в списке. Значение параметра по умолчанию: пустой список
Ограничения получателя	Список проверок, выполняемых на этапе идентификации получателей письма (RCPT). Возможно использование следующих проверок: • **mark_trust** – Пометить IP-адрес клиента как доверенный (trusted). Если есть еще ограничения после данного, то они будут пропущены. • **sleep** – Приостановить SMTP-соединение на заданное время (в секундах). Требуется указать время приостановки (целое число, не меньшее 1). • **tempfail** – Вернуть клиенту временную ошибку (с кодом 4*). • **reject** – Вернуть клиенту постоянную ошибку (с кодом 5*). • **reject_unknown_domain** – Если имя хоста клиента не имеет ни DNS-записи "A", ни DNS-записи "MX", то прием сообщений от клиента блокируется. • **reject_unknown_rcpts** – Если имя получателя отсутствует в списке **Защищаемые адреса**, то письмо на такой адрес блокируется.

Параметр	Описание
	• **reject_unauth_destination** – Если домена получателя нет ни в списке **Почтовые домены**, ни в списке **Защищаемые домены** (задается в параметрах Ядра), то прием письма для этого получателя отвергается. Для добавления ограничения в список необходимо щелкнуть по его названию. Удаление ограничения из списка производится нажатием на пиктограмму  возле ограничения в списке. Значение параметра по умолчанию: **reject_unauth_destination**
Ограничение данных	Список проверок, выполняемых на этапе передачи данных письма (DATA). Возможно использование следующих проверок: • **mark_trust** – Пометить IP-адрес клиента как доверенный (trusted). Если есть еще ограничения после данного, то они будут пропущены. • **sleep** – Приостановить SMTP-соединение на заданное время (в секундах). Требуется указать время приостановки (целое число, не меньшее 1). • **tempfail** – Вернуть клиенту временную ошибку (с кодом 4*). • **reject** – Вернуть клиенту постоянную ошибку (с кодом 5*).. • **reject_spam_trap** – Проверка на спам-ловушку. Адрес получателя должен иметь формат `<USER@HOST>`. Если `HOST` находится в в списке **Защищаемые домены** (задается в параметрах Ядра), а `USER` – в списке, заданном в значении параметра **Ловушка для спама**, то прием сообщения блокируется.

Параметр	Описание
	• **reject_multi_recipient_bounce** – Блокировать прием сообщения, если поле `From:` пустое, а получателей сообщения более одного. Для добавления ограничения в список необходимо щелкнуть по его названию. Удаление ограничения из списка производится нажатием на пиктограмму возле ограничения в списке. Значение параметра по умолчанию: пустой список
Откладывать блокирование писем до стадии RCPT	Определяет, будет ли блокировка писем производиться сразу при срабатывании ограничений (если они произошли на этапе подключения или HELO/EHLO), или откладывать ее до стадии RCPT. Установка данного параметра в значение "Да" позволяет работать с устаревшими версиями почтовых клиентов и выводить список заблокированных адресов получателей в файл журнала. Для установки значения параметра выберите его значение из выпадающего списка. Значение параметра по умолчанию: **Да**
Черный список сетей	Задает черный список сетей, используемый ограничением **reject_black_networks**. Сетью считается непрерывный диапазон IP-адресов, задаваемый в формате CIDR (IP/MASK, например, `192.168.10.0/8`). Чтобы добавить в список новую сеть, укажите ее IP-диапазон в поле ввода, и нажмите пиктограмму . Удаление сети из списка производится нажатием пиктограммы в списке возле адреса сети. Значение параметра по умолчанию: пустой список

Параметр	Описание
Белый список сетей	Задает белый список сетей, используемый ограничением **trust_white_networks**. Сетью считается непрерывный диапазон IP-адресов, задаваемый в формате CIDR (IP/MASK, например, `192.168.10.0/8`). Чтобы добавить в список новую сеть, укажите ее IP-диапазон в поле ввода, и нажмите пиктограмму  . Удаление сети из списка производится нажатием пиктограммы  в списке возле адреса сети. Значение параметра по умолчанию: пустой список
Серверы DNSBL	Задает белый список серверов DNSBL (сервера черных списков почтовых доменов), используемых ограничением **reject_dnsbl**. Чтобы добавить в список новый сервер DNSBL, укажите его в поле ввода, и нажмите пиктограмму  . Удаление сервера из списка производится нажатием пиктограммы  в списке возле сервера DNSBL. Значение параметра по умолчанию: пустой список
Время ожидания кеширования положительных ответов серверов DNSBL	Максимальный промежуток времени для кеширования положительных ответов от DNSBL-серверов (используется с целью минимизировать количество запросов к DNSBL). Слишком большое значение параметра устанавливать не рекомендуется, поскольку ранее кешированные данные могут устареть. Для задания параметра в поле ввода указывается величина периода ожидания (положительное целое число) и выбирается единица измерения периода времени (секунд, минут, часов, дней) из выпадающего списка. Значение параметра по умолчанию: **24 часа**

Параметр	Описание
Время ожидания кеширования отрицательных ответов серверов DNSBL	Аналогично **Времени ожидания кеширования положительных ответов серверов DNSBL**, только указывается время кеширования отрицательных ответов от серверов DNSBL. Значение параметра по умолчанию: **10 минут**
Время ожидания кеширования отрицательных ответов серверов DNS	Аналогично **Времени ожидания кеширования отрицательных ответов серверов DNSBL**, только указывается время кеширования отрицательных ответов от DNS-серверов. Значение параметра по умолчанию: **10 минут**
Черный список доменов	Черный список доменов, используемый ограничением **reject_black_domains**. Для задания поддоменов возможно использование регулярного выражения (например, `regex:.*.domain.com` – все поддомены `domain.com`). Для добавления почтового домена или регулярного выражения в список необходимо ввести его в поле редактирования, выбрать тип из выпадающего списка (другое значение или регулярное выражение) и нажать пиктограмму  . Удаление домена из списка производится нажатием на пиктограмму  возле адреса в списке. Значение параметра по умолчанию: пустой список
Белый список доменов	Белый список доменов, используемый ограничением **trust_white_domains**. Для задания поддоменов возможно использование регулярного выражения (например, regex:.*.domain.com - все поддомены domain.com).

Параметр	Описание
	Для добавления почтового домена или регулярного выражения в список необходимо ввести его в поле редактирования, выбрать тип из выпадающего списка (другое значение или регулярное выражение) и нажать пиктограмму  . Удаление домена из списка производится нажатием на пиктограмму  возле адреса в списке. Значение параметра по умолчанию: пустой список
Ловушка для спама	Список адресов для ловушки для спама, используемых в действии **reject_spam_trap**. В список могут быть добавлены как непосредственно адреса (в формате `user@domain`), так и регулярные выражения, которые будут описывать группы адресов. Для добавления адреса или регулярного выражения в список необходимо ввести его в поле редактирования, выбрать тип из выпадающего списка (другое значение или регулярное выражение) и нажать пиктограмму  . Удаление адреса из списка производится нажатием на пиктограмму  возле адреса в списке. Значение параметра по умолчанию: пустой список
Репутационный IP-фильтр	Репутационный IP-фильтр позволяет выставлять счет IP-адресу клиента-отправителя сообщений на основе набираемой по данному адресу статистики и временно блокировать IP-адрес в случае, если его итоговый счет превышает некоторое пороговое значение. Фильтры проверяются в порядке их задания в списке. Доступны следующие фильтры:

Параметр	Описание
	• **anti_dha** – противодействие DHA-атакам. Для использования этого фильтра необходимо задать список **Защищаемых адресов**. Параметры, которые могут использоваться только этим фильтром: ○ **wrong_per_valid_rcpts** – отношение ошибочных получателей письма (которые были отклонены после команды RCPT TO) к корректным получателям. Основной параметр, которые определяет работу фильтра. Если не было найдено ни одного корректного получателя, то это число принимается равным единице. Если значение установлено в 0, фильтр полностью игнорируется. Вещественное неотрицательное число. Значение по умолчанию: **10.0**. Значения общих параметров по умолчанию (см. ниже): ○ **min_msgs=0.** ○ **min_errors=0.** ○ **min_wrong_rcpts=20.** ○ **min_conn=0.** ○ **block_period=2h.** ○ **score=0.** • **errors_filter** – позволяет отфильтровывать IP-адреса на основании количества ошибок в SMTP-сессии, которые происходят при общении с данным IP-адресом. Параметры, которые могут использоваться только этим фильтром: ○ **errors_per_msg** – отношение числа ошибок на этапе SMTP-сессии к переданным в **Почтовый прокси** сообщениям. Если не было передано ни одного сообщения, то это число принимается равным единице. Если

Параметр	Описание
	параметр установлен в 0, то проверка игнорируется. Вещественное неотрицательное число. Значение по умолчанию: **0**. ○ **errors_per_conn** – отношение числа ошибок на этапе SMTP-сессии к числу соединений с этого IP-адреса. Проверка срабатывает только в том случае, если значение параметра установлено не в 0 и было хотя бы одно соединение с этого IP-адреса. Вещественное неотрицательное число. Значение по умолчанию: **2.0**. Значения общих параметров по умолчанию (см. ниже): ○ **min_msgs=0.** ○ **min_errors=100.** ○ **min_wrong_rcpts=0.** ○ **min_conn=50.** ○ **block_period=2h.** ○ **score=0.** • **score_filter** – позволяет отфильтровывать IP-адреса на основании среднего значения счета, выставленного всем сообщениям и сессиям с этого IP-адреса. Входит в общую систему счета и позволяет, к примеру, блокировать злостных распространителей спама уже на этапе SMTP-соединения. Параметры, которые могут использоваться только этим фильтром: ○ **score_per_msg** – отношение общего счета для данного IP (сумма всех счетов сообщений, отправленных с данного IP, и счетов, выставленных сессиям (например, другими репутационными IP фильтрами или restrictions)) к переданным в **Почтовый прокси** сообщениям. Если

Параметр	Описание
	не было передано ни одного сообщения, то это число принимается равным единице. Если параметр установлен в 0, то проверка игнорируется. Вещественное неотрицательное число. Значение по умолчанию: **0**. ○ **score_per_conn** – отношение общего счета для данного IP-адреса к числу соединений с этого IP-адреса. Проверка срабатывает только в том случае, если значение параметра установлено не в 0 и было хотя бы одно соединение с этого IP-адреса. Вещественное неотрицательное число. Значение по умолчанию: **100.0**. Если заданы оба параметра, то в начале проверяется **score_per_msg**, а затем **score_per_conn**. Если оба параметра установлены в 0, то фильтр игнорируется. Значения общих параметров по умолчанию (см. ниже): ○ **min_msgs=0.** ○ **min_errors=0.** ○ **min_wrong_rcpts=0.** ○ **min_conn=100.** ○ **block_period=2h.** ○ **score=0.** Параметры, которые могут применяться с любым из фильтров: ○ **min_msgs** – минимальное число переданных на проверку в **Почтовый прокси** сообщений, после которого срабатывает фильтр (положительное целое число). Если значение равно 0, то параметр игнорируется. ○ **min_errors** – минимальное число ошибок,

Параметр	Описание
	зарегистрированных на этапе SMTP-сессии, после которого срабатывает фильтр. (положительное целое число) Если значение равно 0, то параметр игнорируется. ○ **min_wrong_rcpts** – минимальное число ошибочных получателей письма (которые были отклонены после команды RCPT TO), переданных SMTP-клиентом, после которого срабатывает фильтр (положительное целое число). Если значение равно 0, то параметр игнорируется. ○ **min_conn** – минимальное число соединений с этого IP адреса, после которого срабатывает фильтр (положительное целое число). Если значение равно 0, то параметр игнорируется. ○ **block_period** – задает время блокировки IP адреса, если он подпадает под ограничения данного фильтра (время в формате num{s|m|h}, например, 2s – две секунды). Если значение установлено в 0, то блокировки не происходит, даже если IP подпадает под ограничения фильтра. ○ **score** – счет, который будет выставлен всем сообщениям в данной сессии. Также он будет добавлен к общему счету IP-адреса (см. ниже). Если это значение установлено не в 0, то при срабатывании фильтра вместо блокировки IP-адреса на время, указанное в значении параметра **block_period**, будет производиться выставление счета, на основе которого можно будет в дальнейшем осуществлять фильтрацию писем/адресов.

Параметр	Описание
	При вводе параметра фильтры в текстовом поле перечисляются через запятую. Для каждого фильтра указывается его название, затем перечисляются параметры фильтра, разделяемые пробелами (параметры фильтров не являются обязательными). Параметры указываются в виде пар ПАРАМЕТР=ЗНАЧЕНИЕ (например: `errors_filter score=20`). Значение параметра по умолчанию: **score_filter**

* Ограничения проверяются в перечисленном в списке порядке до тех пор, пока либо письмо не будет отклонено, либо пока оно не будет помечено как доверенное (trusted). Если письмо на каком-либо этапе помечается как "доверенное", все оставшиеся проверки пропускаются.

Дополнительные параметры приема почты

В этой секции имеется возможность задания следующих дополнительных параметров приема почты:

Параметр	Описание
Время обработки застрявших писем	Промежуток времени, отводимый на обработку "застрявших" писем. "Застрявшие" письма – сообщения, полученные, но не обработанные модулями проверки вовремя. Для задания параметра в поле ввода указывается величина времени обработки (положительное целое число) и выбирается единица измерения периода времени (секунд, минут, часов, дней) из выпадающего списка. Значение параметра по умолчанию: **10 минут**
Время ожидания исполнения команды	Максимальный промежуток времени, отводимый на исполнение одной команды протокола SMTP.

Параметр	Описание
	Для задания параметра в поле ввода указывается величина периода времени ожидания (положительное целое число) и выбирается единица измерения периода времени (секунд, минут, часов, дней) из выпадающего списка. Значение параметра по умолчанию: **5 минут**
Время ожидания получения сообщения	Максимальный промежуток времени, отводимый на ожидание получения от клиента следующей команды протокола SMTP. Для задания параметра в поле ввода указывается величина периода ожидания (положительное целое число) и выбирается единица измерения периода времени (секунд, минут, часов, дней) из выпадающего списка. Значение параметра по умолчанию: **10 минут**
Максимальное количество неосновных команд	Максимальное число неосновных команд SMTP (RSET, NOOP и VRFY), разрешенных в течение SMTP-сессии с клиентом. Если число команд превысит указанное значение, то начнет увеличиваться счетчик ошибок. Значение счетчика сбрасывается при каждой успешной обработке письма **Почтовым прокси**. Если значение равно 0, то данное ограничение не используется. Для задания параметра в поле ввода указывается разрешенное количество команд (положительное целое число). Значение параметра по умолчанию: **100**
Максимальное количество команд приветствия	Максимальное число команд HELO/EHLO/LHLO, разрешенных в течение SMTP-сессии с клиентом. Если число команд превысит указанное значение, то начнет увеличиваться счетчик ошибок. Значение счетчика сбрасывается при каждой успешной обработке письма **Почтовым прокси**. Если значение равно 0, то данное ограничение не используется.

Параметр	Описание
	Для задания параметра в поле ввода указывается разрешенное количество команд (положительное целое число). Значение параметра по умолчанию: **20**
Пороговое значение счета для сессии	Пороговое значение для максимального общего счета для каждой сессии. Если общий счет сессии превысит указанное значение, то соединение закрывается с возвращением клиенту временной ошибки. Если значение установлено в 0, то данный параметр игнорируется. Для задания параметра в поле ввода указывается значение счета (целое число из диапазона [-10000, 10000]). Значение параметра по умолчанию: **10000**

Настройка отправки почты

Для доступа к управлению настройками отправки почты **Почтовым прокси Dr.Web** необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния комплекса;
- На странице настроек **Почтового прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Отправка почты**.

Основные параметры отправки почты

На данной вкладке имеется возможность задания следующих основных параметров отправки почты:

Параметр	Описание
Адрес	Список адресов (не менее одного), используемых для отправки исходящих сообщений (проверенных сообщений и отчетов). Адрес отправки имеет вид `inet:<port>@<host>` (где <port> – порт, прослушиваемый сервером, а <host> – IP-адрес или имя хоста, на котором расположен почтовый сервер), или MX:<hostname> (где <hostname> – имя хоста). Этот параметр должен соответствовать значению параметра **Адрес**, указанного на странице Основных настроек). Для добавления адреса в список необходимо ввести адрес в поле редактирования и нажать пиктограмму  . Удаление адреса из списка производится нажатием на пиктограмму  возле адреса в списке. Значение параметра по умолчанию: **inet:3003@127.0.0.1**
Отправлять DSN-отчеты	Параметр указывает, будут ли отсылаться отчеты DSN (delivery status notification) при работе **Почтового прокси**. Имеются два значения "Да" и "Нет". Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Маршрутизация	Список правил маршрутизации сообщений в зависимости от их получателей. Сообщения, адресованные разным получателям, могут быть отправлены с разных адресов.

Параметр	Описание
	В случае, если сообщение имеет несколько получателей, причем разным получателям оно должно быть отправлено с разных адресов, то список получателей сообщения следует разделить на группы таким образом, чтобы на адреса каждой группы сообщение отправлялось с отдельного адреса. Копия сообщения создается для каждой группы получателей. Значения параметра задаются в формате <DOMAIN> <ADDRESS>, где • <DOMAIN> – строка, которая полностью должна содержаться в адресе получателя (адрес получателя имеет формат `<user@host>`). Регистр символов не учитывается. Например, если ищется строка `'@localhost'`, то совпадения будут найдены в адресах `'<test@LOCALHOST>'` и `'<yy@localhost.localdomain>'`, а если ищется строка `'@localhost>'`, то совпадение будет найдено только в конверте `'<test@LOCALHOST>'`. Допускается также в качестве <DOMAIN> указывать регулярное выражение. В этом случае отобраны будут те получатели, адреса которых будут удовлетворять указанному регулярному выражению. • <ADDRESS> – адреса, на которые будут отправляться сообщения, если строка <DOMAIN> найдена в адресе получателя. Формат строки <ADDRESS> аналогичен формату параметра **Адрес**.

Параметр	Описание
	Возможно указание нескольких адресов с разделением их символом "|", тогда письмо будет доставлено по первому адресу, с которым удалось установить соединение (пример: '@main.server.com> mx:main.server.com| inet:25@backup.server.com'). Обратите внимание, что каждому конкретному домену в соответствие ставится один адрес, поэтому конструкции вида 'domain, domain2 25@host' недопустимы. Для добавления правила в список необходимо выбрать типа строки поиска соответствия домена (регулярное выражение или другое значение), ввести пару <DOMAIN> <ADDRESS> в поле редактирования и нажать пиктограмму  . Удаление правила из списка производится нажатием на пиктограмму  возле адреса в списке. Значение параметра по умолчанию: пустой список

Дополнительные параметры отправки почты

В этой секции имеется возможность задания следующих дополнительных параметров отправки почты:

Параметр	Описание
Время для обработки застрявших сообщений	Промежуток времени, отводимый на обработку "застрявших" писем. "Застрявшие" письма – сообщения, полученные, но не обработанные модулями проверки вовремя. Для задания параметра в поле ввода указывается величина времени обработки (положительное целое число) и выбирается единица измерения периода времени (секунд, минут, часов, дней) из выпадающего списка. Значение параметра по умолчанию: **10 минут**

Параметр	Описание
Время между попытками отправки сообщений	Промежутки времени между попытками отправить "застрявшие" письма. Для задания параметра в поле ввода указывается промежуток в формате <num>{s|m|h|d}, где num – длина временного отрезка (положительное целое число), а буква - указатель единиц измерения (секунды, минуты, часы, дни соответственно). Можно указать более одного промежутка, в этом случае они задаются через запятую. Значение параметра по умолчанию: **0s, 10m, 1h, 4h, 12h, 1d**
Время ожидания выполнения команд приветствия	Максимальный промежуток времени, отводимый на посылку команд приветствия к серверу. Если по достижении этого времени приветствие не состоялось, подключение разрывается. Для задания параметра в поле ввода указывается величина периода ожидания (положительное целое число) и выбирается единица измерения периода времени (секунд, минут, часов, дней) из выпадающего списка. Значение параметра по умолчанию: **5 минут**
Время ожидания выполнения команды MAIL	Аналогично параметру **Время ожидания выполнения команд приветствия**, только для SMTP-команды MAIL. Значение параметра по умолчанию: **5 минут**
Время ожидания выполнения команды RCPT	Аналогично параметру **Время ожидания выполнения команд приветствия**, только для SMTP-команды RCPT. Значение параметра по умолчанию: **5 минут**
Время ожидания выполнения команд DATA/ BDAT	Аналогично параметру **Время ожидания выполнения команд приветствия**, только для SMTP-команды DATA/BDAT. Значение параметра по умолчанию: **2 минуты**

Параметр	Описание
Время ожидания отправки сообщения	Максимальный промежуток времени, отводимый на отправку сообщения серверу. Если по достижении этого времени сообщение не отправилось, подключение разрывается. Значение параметра по умолчанию: **3 минуты**
Время ожидания подтверждения доставки	Максимальный промежуток времени, отводимый на ожидания подтверждения доставки от сервера. Значение параметра по умолчанию: **10 минут**
Время ожидания выполнения других команд	Аналогично параметру **Время ожидания выполнения команд приветствия**, только для других SMTP-команд (не HELO/EHLO, MAIL, RCPT, DATA/BDAT). Значение параметра по умолчанию: **2 минуты**

Параметры антивируса

Для доступа к управлению настройками **Антивируса**, входящего в состав **Почтовым прокси Dr.Web** необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния комплекса;
- На странице настроек **Почтового прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Антивирус**.

Основные настройки Антивируса

На данной вкладке имеется возможность задания следующих основных настроек **Антивируса**:

Действие	Описание

Адрес сокета	Перечень сокетов (не менее одного), через которые **Почтовый прокси** взаимодействует с модулем **Антивирус**. Изменять параметр не рекомендуется. Для добавления сокета в список необходимо ввести адрес сокета в поле редактирования и нажать пиктограмму  . Удаление сокета из списка производится нажатием на пиктограмму  возле адреса в списке. Значение параметра по умолчанию: **pid:/var/drweb/run/drwebd.pid**
Время ожидания	Максимальное время ожидания исполнения команды модулем **Антивирус**. Если значение параметра равно **0**, время ожидания не ограничено. Для задания параметра в поле ввода указывается величина времени обработки (положительное целое число) и выбирается единица измерения периода времени (секунд, минут, часов, дней) из выпадающего списка. Значение параметра по умолчанию: **30 секунд**
Эвристический анализ	Включение эвристического анализатора. Эвристический анализатор позволяет **Антивирусу** обнаруживать неизвестные вирусы. При отключении эвристического анализатора будут обнаружены только уже известные вирусы, информация о которых хранится в антивирусных базах. При включении анализатора **Антивирус** может посылать ложные сообщения об обнаружении вирусов, поскольку работа полезных программ иногда бывает похожа на вирусную активность. Использование эвристического анализатора может привести к увеличению времени сканирования. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Да**

Добавлять X заголовки	Добавление заголовков `X-Antivirus` и `X-Antivirus-Code` к проверенным демоном `drwebd` сообщениям. Если указано значение **Да**, к каждому проверенному демоном `drwebd` сообщению добавляются заголовки `X-Antivirus` и `X-Antivirus-Code`. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Да**
Параноидальное сканирование	Настройка "параноидального" режима сканирования. Если у параметра указано значение **Да**, все сообщения будут сканироваться в "параноидальном" режиме. В этом случае **Антивирус** будет обрабатывать каждое сообщение дважды: целиком и по частям. Такой подход позволяет повысить надежность обнаружения вирусов, но одновременно приводит к увеличению времени сканирования. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Да**
Выражения для блокирования по имени файла	Список регулярных выражений, используемыхпри проверке имен файлов в отчете, присылаемом **Антивирусом** после сканирования сообщения. Имена файлов, находящихся в архивах, будут начинаться с символа > (количество символов > перед именем файла будет зависеть от степени вложенности архива). При совпадении части имени файла с каким-либо из элементов списка, выполняется действие, заданное в настройках параметра **Заблокированные по имени файла**. Данная проверка будет производится только для файлов, в которых не найдено вирусов. Пример регулярного выражения: `^>.*?\\s{5\\,}`

	Требуемое значение параметра вводится в поле редактирования. При необходимости использования нескольких регулярных выражений они перечисляются через запятую. Значение параметра по умолчанию: пусто
Лицензионные ограничения	Выбираются действия, которые следует совершить с письмом, в случае если оно не было проверено вследствие лицензионных ограничений на работу модуля **Антивирус**. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Перечень доступных обязательных действий: • **пропустить** – пропустить письмо к получателю; • **отклонить без уведомления** – отклонить письмо без уведомления получателя; • **отклонить** – отклонить письмо и уведомить получателя; • **временная ошибка** – уведомить отправителя, что письмо временно не может быть доставлено. В качестве дополнительных действий можно выбрать следующее: • **карантин** – поместить письмо в карантин; • **перенаправить** – перенаправить письмо на другой адрес (требуется ввести в поле ввода адрес получателя). Можно указать несколько адресов, разделяя их символом '|'; • **информировать** – выслать отчет о найденных в письме угрозах (обработка письма не прекращается); • **добавить заголовок** – добавить к письму дополнительный заголовок. Заголовок задается в виде [ИМЯ:] ЗНАЧЕНИЕ, где:

	○ ИМЯ – название заголовка (по умолчанию, если не указано, `X-DrWeb-MailD`), ○ ЗНАЧЕНИЕ – значение заголовка. При использовании в заголовке символа ';', а также символов '(' и ')' их необходимо экранировать, поставив перед ними трижды символ обратного слэша '\' (например: `X-Additional-Header: LicenseRestricted\\\; );` • **добавить счет** – добавить к значению Счета сообщения указанное значение. Добавляемое значение - это указанное целое число (может быть отрицательным). Основное действие выбирается из выпадающего списка **Основное действие**, а дополнительные действия добавляются в список **Дополнительные действия** нажатием на иконку  . Значение параметра по умолчанию: • Обязательное действие: **пропустить** • Дополнительные действия: нет
Зараженные	Выбираются действия, которые следует совершить с письмом, в случае если модулем **Антивирус** в нем были найдены объекты, зараженные вирусами. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Перечень доступных обязательных действий: • **лечить** – выполнить попытку излечения вложения (удаления вируса без повреждения содержащего его файла); • **удалить** – удалить зараженное вложение из письма; • **отклонить без уведомления**; • **отклонить**. В качестве дополнительных действий можно выбрать следующее: • **карантин**;

	• **перенаправить**; • **информировать**; • **добавить заголовок**; • **добавить счет**. Основное действие выбирается из выпадающего списка **Основное действие**, а дополнительные действия добавляются в список **Дополнительные действия** нажатием на иконку  . Значение параметра по умолчанию: • Обязательное действие: **лечить** • Дополнительные действия: **карантин**
Подозрительные	Выбираются действия, которые следует совершить с письмом, в случае если модулем **Антивирус** выделены объекты, подозрительные на вредоносное поведение. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Перечень доступных обязательных действий: • **пропустить**; • **удалить**; • **отклонить без уведомления**; • **отклонить**. В качестве дополнительных действий можно выбрать следующее: • **карантин**; • **перенаправить**; • **информировать**; • **добавить заголовок**; • **добавить счет**. Основное действие выбирается из выпадающего списка **Основное действие**, а дополнительные действия добавляются в список **Дополнительные действия** нажатием на иконку  .

	Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**, **информировать**
Неизлечимые	Выбираются действия, которые следует совершить с письмом, в случае если модулю **Антивирус** не удалось вылечить вложение (т.е. невозможно удалить вредоносное содержимое, не нарушив целостность вложения). Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Перечень доступных обязательных действий: • **удалить**; • **отклонить без уведомления**; • **отклонить**. В качестве дополнительных действий можно выбрать следующее: • **карантин**; • **перенаправить**; • **информировать**; • **добавить заголовок**; • **добавить счет**. Основное действие выбирается из выпадающего списка **Основное действие**, а дополнительные действия добавляются в список **Дополнительные действия** нажатием на иконку  . Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**, **информировать**

Рекламные программы	Выбираются действия, которые следует совершить с письмом, в случае если модуль **Антивирус** обнаружил в письме рекламную программу. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Перечень доступных обязательных действий: • **пропустить**; • **удалить**; • **отклонить без уведомления**; • **отклонить**. В качестве дополнительных действий можно выбрать следующее: • **карантин**; • **перенаправить**; • **информировать**; • **добавить заголовок**; • **добавить счет**. Основное действие выбирается из выпадающего списка **Основное действие**, а дополнительные действия добавляются в список **Дополнительные действия** нажатием на иконку  . Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**, **информировать**
Программы дозвона	Выбираются действия, которые следует совершить с письмом, в случае если модуль **Антивирус** обнаружил в письме программу дозвона. Аналогично параметру **Рекламные программы**. Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**, **информировать**

Программы-шутки	Выбираются действия, которые следует совершить с письмом, в случае если модуль **Антивирус** обнаружил в письме программу-шутку. Аналогично параметру **Рекламные программы**. Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**, **информировать**
Потенциально опасные программы	Выбираются действия, которые следует совершить с письмом, в случае если модуль **Антивирус** обнаружил в письме программу, потенциально являющуюся опасной. Аналогично параметру **Рекламные программы**. Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**, **информировать**
Программы взлома	Выбираются действия, которые следует совершить с письмом, в случае если модуль **Антивирус** обнаружил в письме программу, предназначенную для взлома компьютеров или сетей. Аналогично параметру **Рекламные программы**. Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**, **информировать**
Пропущенные	Выбираются действия, которые следует совершить с письмом, в случае если модуль **Антивирус** обнаружил в нем объекты, содержимое которых не может быть проверено. Невозможность проверки может возникнуть в следующих случаях: • Во вложении находятся защищенные

	паролем или испорченные архивы, символические ссылки, файлы нестандартных форматов. • Достигнуто максимальное время ожидания проверки сообщения. Аналогично параметру **Рекламные программы**. Значение параметра по умолчанию: • Обязательное действие: **пропустить** • Дополнительные действия: пустой список
Ограничения для архивов	Выбираются действия, которые следует совершить с письмом, в случае если модуль **Антивирус** обнаружил в нем архивы, содержимое которых не может быть проверено. Невозможность проверки архивов может возникнуть в следующих случаях: • Степень сжатия архивов превышает заданное для модуля значение. • Размер запакованных объектов превышает заданное для модуля значение. • Степень вложенности архивов превышает заданное для модуля значение. Аналогично параметру **Рекламные программы**. Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**, **информировать**
Ошибки сканирования	Выбираются действия, которые следует совершить с письмом, в случае если модуль **Антивирус** не может проверить объекты, находящиеся в нем, вследствие ошибок. Аналогично параметру **Рекламные программы**. Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**

Ошибки обработки	Выбираются действия, которые следует совершить с письмом, в случае если модуль **Антивирус** не может обработать объекты, находящиеся в нем, вследствие ошибок. Аналогично параметру **Рекламные программы**. Значение параметра по умолчанию: • Обязательное действие: **пропустить** • Дополнительные действия: **карантин**
Заблокированные по имени файла	Действия, выполняющиеся в случае совпадения одного из регулярных выражений, указанных в настройках параметра **Выражения для блокирования по имени файла**, с именем файла из отчета, присылаемого модулем **Антивируса** после сканирования сообщения. Действие, заданное в настройках этого параметра, будет применяться ко всем письмам, включающим архивы или файлы, в именах которых содержится 5 и более символов пробела. Аналогично параметру **Рекламные программы**. Значение параметра по умолчанию: • Обязательное действие: **отклонить** • Дополнительные действия: **карантин**, **информировать**
Максимальный размер	Максимальный размер проверяемого сообщения. При значении **0** ограничения отсутствуют. Если размер сообщения превысит указанное значение, будет зафиксирована **Ошибка обработки**. В поле редактирования необходимо указать целое неотрицательное число, а в выпадающем списке выбрать единицы измерения параметра (байты, килобайты, мегабайты). Значение параметра по умолчанию: **10 МБ**

Дополнительные настройки Антивируса

В данном разделе имеется возможность задания следующих дополнительных настроек **Антивируса**:

Действие	Описание
Использовать настраиваемые сообщения	Определяет, следует ли использовать перечень настраиваемых сообщений (их перечень дается в этом же разделе ниже) для формирования ответных сообщений отправителю сообщения при возникновении ошибок их приема или обработки. Значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Использовать TCP_NODELAY	Использовать ли параметр TCP_NODELAY. Если вы не испытываете проблем с сетью, не изменяйте заданное по умолчанию значение. Значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Ограничение размера файла отчета	Максимальный размер файла отчета о работе модуля **Антивирус**. При значении **0** ограничения отсутствуют. Не рекомендуется устанавливать значение равным 0, так как впротивном случае размер файла отчёта может превысить несколько МБайт после обнаружения в сообщениях вредоносных программ или почтовых бомб. В поле редактирования необходимо указать целое неотрицательное число, а в выпадающем списке выбрать единицы измерения параметра (байты, килобайты, мегабайты). Значение параметра по умолчанию: **50 КБ**
Сообщение о зараженных файлах	Текст сообщения, высылаемого при обнаружении в письме зараженных файлов. Текст вводится в текстовое поле. Текст, содержащий пробелы, должен быть заключён в кавычки.

	Значение параметра по умолчанию: **"DrWEB Antivirus: Message is rejected because it contains a virus."**
Сообщение о вредоносных программах	Текст сообщения, высылаемого при обнаружении в письме вредоносных программ. Аналогично **Сообщению о зараженных файлах**. Значение параметра по умолчанию: **"DrWEB Antivirus: Message is rejected because it contains a malware."**
Сообщение о подозрительных файлах	Текст сообщения, высылаемого при обнаружении в письме подозрительных файлов. Текст вводится в текстовое поле. Текст, содержащий пробелы, должен быть заключён в кавычки. Значение параметра по умолчанию: **"DrWEB Antivirus: Message is rejected because it contains suspicious content."**
Сообщение о пропущенных файлах	Текст сообщения, высылаемого при обнаружении в письме файлов, пропущенных при проверке. Аналогично **Сообщению о зараженных файлах**. Значение параметра по умолчанию: **"DrWEB Antivirus: Message is rejected because it cannot be checked."**
Сообщение об архивных ограничениях	Текст сообщения, высылаемого при обнаружении в письме архивов с ограничениями проверки. Аналогично **Сообщению о зараженных файлах**. Значение параметра по умолчанию: **"DrWEB Antivirus: Message is rejected because it contains archive which violates restrictions."**
Сообщение об ошибках проверки	Текст сообщения, высылаемого при ошибке проверки файлов в письме

	Аналогично **Сообщению о зараженных файлах**. Значение параметра по умолчанию: **"DrWEB Antivirus: Message is rejected due to software error."**
Сообщение о файлах, заблокированных по имени	Текст сообщения, высылаемого при обнаружении в письме файлов, заблокированных по имени Аналогично **Сообщению о зараженных файлах**. Значение параметра по умолчанию: **"DrWEB MailD: Message is rejected due to filename pattern"**

Параметры антиспама

Для доступа к управлению настройками **Антиспам-модуля**, входящего в состав **Почтовым прокси Dr.Web** необходимо:

- Перейти по ссылке **Почтовый прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка почты** на странице просмотра состояния комплекса;
- На странице настроек **Почтового прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Антиспам**.

Основные настройки Антиспам-модуля

На данной вкладке имеется возможность задания следующих основных настроек **Антиспам-модуля**:

Действие	Описание

Полная проверка	Включение полной проверки сообщения модулем **Антиспам** на наличие спама. По результатам прохождения проверки сообщение получает оценку (счет) в виде целого числа из диапазона [-10000, 10000]. Чем меньше оценка, тем больше вероятность того, что письмо не является спамом. Обратите внимание, что при использовании этой опции общая скорость работы может уменьшиться. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Да**
Игнорировать встроенные домены	Включение игнорирования проверки на спам писем, идущих на встроенные адреса **Почтового прокси** (ящики типа nospam@domain.ru). Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Да**
Добавлять заголовок с версией	Добавление к сообщениям заголовка `X-Drweb-SpamVersion`, содержащего информацию о версии Антиспам-модуля **VadeRetro**. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Добавлять заголовок со статусом сообщения	Добавление к сообщениям заголовка `X-Drweb-SpamState-Num`, в который входит числовое значение, присвоенное сообщению Антиспам-модулем **VadeRetro** по результатам классификации: **0** – письмо не является спамом; **1** – письмо является спамом; **2** – письмо содержит вирус; **3** – уведомлением о невозможности доставки письма.

	Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Добавлять заголовок с уровнем спама	Добавление к сообщениям заголовка `X-Spam-Level`, состоящего из символов "*". Один символ "*" добавляется за каждые 10 очков, присвоенных письму. Например, при счете 110 к письму будет добавлено: `X-Spam-Level: **********`. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Добавлять заголовки	Добавление к сообщениям заголовков `X-Drweb-SpamState` и `X-Drweb-SpamScore`, содержащих информацию о том, является ли сообщение спамом и каков его итоговый счет по результатам проверки. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Да**
Проверять уведомления о доставке	Выполнять ли проверку на спам уведомлений о доставке сообщений. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Префикс для спама	Префикс, добавляемый к теме сообщения, если оно отмечено как спам. Он добавляется в случае, когда оценка, полученная письмом, больше, чем значение параметра **Граница безусловного спама** (что позволяет однозначно классифицировать сообщение как спам). Текст префикса указывается в поле ввода. В случае наличия пробелов следует заключить текст в кавычки Значение параметра по умолчанию: [**SPAM**]

Префикс для уведомлений	Префикс, добавляемый к теме сообщения, если оно является уведомлением о невозможности доставки и, соответственно, определено в 3 класс писем Антиспам-модулем **VadeRetro**. Аналогично параметру **Префикс для спама**. Значение параметра по умолчанию: пусто
Граница безусловного спама	Количество очков счета, которое должно получить сообщение, чтобы быть отнесенным к классу безусловного спама. Значение этого параметра должно быть не меньше значения параметра **Граница спама**. В поле редактирования необходимо указать целое число из диапазона [-10000, 10000]. Значение параметра по умолчанию: **1000**
Префикс для безусловного спама	Префикс, добавляемый к теме сообщения, если оно помечено как безусловный спам (когда оценка, полученная письмом, больше, чем значение параметра **Граница безусловного спама**). Аналогично параметру **Префикс для спама**. Значение параметра по умолчанию: [**SPAM**]
Граница спама	Количество очков счета, которое должно получить сообщение, чтобы быть отнесенным к классу спама. Значение этого параметра должно быть не больше значения параметра **Граница безусловного спама**. В поле редактирования необходимо указать целое число из диапазона [-10000, 10000]. Значение параметра по умолчанию: **100**
Действие для безусловного спама	Выбираются действия, которые следует совершить с письмом, в случае если оно было отнесено модулем **Антиспам** к классу безусловного спама. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Перечень доступных обязательных действий:

- **пропустить** – пропустить письмо к получателю;
- **отклонить без уведомления** – отклонить письмо без уведомления получателя;
- **отклонить** – отклонить письмо и уведомить получателя;
- **временная ошибка** – уведомить отправителя, что письмо временно не может быть доставлено.

В качестве дополнительных действий можно выбрать следующее:

- **карантин** – поместить письмо в карантин;
- **перенаправить** – перенаправить письмо на другой адрес (требуется ввести в поле ввода адрес получателя). Можно указать несколько адресов, разделяя их символом '|';
- **добавить заголовок** – добавить к письму дополнительный заголовок. Заголовок задается в виде [ИМЯ:] ЗНАЧЕНИЕ, где:
  - ИМЯ – название заголовка (по умолчанию, если не указано, `X-DrWeb-MailD`),
  - ЗНАЧЕНИЕ – значение заголовка.

  При использовании в заголовке символа ';', а также символов '(' и ')' их необходимо экранировать, поставив перед ними трижды символ обратного слэша '\' (например: `X-Additional-Header: LicenseRestricted\\\;`).

Основное действие выбирается из выпадающего списка **Основное действие**, а дополнительные действия добавляются в список **Дополнительные действия** нажатием на иконку  .

Значение параметра по умолчанию:

- Обязательное действие: **пропустить**

	• Дополнительные действия: нет
Действие для спама	Выбираются действия, которые следует совершить с письмом, в случае если оно было отнесено модулем **Антиспам** к классу спама. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Список действий заполняется аналогично параметру **Действие для безусловного спама**. Значение параметра по умолчанию: • Обязательное действие: **пропустить** • Дополнительные действия: нет
Действие для уведомлений	Выбираются действия, которые следует совершить с письмом, в случае если оно было отнесено модулем **Антиспам** к классу уведомлений. Требуется указать основное действие (обязательно) и список дополнительных (при необходимости). Список действий заполняется аналогично параметру **Действие для безусловного спама**. Значение параметра по умолчанию: • Обязательное действие: **пропустить** • Дополнительные действия: нет
Настраиваемое сообщение	Текст сообщения, высылаемого в сессии SMTP в случае, когда выполняется действие отклонить (в **Действии для безусловного спама**, **Действие для спама** или **Действии для уведомлений**). Текст вводится в текстовое поле. Текст, содержащий пробелы, должен быть заключён в кавычки. Значение параметра по умолчанию: **"Dr.WEB vaderetro plugin: Message is rejected by vaderetro"**

Белый список	Белый список отправителей. Адреса отправителей получаются из поля `From:` в теле письма. Если тело письма не будет содержать полей `From:`, либо если перед полем `From:` в теле письма будет стоять одна или несколько пустых строк, то поиск отправителя в белом списке производится не будет. Если в теле содержатся два поля From, то адрес будет взят из первого найденного поля. Если адрес из поля `From:` был найден в белом списке, то от общего счета письма отнимается 5000 баллов. Обратите внимание, что белый список не сортируется, поэтому один и тот же адрес может быть случайно указан несколько раз. В таком случае 5000 баллов будут отниматься от общего счета письма столько раз, сколько раз адрес встречается в списке (указан 3 раза – отнимется 15000 баллов). Допустимо использование шаблонов (например, чтобы добавить в белый список все адреса, принадлежащие конкретному домену, достаточно указать символ '*' вместо имени пользователя: *@mycompany.com). Для добавления адреса или регулярного выражения в список необходимо ввести его в поле редактирования, выбрать тип из выпадающего списка (другое значение или регулярное выражение) и нажать пиктограмму  . Удаление адреса из списка производится нажатием на пиктограмму  возле адреса в списке. Значение параметра по умолчанию: пустой список
Черный список	Аналогично **Белому списку**, только при нахождении адреса отправителя (из поля From) в этом списке к общему счету письма будет прибавлено 5000 баллов.

	Обратите внимание, что черный список также не сортируется, поэтому один и тот же адрес может быть случайно указан несколько раз. В таком случае 5000 баллов будут прибавляться к общему счету письма столько раз, сколько раз адрес встречается в списке (указан 3 раза – прибавится 15000 баллов). Для добавления адреса или регулярного выражения в список необходимо ввести его в поле редактирования, выбрать тип из выпадающего списка (другое значение или регулярное выражение) и нажать пиктограмму  . Удаление адреса из списка производится нажатием на пиктограмму  возле адреса в списке. Значение параметра по умолчанию: пустой список
Максимальный размер	Максимальный размер проверяемого сообщения. При значении **0** ограничения отсутствуют. Если размер сообщения превысит указанное значение, будет зафиксирована **Ошибка обработки**. В поле редактирования необходимо указать целое неотрицательное число, а в выпадающем списке выбрать единицы измерения параметра (байты, килобайты, мегабайты). Значение параметра по умолчанию: **10 МБ**

Дополнительные настройки Антиспам-модуля

В данном разделе имеется возможность задания следующих дополнительных настроек **Антиспам-модуля**:

Действие	Описание
Проверять на вирусы	Включение эвристической проверки сообщений модулем **Антиспам** на вирусы. Требуемое значение параметра выбирается из выпадающего списка.

	Значение параметра по умолчанию: **Да**
Разрешить кириллицу	Определяет, добавлять или нет дополнительные баллы к счету письма, если оно содержит текст на кириллице (если выбрано **Нет**, баллы будут прибавляться). Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Да**
Разрешить восточно-азиатские языки	Определяет, добавлять или нет дополнительные баллы к счету письма, если оно содержит текст на китайском, японском или корейском языке (если выбрано **Нет**, баллы будут прибавляться). Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Использовать настраиваемые сообщения	Определяет, будет ли высылаться настраиваемое сообщение, заданное параметром **Настраиваемое сообщение**, в случае обнаружения спама. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**
Добавлять к счету для защищаемых сетей	Количество очков счета, которое нужно прибавить к счету сообщения, если оно идет из **Защищаемой сети** (список защищаемых сетей задается в настройках Ядра). В поле редактирования необходимо указать целое число из диапазона [-10000, 10000]. Значение параметра по умолчанию: **0**
Использовать кэш ответов	Определяет, будет ли использоваться кэш для хранения ответов о том, что IP-адрес клиента, от которого идет письмо, принадлежит защищаемой сети. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Нет**

Время жизни кэша ответов	Максимальный промежуток времени, отводимый на хранение ответа в кэше ответов. Для задания параметра в поле ввода указывается величина периода ожидания (положительное целое число) и выбирается единица измерения периода времени (секунд, минут, часов, дней) из выпадающего списка. Значение параметра по умолчанию: **0 минут**
Добавлять к счету для кэша ответов	Количество очков счета, которое нужно прибавить к счету сообщения, если информация о том, что оно идет из **Защищаемой сети,** взята из кэша ответов. В поле редактирования необходимо указать целое число из диапазона [-10000, 10000]. Значение параметра по умолчанию: **0**

Сетевые настройки почты

Включение проверки почты

Для корректной работы почтовой системы при включении в структуру сети устройства **Dr.Web Office Shield** следует внести следующие изменения в конфигурацию сети:

1. В конфигурационных файлах DNS-сервера, отвечающего за домен организации, необходимо изменить MX-запись, указав в качестве почтового сервера, обрабатывающего почту, направляемую в домен, IP-адрес (или доменное имя), присвоенный **Dr.Web Office Shield**.

2. В основных настройках **Почтового прокси Dr.Web**, входящего в состав **Dr.Web Office Shield**, в качестве адреса, на который следует отправлять проверенные сообщения, следует указать IP-адрес (или MX-запись) почтового сервера домена.

После этого вся внешняя почта, направляемая в домен, будет передаваться на **Почтовый прокси Dr.Web**, который, после ее проверки передаст ее для окончательной доставки почтовому серверу домена.

Обратите внимание, что сообщения, передаваемые по защищенному протоколу SMTPS (и вообще, весь трафик, следующий через защищенные соединения SSL/TLS) не проверяются.

Отключение проверки почты

1. Отключение компонентов антивирусной и антиспам-проверки на странице основных настроек **Почтового прокси Dr.Web** приводит к тому, что почта, направляемая в домен, просто проходит через прокси без проверки.
2. Чтобы полность исключить **Почтовый прокси Dr.Web** из цепочки обработки почты, следует изменить MX-запись в конфигурационных файлах DNS-сервера, отвечающего за домен организации, указав там IP-адрес почтового сервера домена.

Обратите внимание, что если в правилах межсетевого экрана **Dr.Web Office Shield** стоит запрет на проследование трафика SMTP за пределы сетевых зон LAN и Firewall, передача почты при удалении **Почтового прокси Dr.Web** из цепочки обработки почты станет невозможной.

В этом случае откорректируйте соответствующие правила межсетевого экрана (например, добавив правило SMTP/ ACCEPT Any → Any).

Веб-прокси Dr.Web

Веб-прокси Dr.Web, входящий в состав **Dr.Web Office Shield**, предназначен для проверки всего входящего HTTP- и FTP-трафика на наличие вирусов. Кроме того, **Веб-прокси**

позволяет фильтровать доступ к веб-ресурсам как по их MIME-типу и размеру, так и по имени хоста, с которого они запрашиваются. Также с его помощью можно ограничивать доступ к нежелательным и вредоносным страницам благодаря использованию обновляемых тематических черных списков.

Для того, чтобы **Веб-прокси Dr.Web** мог проверять Интернет-трафик, в состав **Dr.Web Office Shield**, входят прокси-сервера **Squid** (для HTTP) и **Frox** (для FTP). **Frox** передает запросы на обработку **Squid**, который взаимодействует с **Веб-прокси** по протоколу ICAP. Прокси-сервера работают в прозрачном для пользователей локальной сети режиме, то есть пользователям не требуется задавать прокси-сервер для доступа к Интернету. Это достигается за счет того, что в межсетевом экране, входящем в состав **Dr.Web Office Shield**, настроены правила перенаправления Интернет-трафика на прокси-сервера.

Обратите внимание, что:

- Трафик, передаваемый по защищенному протоколу HTTPS (и вообще, весь трафик, следующий через защищенные соединения SSL/TLS), не проверяется.
- При включенном **Веб-прокси** могут оказаться недоступными FTP-ресурсы. Убедитесь, что FTP-клиенты используют активный режим FTP-подключения.

Структура Веб-прокси Dr.Web

Веб-прокси Dr.Web состоит из следующих модулей:

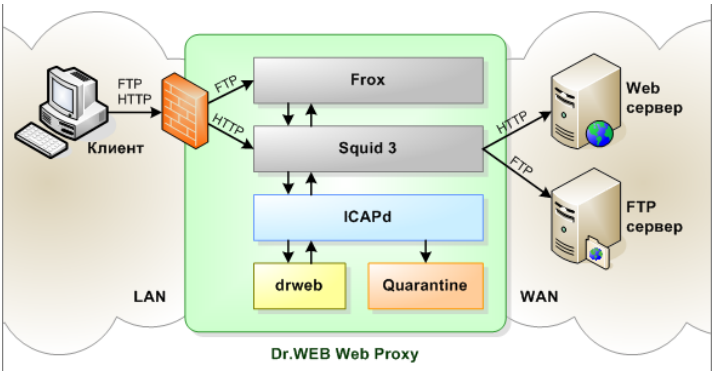
Модуль	Назначение
ICAPd	Модуль, осуществляющий взаимодействие с прокси-сервером **Squid**, обслуживающими запросы пользователей. Принимает на анализ запросы пользователей (URI) и содержимое ответов от серверов. URI пользователей проверяются на попадание в тематические списки запрещенных ресурсов, а содержимое ответов от серверов передается на анализ антивирусному модулю **drweb**

Модуль	Назначение
Quarantine	Специальный каталог, используемый для хранения подозрительных или инфицированных ответов от серверов
drweb	Модуль антивирусной проверки содержимого в ответах, поступающих от серверов

Компоненты, входящие в состав **Dr.Web Office Shield**, необходимые для функционирования **Веб-прокси**:

Модуль	Назначение
Squid	Прокси-сервер HTTP, передает модулю **ICAPd** запросы клиентов и ответы HTTP-серверов на анализ по протоколу ICAP. В зависимости от ответа **ICAPd** разрешает или запрещает получение ответа от сервера и его возврат клиенту
Frox	Прокси-сервер FTP, передает запросы клиентов прокси-серверу **Squid**, возвращает клиенту полученные ответы
Firewall	Межсетевой экран, перехватывающий HTTP- и FTP-запросы, и отправляющий их на прокси-сервера **Squid** и **Frox** соответственно

Структура **Веб-прокси**, а также типовое включение его в сеть в составе **Dr.Web Office Shield** изображены на рисунке ниже.



В типовом варианте использования **Dr.Web Веб-прокси** в составе **Dr.Web Office Shield** проверяет все HTTP- и FTP-

запросы, следующие из сетевых зон LAN и VPN, и ответы на них.

Вирусные базы, используемые модулем Антивируса **drweb**, и тематические списки вредоносных Интернет-ресурсов регулярно обновляются автоматически, что позволяет сохранять стабильно высокое качество фильтрации Интернет-трафика. Автоматическое обновление баз и тематических списков выполняет встроенный модуль **drweb-updater** согласно расписанию, заданному в планировщике **cron** операционной системы **Dr.Web Office Shield**.

По трафику, прошедшему через **Веб-прокси**, формируется статистика.

В случае истечения срока действия ключа, разрешающего работу **Веб-прокси Dr.Web**, останавливается прохождение HTTP- и FTP-трафика через устройство.

Для продолжения работы **Веб-прокси Dr.Web** необходимо приобрести новый ключ. Для предоставления доступа к Интернет без фильтрации трафика следует отключить использование **Веб-прокси Dr.Web**.

Алгоритм анализа Интернет-трафика

1. Межсетевой экран переадресует HTTP- и FTP-запросы клиентов на прокси-сервера (**Squid** и **Frox** соответственно).
2. **Frox** переадресует FTP-запросы прокси-серверу **Squid**.
3. Прокси-сервер **Squid** передает на анализ компоненту **ICAPd** ответ, поступивший от сервера, к которому обращался клиент.
4. Если URI, запрошенный клиентом, принадлежит черному списку, то модуль **ICAPd** формирует ответ, запрещающий прокси-серверу возвращать ответ сервера клиенту.
5. В противном случае содержимое (тело) ответа, полученного от сервера, передается на анализ антивирусному модулю **drweb**, который анализирует содержимое на наличие вирусов или прочего вредоносного программного обеспечения.
6. В случае если содержимое ответа не прошло проверку, оно отправляется в каталог карантина (**Quarantine**), а прокси-серверу – ответ, запрещающий возвращать его клиенту.

Настройка Веб-прокси для Dr.Web Office Shield

Доступ к настройке **Dr.Web Почтовый прокси** производится в разделе **Безопасность → Веб-прокси** главного меню. На странице настроек веб-прокси доступно три вкладки:

- На вкладке Основные настройки отображен список защищаемых сетевых интерфейсов.
- На вкладке Карантин представлен список ссылок на файлы, по которым их можно загрузить, чтобы ознакомиться с содержимым. Подозрительные файлы помещаются в карантин целиком, а имена их создаются по специальным правилам из адресов тех веб-страниц, откуда файл был скачан.
- На вкладке Расширенные настройки представлены следующие разделы по управлению работой веб-прокси:
  - Набор действий над угрозами позволяют задать действия для различных инцидентов, например для файлов с неизлечимым или подозрительным вирусом.
  - Тематический фильтр позволяет отсеивать веб-страницы по типу их содержимого (например, порнографического или иного нежелательного содержания).
  - Системные настройки позволяют задать адрес для отправления уведомлений, определить события для отправки уведомлений.
  - Правила фильтрации трафика определяют правила обработки файлов в зависимости от их MIME-типа.
  - Черные и белые списки ограничивают круг ресурсов в Интернете, доступных для просмотра пользователями.

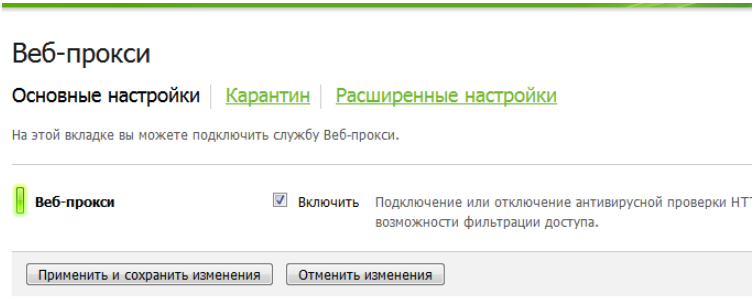
Основные настройки

На вкладке **Основные настройки** выполняется простейшая настройка работы **Веб-прокси**.

Для доступа к странице основных настроек необходимо:

- Перейти по ссылке **Веб-прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка HTTP и FTP трафика** на странице просмотра состояния комплекса;
- На странице настроек **Веб-прокси** активировать вкладку **Основные настройки.**

Вид страницы основных настроек **Веб-прокси** показан на рисунке ниже.



Основные настройки

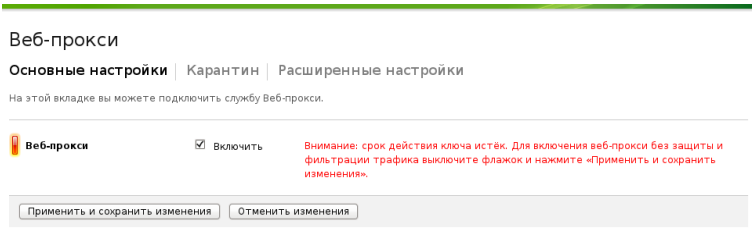
На странице основных настроек **Веб-прокси** доступны следующие настройки:

- Включение и отключение антивирусной проверки и фильтрации HTTP- и FTP-трафика. Работа **Веб-прокси** может быть включена или выключена активацией или деактивацией флажка **Включить.**

Обратите внимание, что отключение компонента **Веб-прокси Dr.Web** отключает работу прокси-серверов, через которые проходит Интернет-трафик клиентов, и разрешает его прохождение в зону WAN "сквозь устройство" напрямую. Это приводит к тому, что статистика обращений к Интернет не собирается.

В случае истечения срока действия ключа, разрешающего работу **Веб-прокси Dr.Web**, останавливается прохождение HTTP- и FTP-трафика через устройство. Для продолжения работы **Веб-прокси Dr.Web** необходимо приобрести новый

ключ. Для предоставления доступа к Интернет без фильтрации трафика следует отключить использование **Веб-прокси Dr. Web**, о чем в этом случае будет напоминать соответствующее сообщение:



Для применения указанных изменений нажмите кнопку **Применить и сохранить изменения.** Если необходимо отменить внесенные изменения и вернуть предыдущие сохраненные настройки, нажмите кнопку **Отменить изменения.**

Карантин

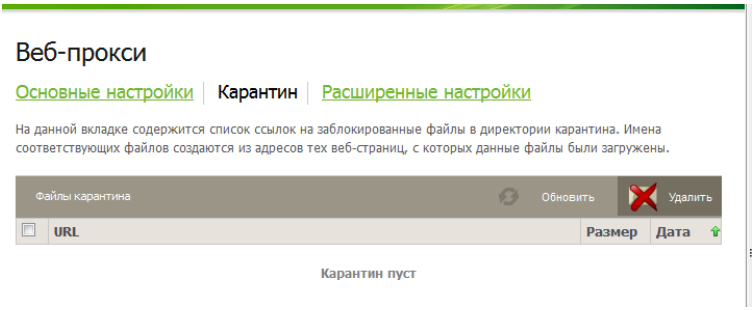
Карантин – это специальный каталог, содержащий подозрительные файлы и заблокированные ссылки.

На вкладке **Карантин** представлен список заблокированных веб-адресов. Подозрительные файлы помещаются в карантин целиком, а имена их создаются по специальным правилам из адресов тех веб-страниц, откуда файл был скачан.

Для просмотра ресурсов, помещенных **Веб-прокси Dr.Web** в карантин, необходимо:

- Перейти по ссылке **Веб-прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка HTTP и FTP трафика** на странице просмотра состояния комплекса;
- На странице настроек **Веб-прокси** активировать вкладку **Карантин**.

Вид страницы просмотра карантина показан на рисунке ниже.



Чтобы удалить URL из директории карантина, нужно выделить его и нажать кнопку **Удалить**. Данное действие является необратимым.

Расширенные настройки

Разделы расширенных настроек

На вкладке **Расширенные настройки** представлены следующие разделы по управлению работой **Веб-прокси**:

- Действия над угрозами. Позволяют задать действия при обнаружении различных типов файлов или при возникновении ошибок.
- Тематический фильтр. Настройка блокировки web-страниц по типу их содержимого (например, порнографического или иного нежелательного содержания).
- Системные настройки. Позволяют задать адрес для отправления уведомлений, определить события для отправки уведомлений
- Правила фильтрации трафика. Позволяют определить правила обработки файлов в зависимости от их MIME-типа
- Черный и Белый списки. Позволяют задать перечень адресов, разрешенных и не разрешенных для просмотра.

Для доступа к расширенным настройкам **Веб-прокси Dr.Web** необходимо:

- Перейти по ссылке **Веб-прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка HTTP и FTP трафика** на странице просмотра состояния комплекса;
- На странице настроек **Веб-прокси** активировать вкладку **Расширенные настройки.**

Переход к нужному разделу расширенных настроек осуществляется выбором нужной вкладки на странице **Расширенные настройки.**

Общие принципы редактирования расширенных настроек

На каждой странице редактирования расширенных настроек все параметры выводятся в виде таблицы, причем одна строка таблицы соответствует ровно одному параметру. В правой части строки выводится краткое описание параметра и ссылка **подробнее.** При нажатии на эту ссылку краткое описание параметра разворачивается в более подробное.

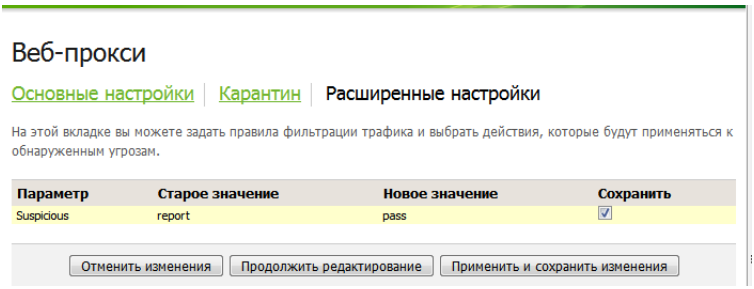
При задании расширенных настроек значение каждого параметра либо выбирается из выпадающего списка, либо вводится в соответствующее поле ввода. Если параметр может иметь более одного значения, то перечень заданных значений выводится в виде списка. При задании и изменении значений параметров рядом с полями значений доступны пиктограммы, нажатие на которые выполняет действия, приведенные в таблице:

	Установка значения параметра по умолчанию
	Отмена изменения значения параметра и возврат к предыдущему значению
	Удаление значения из списка значений параметра (только если параметр может принимать более 1 значения)
	Добавление нового значения в список значений параметра (только если параметр может принимать более 1 значения)

	Перемещение значения в списке на более приоритетную позицию (только если параметр может принимать более 1 значения)
	Перемещение значения в списке на менее приоритетную позицию (только если параметр может принимать более 1 значения)

Просмотр и сохранение внесенных изменений

Для того чтобы просмотреть все внесенные в настройку изменения, нажмите кнопку **Предпросмотр** внизу страницы редактирования параметров. На появившейся странице вы можете выбрать те изменения, которые желаете сохранить, отметив соответствующую ячейку. Вид страницы просмотра внесенных изменений показан на рисунке ниже.



Если вы хотите внести дополнительные изменения, вы можете вернуться к предыдущей странице, нажав на кнопку **Продолжить редактирование.** Если вы хотите отменить изменения, то нажмите кнопку **Отменить изменения.** Если сделанные изменения вас устраивают, нажмите на кнопку **Применить и сохранить изменения.**

Действия над угрозами

На данной вкладке вы можете настроить действия, которые должен выполнить **Веб-прокси Dr.Web** при обнаружении различных типов угроз или при возникновении ошибок.

Для доступа к настройкам действий **Веб-прокси Dr.Web** необходимо:

- Перейти по ссылке **Веб-прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка HTTP и FTP трафика** на странице просмотра состояния комплекса;
- На странице настроек **Веб-прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Действия над угрозами**.

Параметры реагирования на угрозы

На данной вкладке имеется возможность задания следующих параметров:

Параметр	Описание
Подозрительные	Действие, совершаемое с подозрительными (потенциально заражёнными) файлами. Возможные действия: • **В карантин** – поместить объект (URL, файл) в карантин. • **Игнорировать** – игнорировать угрозу, вернуть ответ клиенту. • **Отсечь** – вернуть ответ, вырезав из него подозрительный объект. • **Информировать** – вернуть клиенту страницу с сообщением о подозрении. • **Лечить** (доступно только для объектов, отмеченных как "Зараженные") – попытаться вылечить зараженный объект, удалив из него вредоносное содержимое. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**
Зараженные	Действие, совершаемое с заражёнными файлами, которые, возможно, удастся вылечить.

Параметр	Описание
	Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Лечить**
Неизлечимые	Действие, совершаемое с файлами, содержащими неизлечимые вирусы. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**
Рекламные программы	Действие, совершаемое с рекламными программами. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**
Программы дозвона	Действие, совершаемое с программами дозвона. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**
Программы-шутки	Действие, совершаемое с программами-шутками. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**
Потенциально опасные программы	Действие, совершаемое с потенциально опасными программами. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**

Параметр	Описание
Программы для взлома	Действие, совершаемое с программами для несанкционированного доступа. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**
Архивные ограничения	Действие, совершаемое с архивами, которые не могут быть проверены демоном по причине превышения значений ряда параметров (степени сжатия, размера запакованных объектов, степени вложенности). Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**
Ошибка Демона	Действие, совершаемое с файлами, вызывающими у Демона ошибки в процессе проверки. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**
Пропускаемые файлы	Действие, совершаемое с файлами, которые не могут быть проверены демоном. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**
Ошибка лицензии	Действие, совершаемое с файлами, при проверке которых произошла ошибка лицензии. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Информировать**

Параметр	Описание
Эвристический анализатор	Включение эвристического анализатора. Эвристический анализатор позволяет **Антивирусу** обнаруживать неизвестные вирусы. При отключении эвристического анализатора будут обнаружены только уже известные вирусы, информация о которых хранится в антивирусных базах. При включении анализатора **Антивирус** может посылать ложные сообщения об обнаружении вирусов, поскольку работа полезных программ иногда бывает похожа на вирусную активность. Использование эвристического анализатора может привести к увеличению времени сканирования. Требуемое значение параметра выбирается из выпадающего списка. Значение параметра по умолчанию: **Да**

Тематические фильтры

На данной вкладке вы можете настроить блокировку веб-страниц по типу их содержимого: например, заблокировать порнографию или сайты с информацией про наркотики.

Для доступа к настройкам тематических фильтров **Веб-прокси Dr.Web** необходимо:

- Перейти по ссылке **Веб-прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка HTTP и FTP трафика** на странице просмотра состояния комплекса;
- На странице настроек **Веб-прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Тематический фильтр**.

Параметры фильтрования сайтов

На данной вкладке имеется возможность задания следующих параметров (значения параметров могут быть выбраны из

раскрывающихся списков, содержащих значения **Да** и **Нет**):

Параметр	Описание
Язык шаблонов	Выбор языка, на котором пользователю будет выводиться сообщение, что доступ к запрошенной им странице заблокирован. Перечень доступных языков зависит от конфигурации **Веб-прокси Dr.Web** Нужный язык выбирается из выпадающего списка. Значение параметра по умолчанию: **Английский**
Блокировать порнографические сайты	Возможность блокировать порнографические интернет-ресурсы. Значение параметра по умолчанию: **Да**
Блокировать сайты, посвященные насилию	Возможность блокировать интернет-ресурсы, посвященные жестокости и насилию. Значение параметра по умолчанию: **Да**
Блокировать сайты, посвященные оружию	Возможность блокировать интернет-ресурсы, посвященные всем типам вооружений. Значение параметра по умолчанию: **Да**
Блокировать сайты, посвященные азартным играм	Возможность блокировать интернет-ресурсы, посвященные азартным играм на деньги. Значение параметра по умолчанию: **Да**
Блокировать сайты, посвященные наркотикам	Возможность блокировать интернет-ресурсы, посвящённые наркотикам. Значение параметра по умолчанию: **Да**
Блокировать сайты, содержащию нецензурную лексику	Возможность блокировать интернет-ресурсы, содержащие нецензурную лексику. Значение параметра по умолчанию: **Да**
Блокировать чаты	Возможность блокировать все чаты. Значение параметра по умолчанию: **Да**

Параметр	Описание
Блокировать сайты, посвященные терроризму	Возможность блокировать интернет-ресурсы, посвящённые терроризму. Значение параметра по умолчанию: **Да**
Блокировать почтовые сайты	Возможность блокировать интернет-ресурсы, предоставляющие бесплатную регистрацию почтового ящика. Значение параметра по умолчанию: **Да**
Блокировать социальные сети	Возможность блокировать доступ к разнообразным социальным сетям. Значение параметра по умолчанию: **Да**
Блокировать сайты, содержащие вредоносные программы	Возможность блокировать интернет-ресурсы, содержащие вирусы и другие вредоносные программы. Значение параметра по умолчанию: **Да**
Блокировать нерекоменду-емые сайты	Возможность заблокировать нерекомендумые сайты, которые могут использоваться для фишинга и мошенничества. Значение параметра по умолчанию: **Да**

Системные настройки

На данной вкладке вы можете указать почтовый адрес администратора и настроить отправку уведомлений о попытках открытия заблокированных веб-страниц.

Для доступа к системным настройкам **Веб-прокси Dr.Web** необходимо:

- Перейти по ссылке **Веб-прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка HTTP и FTP трафика** на странице просмотра состояния комплекса;
- На странице настроек **Веб-прокси** активировать вкладку **Расширенные настройки**.

- Выбрать вкладку **Системные настройки**.

Системные настройки

На данной вкладке имеется возможность задания следующих системных параметров:

Параметр	Описание
Адрес администратора	Указывается адрес почтового ящика администратора, на который шлются уведомления. Адрес указывается в фомате <user>@<host>. Значение по умолчанию: **root@localhost**
Время ожидания	Максимальное время в секундах, в течение которого сокет, через который идет взаимодействие с прокси-сервером, может находиться врежиме ожидания. Значение по умолчанию: **300**
Посылать уведомления	Следует ли посылать администратору уведомления о попытках открытия блокируемой страницы. Если **Да**, то уведомления будут посылаться на почтовый адрес, указанный в параметре **Адрес администратора**. Значение выбирается из выпадающего списка Значение по умолчанию: **Нет**
Команда отправления почты	Команда, выполняемая для отправления администратору почтового уведомления. Значение по умолчанию изменять не рекомендуется. Значение по умолчанию: **/opt/drweb/drweb-inject -f drweb@appliance -t --timeout 60**
Ожидание перед повторной отправкой	Промежуток времени в секундах, в течение которого уведомления администратору о повторных попытках открытия одной и той же блокированной страницы не высылаются. Значение по умолчанию: **60**

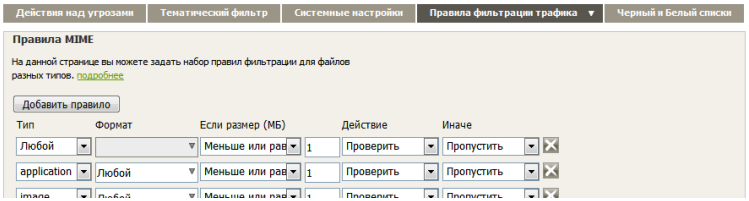
Правила фильтрации трафика

На данной вкладке вы можете настроить и создать правила обработки содержимого ответов, поступающих от удаленных серверов, в зависимости от их MIME-типа.

Для доступа к настройкам правил фильтрации трафика **Веб-прокси Dr.Web** необходимо:

- Перейти по ссылке **Веб-прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка HTTP и FTP трафика** на странице просмотра состояния комплекса;
- На странице настроек **Веб-прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Правила фильтрации трафика**.

Вид страницы настройки правил фильтрации трафика (фрагмент) изображен на рисунке ниже:



Настройка правил фильтрации трафика

Для добавления нового правила фильтрации в список необходимо нажать кнопку **Добавить правило**. Это приведет к добавлению в список правил новой строки описания правила.

Каждая строка описания правила состоит из 5 частей:

Параметр	Описание
Тип	Класс MIME-типов трафика, для которого предназначено правило. Выбирается из выпадающего списка. Доступны следующие типы: • **Любой** – Правило будет применяться ко всем видам трафика (к любому типу данных, содержащихся в теле ответа) • **application** – Правило будет применяться к ответам, содержащим программы • **audio** – Правило будет применяться к ответам, содержащим аудио-файлы любого типа • **image** – Правило будет применяться к ответам, содержащим файлы изображений любого типа • **message** – Правило будет применяться к ответам, содержащим сообщения (e-mail, MMS и т.п.) • **model** – Правило будет применяться к ответам, содержащим файлы моделей любого типа • **multipart** – Правило будет применяться к ответам, состоящим из нескольких частей • **text** – Правило будет применяться к ответам, содержащим текст • **video** – Правило будет применяться к ответам, содержащим видео-файлы любого типа По умолчанию: **Любой**
Формат	Конкретный MIME-тип из выбранного класса (указывается в поле **Тип**). Выбирается из выпадающего списка. Перечень форматов зависит от выбранного типа. При выборе пункта **Любой** правило будет срабатывать для любого формата указанного типа. По умолчанию: **Любой**

Параметр	Описание
Если размер...	Указывается условие на срабатывание правила фильтрации в зависимости от размера содержимого. Тип условия выбирается из выпадающего списка (**Больше**, **Меньше или равно**, **Любой**). В поле редактирования, расположенном справа от списка, указывается пороговый размер для условия (в мегабайтах, целое неотрицательное число). Если выбрано условие **Любой**, пороговый размер не указывается. По умолчанию: **Любой**
Действие	Указывается действие, которое следует применить к содержимому сообщения, если оно удовлетворяет указанным условиям. Действие выбирается из выпадающего списка. Доступны следующие действия: • **Проверить** – Произвести проверку содержимого при помощи компонента **Антивирус**. • **Пропустить** – Вернуть содержимое ответа клиенту не проверяя. • **Отклонить и уведомить** – Отклонить ответ, уведомив клиента. • **Отклонить не уведомляя** – Отклонить ответ не уведомляя клиента. По умолчанию: **Проверить**
Иначе	Указывается действие, которое следует применить к содержимому сообщения, если оно не удовлетворяет указанным условиям. Действие выбирается из выпадающего списка. Перечень доступных действий аналогичен параметру **Действие**. По умолчанию: **Пропустить**

Для изменения любого правила достаточно внести изменения в поля строки описания правила (например, изменить действие, условие или формат). Для удаления правила из списка следует нажать на пиктограмму  , расположенную в конце строки описания правила.

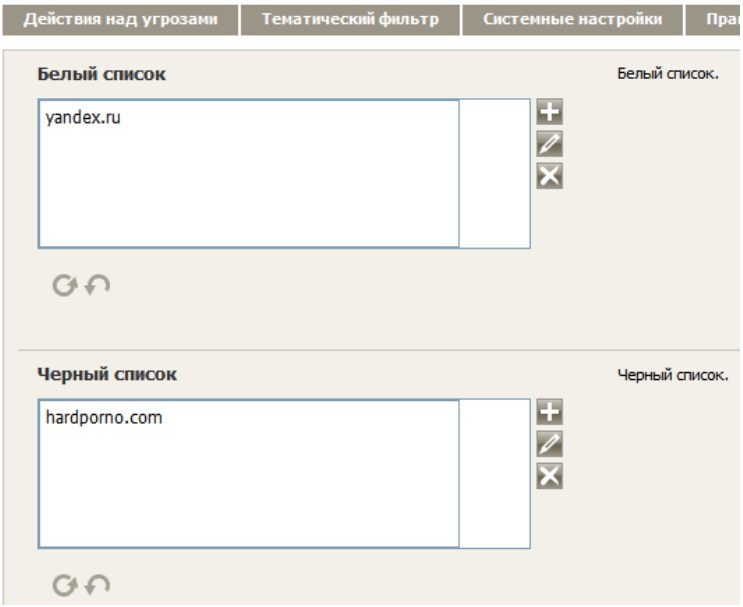
Черный и белый списки

На данной вкладке вы можете создать пользовательские черные и белые списки веб-ресурсов, которым вы не доверяете или доверяете соответственно. Веб-ресурсы, перечисленные в **Белом списке**, не будут проверяться на наличие вирусов. Веб-ресурсы, перечисленные в **Черном списке**, будут блокироваться без проверки на их наличие в тематических черных списках.

Для доступа к настройкам черного и белого списка **Веб-прокси Dr.Web** необходимо:

- Перейти по ссылке **Веб-прокси** в разделе **Безопасность** главного меню или щелкнуть по иконке **Проверка HTTP и FTP трафика** на странице просмотра состояния комплекса;
- На странице настроек **Веб-прокси** активировать вкладку **Расширенные настройки**.
- Выбрать вкладку **Черный и белый списки**.

Вид страницы управления черным и белым списком сайтов (фрагмент) изображен на рисунке ниже:



Настройка черного и белого списков

В секции **Белый список** показывается состав белого списка веб-ресурсов.

Для того, чтобы добавить веб-ресурс в белый список:

1. Нажмите кнопку  , расположенную справа от белого списка веб-ресурсов. Под белым списком веб-ресурсов появится поле ввода и две кнопки: **Применить** и **Отменить**.
2. Введите имя веб-ресурса, которому вы доверяете, в поле ввода (без пробелов, например: `yandex.ru`).
3. Для добавления введенного адреса в список нажмите кнопку **Применить**. В случае если вы хотите отменить добавление ресурса в список, нажмите кнопку **Отменить**.

Для того, чтобы изменить веб-ресурс в белом списке:

1. Выделите адрес ресурса в списке, нажмите кнопку  .
2. В появившемся поле ввода отредактируйте адрес ресурса.
3. Для внесения измененного адреса в список нажмите кнопку **Применить**. В случае если вы хотите отменить изменение ресурса в списке, нажмите кнопку **Отменить**.

Для удаления ресурса из белого списка выделите его в списке и нажмите кнопку  .

Работа с **Черным списком** аналогична работе с **Белым списком**.

Защита рабочих станций

В состав **Dr.Web Office Shield** входит компонент **Dr.Web Enterprise Server**, предназначенный для комплексного централизованного управления антивирусной защитой компьютеров в корпоративной локальной сети. При помощи **Dr.Web Enterprise Server** в рамках локальной сети предприятия строится **Антивирусная сеть Dr.Web**, которая объединяет все рабочие станции пользователей сети, защищаемые от вирусных угроз и вредоносного ПО при помощи антивирусных продуктов компании **«Доктор Веб»**.

Антивирусная сеть Dr.Web имеет клиент-серверную архитектуру, и состоит из сервера **Dr.Web Enterprise Server**, и сети защищаемых станций, оснащенных антивирусным ПО компании **«Доктор Веб»**, а также специальным программным компонентом **Dr.Web Enterprise-Агент**. Компьютеры локальной сети, не оснащенные **Dr.Web Enterprise-Агент**, не входят в состав **Антивирусной сети**.

В рамках **Антивирусной сети Dr.Web Enterprise Server** играет роль единого центра, координирующего обновление антивирусных баз и компонентов установленных антивирусных продуктов. Кроме того он выполняет роль репозитория, хранящего дистрибутивы антивирусных продуктов и их настройки для установки на рабочие станции.

Dr.Web Enterprise Server позволяет централизованно решать следующие задачи:

- Построение **Антивирусной сети** в рамках локальной сети предприятия и управление ее составом, а также политикой безопасности в ее рамках;
- Хранение дистрибутивов и установка антивирусного ПО на защищаемые компьютеры;
- Хранение, синхронизация и тиражирование в рамках **Антивирусной сети** настроек параметров антивирусного ПО;
- Централизованное обновление вирусных баз и антивирусного программного обеспечения и их распространение на защищаемые компьютерах;
- Сбор статистики вирусных инцидентов, а также мониторинг состояния антивирусного ПО и операционных систем на защищаемых компьютерах.

Dr.Web Enterprise-Агенты, устанавливаемые на защищаемые рабочие станции, используются для следующих целей:

- Включение рабочей станции в **Антивирусную сеть Dr.Web** посредством подключения к **Dr.Web Enterprise Server**;
- Применение к антивирусному ПО на компьютере настроек и команд, полученных от **Dr.Web Enterprise Server** и запрет на произвольное изменение настроек пользоваителем для предотвращения возможности нарушения глобальной политики безопасности, заданной для **Антивирусной сети**.
- Получение от **Dr.Web Enterprise Server** обновлений антивирусных баз и компонентов антивирусного программного обеспечения;
- Сбор и отправка на **Dr.Web Enterprise Server** статистики вирусных инцидентов и состояния антивирусного ПО и операционной системы.

Типовая архитектура **Антивирусной сети Dr.Web** изображена на рисунке ниже (в рамки **Антивирусной сети** входит только часть компьютеров из локальной сети).

Обратите внимание, что при любом варианте организации **Антивирусной сети Dr.Web Enterprise Server**, установленный на **Dr.Web Office Shield**, **должен иметь доступ в Интернет** для получения обновлений с серверов **Всемирной Системы Обновлений Dr.Web**.

Управление как работой **Dr.Web Enterprise Server**, так и всей антивирусной сетью в целом, осуществляется через **Центр Управления Dr.Web**, который позволяет управлять настройками как **Dr.Web Enterprise Server**, так и защищаемых компьютеров (через **Dr.Web Enterprise-Агенты**). Так же как и интерфейс управления устройством **Dr.Web Office Shield**, он представляет собой специализированный веб-интерфейс, и потому может быть запущен с любого компьютера в сети, оснащенного веб-браузером.

Доступ к **Центру Управления Dr.Web** осуществляется переходом по ссылке **Защита рабочих станций**, размещенной в разделе **Безопасность** главного меню. На открывшейся странице нажмите кнопку **Перейти к Центру управления Dr. Web**.

Стартовая страница **Центра Управления Dr.Web** открывается в отдельном окне или вкладке браузера. Для доступа к **Центру Управления Dr.Web** вам потребуется указать логин и пароль администратора **Антивирусной сети Dr.Web**.

Обратите внимание, что пароль доступа к **Dr.Web Office Shield** никак не связан с логином и паролем, используемым для доступа к **Центру управления Dr.Web**. Логин и пароль доступа к **Центру управления Dr.Web** задаются в **Центре управления Dr.Web**. По умолчанию (при заводских настройках устройства) в качестве пары логин/пароль задано `admin/root`.

Дополнительные сведения о работе с **Центром Управления Dr.Web** содержатся в Руководстве администратора **Антивирусной сети Dr.Web**, которое доступно по адресу: http://support.drweb.com/esuite/doc_ru.

Настройка работы Dr.Web Office Shield в качестве внутреннего сервера централизованной защиты

При необходимости настроить устройство **Dr.Web Office Shield** на работу только внутреннего сервера централизованной антивирусной защиты локальной сети необходимо выполнить следующее:

1. Выполняются следующие подключения к разъемам устройства:
   - В разъем LAN3 кабель не подключается;
   - В разъем LAN1 подключается кабель из зоны LAN.
2. Настраивается использование сетевых подключений:

- Флажок использования сетевой зоны WAN (Интернет) отключен.
- Флажок использования сетевой зоны LAN включен, и заданы:
  - IP-адрес устройства в зоне LAN;
  - Маска сети;
  - IP-адрес используемого шлюза.

  При необходимости задание начального адреса LAN может быть настроено через кросс-кабель.

3. Производится включение службы DNS:
   - Активировать сервис, выбрав флажок **Включить**;
   - Задать **пользовательский режим** работы встроенного DNS-сервера, указав корректный адрес DNS-сервера, используемого в сети LAN.
4. Загрузить на устройство **Dr.Web Office Shield** через веб-интерфейс ключи `enterprise.key` и `agent.key`, необходимые для функционирования компонентов **Антивирусной сети** (**Сервера** и **Агентов** соответственно).
5. Зайти на страницу **Центра управления Dr.Web**, и выполнить проверку доступности для него **Серверов Обновления Dr.Web**:
   - Авторизуйтесь, введя логин и пароль (по умолчанию – `admin` и `root` соответственно);
   - В разделе **Администрирование** выберите подраздел **Состояние репозитория**, после чего нажмите кнопку **Проверить обновления**. Если проверка наличия обновлений прошла успешно, соединение **Enterprise Server Dr.Web** с **Серверами Обновления Dr.Web** настроено корректно. В противном случае проверьте корректность адреса шлюза, заданного для подключения сетевой зоны LAN, а также корректность адреса и доступность используемого DNS-сервера.

Обратите внимание, что **Enterprise Server**, установленный на **Dr.Web Office Shield**, **должен иметь доступ к Интернет** для получения обновлений с серверов **Всемирной Системы Обновлений Dr.Web**. В противном случае ваша внутренняя **Антивирусная сеть** не будет получать обновлений и не обеспечит надлежащей защиты рабочих станций.

Полные сведения об администрировании **Антивирусной сети** и работе с **Центром Управления Dr.Web** содержатся в Руководстве администратора **Антивирусной сети Dr.Web**, которое доступно по адресу: http://support.drweb.com/esuite/doc_ru.

Настройка системы

При помощи веб-интерфейса **Dr.Web Office Shield** имеется возможность произвести настройку некоторых параметров работы системных компонентов. Доступ к системным настройкам собран в разделе **Система** главного меню.

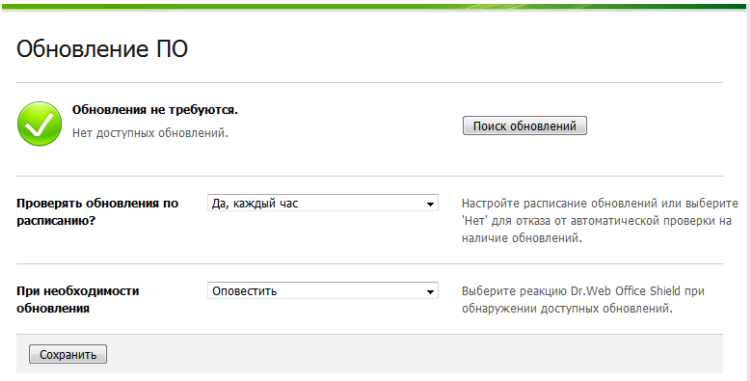
Раздел **Система** содержит следующие пункты:

- Обновление ПО – настройка расписания получения обновлений ПО;
- Сохранение и восстановление – выполнение сохранения настроек компонентов системы и их восстановление при необходимости;
- Системное время – установка, изменение и синхронизация времени на устройстве;
- Перезагрузка и завершение работы – выполнение завершения работы и перезагрузки устройства;
- Установленные пакеты – обзор перечня установленных программных пакетов.

Обновление ПО

На веб-странице **Обновление ПО** отображается индикатор необходимости обновления компонентов программного комплекса **Dr.Web Office Shield**, а также настройки периодичности проверки доступности обновлений.

Доступ к странице обновления осуществляется выбором пункта главного меню **Система** → **Обновление ПО**. Вид страницы обновления ПО приведен на рисунке ниже.



Обновление компонентов программного комплекса **Dr.Web Office Shield** осуществляется с серверов компании «Доктор Веб». В случае наличия доступных обновлений их перечень выводится в верхней части страницы. Если необходимо вручную проверить наличие доступных обновлений, следует нажать кнопку **Поиск обновлений**.

Обновление ПО включает 2 вида обновлений:

- Обновление пакетов системы;
- Обновление образа системы;

Также на этой странице доступно изменение следующих параметров обновления ПО:

Параметр	Описание
Проверять обновления по расписанию	Выбор режима проверки наличия новых обновлений компонентов комплекса. Необходимый режим проверки следует выбрать из выпадающего списка: • **Не проверять** – система не будет автоматически проверять наличие новых обновлений. Проверка наличия обновлений будет осуществляться в ручном режиме (по нажатию кнопки **Поиск обновлений**); • **Да, каждый час** – система будет автоматически проверять наличие обновлений с периодичностью 1 раз в час (*по умолчанию*); • **Да, каждый день** – система будет автоматически проверять наличие обновлений с периодичностью 1 раз в день; • **Да, каждую неделю** – система будет автоматически проверять наличие обновлений с периодичностью 1 раз в неделю.
При необходимости обновления	Выбор действия, которое будет выполняться в случае наличия обновлений. Необходимое действие следует выбрать из выпадающего списка: • **Оповестить** – При наличии обновлений в верхней части веб-страниц будет высвечиваться уведомление с предложением установки доступных обновлением (*по умолчанию*); • **Установить доступные обновления** – Обновления будут автоматически устанавливаться по мере их обнаружения.

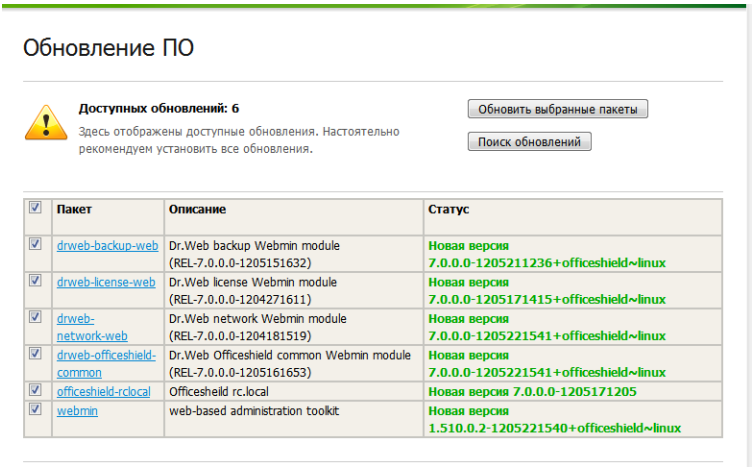
После установки значений параметров обновлений системы нажмите кнопку **Сохранить**.

При наличии доступных обновлений системы в верхней части страниц веб-интерфейса появляется соответствующее уведомление с предложением перейти на страницу

Обновление ПО.

Обновление пакетов

Если доступны пакеты для обновления, то их перечень отображается на странице **Обновление ПО**. Рекомендуется устанавливать все предложенные пакеты. Вид страницы обновления пакетов показан на рисунке ниже.



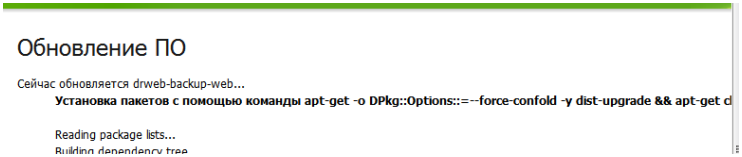
Особенностью системы установки пакетов является то, что она всегда устанавливает все пакеты вне зависимости от того, какие из них были отмечены флажками в списке

Обновление пакетов

1. Нажмите кнопку **Обновить выбранные пакеты** для запуска процесса обновления.
2. На открывшейся странице нажмите кнопку **Установить**

сейчас.

3. После нажатия кнопки **Установить сейчас** на экране откроется страница, отображающая журнал хода установки пакетов, фрагмент которой изображен на рисунке ниже:



После появления надписи "... установка завершена" процесс установки пакетов будет завершен.

Рекомендуется перезагрузить **Dr.Web Office Shield** после установки любых обновлений. Перезагрузка выполняется на странице Перезагрузка и завершение работы.

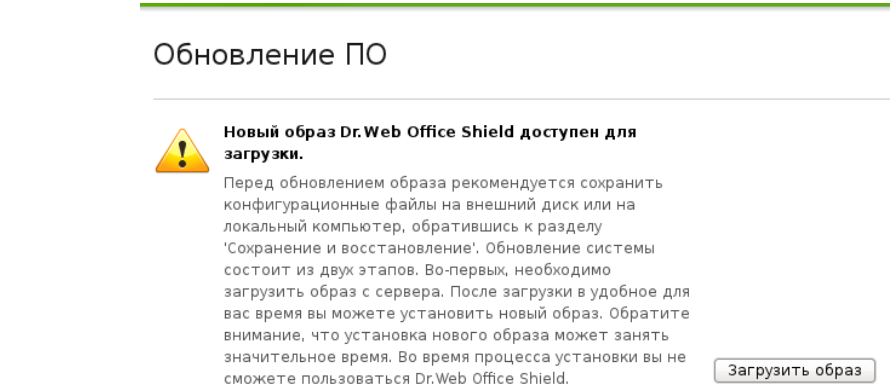
Перечень установленных пакетов и их версий доступен на странице просмотра перечня установленных пакетов.

Пожалуйста, перед перезагрузкой устройства убедитесь, что к нему **не подключен съемный накопитель USB-flash** (отсоедините его, если это не так)!

При перезагрузке устройства загрузка операционной системы **Dr.Web Office Shield** может быть остановлена из-за того, что устройство будет пытаться найти загрузчик операционной системы на вставленном съемном накопителе.

Обновление системы

Если доступен для загрузки новый образ системы, то на странице **Обновление ПО** будет выведено соответствующее уведомление, показанное на рисунке ниже.



Обновление системы рекомендуется выполнять в удобное время, поскольку оно сопряжено с перезагрузкой устройства, в течение которого оно перестанет выполнять свои сервисные функции по комплексной защите сети. Кроме того, для пользователей локальной сети (в зависимости от конфигурации) могут оказаться временно недоступны Интернет и электронная почта.

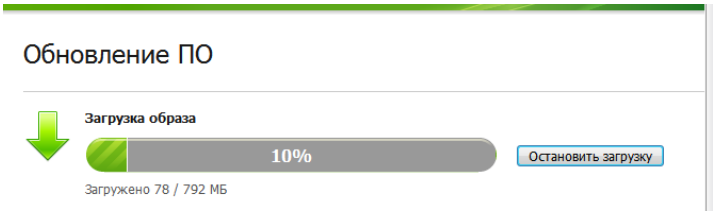
Предупреждение! После установки обновления системы все конфигурационные файлы будут перезаписаны! Перед установкой образа настоятельно рекомендуется сохранить конфигурационные файлы на странице Сохранение и восстановление, сохранив их на съемный USB-накопитель или локальный компьютер.

Обратите внимание, что после обновления образа системы ранее сохраненные настройки могут оказаться несовместимы. В этом случае их загрузка будет невозможной.

Этапы обновления системы

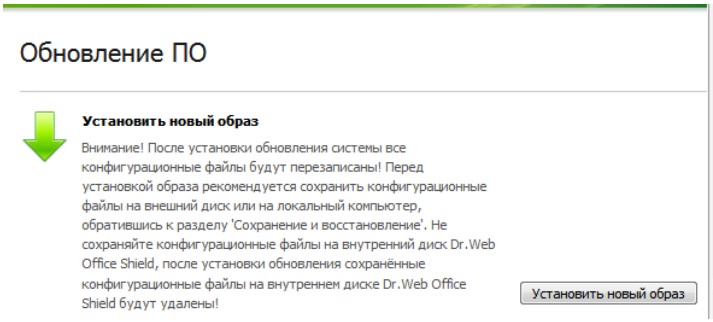
1. Загрузить образ с сервера, нажав кнопку **Загрузить образ**. В процессе загрузки образа с сервера на странице отображается индикатор загрузки и имеется возможность приостановки загрузки, для чего следует нажать кнопку **Остановить загрузку**. Для продолжения прерванной

загрузки снова нажмите кнопку **Загрузить образ**.



Загрузка образа без установки не приводит к обновлению системы. Загруженный образ сохраняется на диске, встроенном в устройство. При необходимости сохраненный образ может быть установлен позже, в более удобное время.

2. Для установки загруженного образа нажмите кнопку **Установить новый образ**. Обратите внимание, что установка нового образа не может быть прервана, образ должен быть установлен полностью, что может занять значительное время. Также обратите внимание, что перед установкой образа рекомендуется сделать резервную копию настроек.



3. После нажатия кнопки **Установить новый образ** последовательно появится окно предупреждением о том, что установка образа может занять длительное время.

   Для продолжения установки образа следует нажать кнопку **ОК**. Нажатие кнопки **Отмена** позволяет отменить

установку. В случае отмены процедуру установки можно провести позже.

Пожалуйста, перед нажатием кнопки **Установить новый образ** убедитесь, что к устройству **Dr.Web Office Shield** **не подключен съемный накопитель USB-flash** (отсоедините его, если это не так)!

При перезагрузке устройства загрузка операционной системы **Dr.Web Office Shield** может быть остановлена из-за того, что устройство будет пытаться найти загрузчик операционной системы на вставленном съемном накопителе.

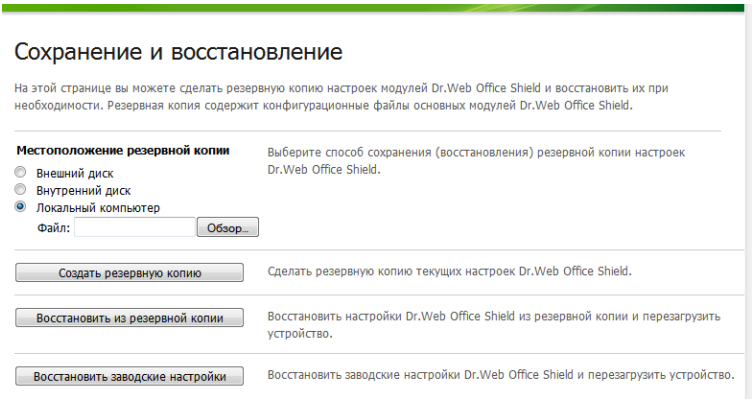
4. Во время процесса установки устройство **Dr.Web Office Shield** будет недоступно, а на экране будет выводиться индикатор установки. Если установка продолжается более 5 минут или выглядит неактивной, то перезагрузите устройство и попробуйте провести установку еще раз.
5. После установки нового образа произойдет автоматическая перезагрузка **Dr.Web Office Shield**.
6. После успешной перезагрузки восстановите ранее сохраненные настройки.
7. В случае если после загрузки образа работа системы нестабильна, выполните восстановление заводских настроек.

Сохранение и восстановление настроек

На странице **Сохранение и восстановление** производится управление резервным копированием и восстановлением из ранее сделанных резервных копий конфигурационных файлов компонентов комплекса **Dr.Web Office Shield**.

Доступ к странице сохранения и восстановления настроек осуществляется выбором пункта главного меню **Система** → **Сохранение и восстановление.** Вид страницы сохранения и

восстановления приведен на рисунке ниже.



Сохранение резервной копии настроек Dr. Web Office Shield

1. Выберите местоположение, в которое будет сохранена резервная копия настроек компонентов. Возможно использование следующих мест:
   - **Внешний диск** – копия настроек будет сохранена на съемный носитель USB, подключенный к устройству **Dr.Web Office Shield**.
   - **Внутренний диск** – копия настроек будет сохранена на диск, встроенный в устройство **Dr.Web Office Shield**.
   - **Локальный компьютер** – копия настроек будет загружена и сохранена на локальный компьютер.
2. После указания места для сохранения копии настроек нажмите кнопку **Создать резервную копию**.

Резервные копии настроек сохраняются в виде единого архива `tar.bz2`.

Восстановление настроек Dr.Web Office Shield из резервной копии

1. Выберите местоположение, из которого будет взята

ранее сохранена резервная копия настроек компонентов. Возможно использование следующих мест:

- **Внешний диск** – копия настроек будет взята со съемного носителя USB, подключенного к устройству **Dr.Web Office Shield**.
- **Внутренний диск** – копия настроек будет взята с диска, встроенного в устройство **Dr.Web Office Shield**.
- **Локальный компьютер** – копия настроек будет загружена с локального компьютера (требуется указать путь к загружаемому файлу архива `tar.bz2`, для чего следует нажать кнопку **Обзор...**).

2. После указания места, откуда должна быть загружена ранее сохраненная копия настроек, нажмите кнопку **Восстановить из резервной копии**.

Обратите внимание, что после обновления образа системы **Dr.Web Office Shield** ранее сохраненные настройки могут оказаться несовместимы. В этом случае их загрузка будет невозможной.

Если вы настроили **Антивирусную сеть Dr.Web** при помощи **Dr.Web Enterprise Server**, входящего в состав комплекса, а восстанавливаемые настройки не содержат настроек **Dr.Web Enterprise Server**, то восстановление настроек может привести к тому, что **Антивирусная сеть Dr.Web** окажется недоступной!

В случае если после восстановления настроек доступ к **Антивирусной сети Dr.Web** утрачен, выполните восстановление **Антивирусной сети Dr.Web**.

Дополнительные сведения об управлении **Антивирусной сетью Dr.Web** содержатся в Руководстве администратора **Антивирусной сети Dr.Web**, которое доступно по адресу: http://support.drweb.com/esuite/doc_ru.

Восстановление заводских настроек Dr.Web Office Shield

1. Нажмите кнопку **Восстановить заводские настройки**.

Восстановление заводских настроек приведет к тому, что

состояние всех настроек всех компонентов **Dr.Web Office Shield** будет приведено к первоначальному состоянию.

2. После восстановления настроек произойдет автоматическая перезагрузка устройства **Dr.Web Office Shield**.

После восстановления заводских настроек необходимо:

- Восстановить настройки из ранее сохраненной резервной копии;
- Выполнить обновление компонентов.

Если вы настроили **Антивирусную сеть Dr.Web** при помощи **Dr.Web Enterprise Server**, входящего в состав комплекса, то сброс устройства в заводское состояние приведет к тому, что **Антивирусную сеть Dr.Web** окажется недоступной!

В случае если восстановления заводских настроек избежать не удается, после выполнения возврата к заводским настройкам выполните восстановление **Антивирусной сети Dr.Web**.

Дополнительные сведения об управлении **Антивирусной сетью Dr.Web** содержатся в Руководстве администратора **Антивирусной сети Dr.Web**, которое доступно по адресу: http://support.drweb.com/esuite/doc_ru.

Восстановление исходного образа операционной системы

Имеется возможность восстановления (полная перезапись) исходного образа операционной системы со сбросом всех настроек, включая пароль администратора.

Для восстановления исходного образа операционной системы выполните следующее:

1. Подключите к разъемам на задней панели устройства **Dr.Web Office Shield** клавиатуру и монитор;
2. Выполните перезагрузку устройства;
3. В появившемся загрузочном меню **Grub** выберите пункт **Load system defaults**.

После восстановления исходного образа операционной системы в качестве пароля администратора будет установлено `drweb`, а настройки всех компонентов будут установлены в изначально заводские. Кроме того, обновления также будут утрачены. После выполнения восстановления исходного образа ОС необходимо:

- Загрузить лицензионные ключи;
- Сменить пароль;
- Восстановить настройки из ранее сохраненной резервной копии;
- Выполнить обновление компонентов.

Если вы настроили **Антивирусную сеть Dr.Web** при помощи **Dr.Web Enterprise Server**, входящего в состав комплекса, то сброс устройства в заводское состояние приведет к тому, что **Антивирусную сеть Dr.Web** окажется недоступной!

В случае если восстановления заводских настроек избежать не удается, после выполнения возврата к заводским настройкам выполните восстановление **Антивирусной сети Dr.Web**.

В качестве логина/ пароля доступа к **Центру управления Dr.Web** при заводских настройках устройства задано `admin/root`.

Дополнительные сведения об управлении **Антивирусной сетью Dr.Web** содержатся в Руководстве администратора **Антивирусной сети Dr.Web**, которое доступно по адресу: http://support.drweb.com/esuite/doc_ru.

Пожалуйста, перед перезагрузкой убедитесь, что к устройству **Dr.Web Office Shield** **не подключен съемный накопитель USB-flash** (отсоедините его, если это не так)!

При перезагрузке устройства загрузка операционной системы **Dr.Web Office Shield** может быть остановлена из-за того, что устройство будет пытаться найти загрузчик операционной системы на вставленном съемном накопителе.

Установка системного времени

Компьютеры используют два вида часов:

- часы с независимым питанием и всегда запущенные (аппаратное время);
- часы, которые зависят от запущенной операционной системы (системное время).

Аппаратное время используется для установки системных часов в момент загрузки ОС, после чего используется системное время до момента выключения питания компьютера.

Веб-интерфейс управления позволяет устанавливать текущее системное и аппаратное время в устройстве **Dr.Web Office Shield**, установить часовой пояс и настроить синхронизацию с выбранным сервером времени.

Доступ к странице управления системным временем осуществляется выбором пункта главного меню **Система** → **Системное время**.

Конфигурация системного времени

На странице управления системным временем доступны следующие разделы:

- Установить время — изменение текущего системного времени, используемого всеми запущенными процессами, и аппаратного времени, если оно используется операционной системой.
- Установить часовой пояс — изменение часового пояса, используемого по умолчанию, который предназначен для преобразования системного времени в удобочитаемый для человека формат.

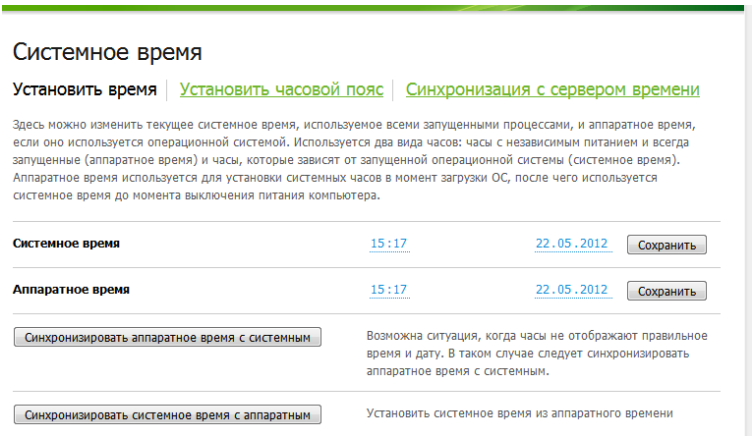
- Синхронизация с сервером времени — настройка автоматической синхронизации времени с удаленным сервером времени. Синхронизация будет осуществляться с использованием протокола UTP или NTP в зависимости от установленных настроек и возможностей удаленного сервера.

Установить время

На этой странице можно изменить текущее системное время, используемое всеми запущенными процессами, и аппаратное время, если оно используется операционной системой. Аппаратное время используется для установки системных часов в момент загрузки ОС, после чего используется системное время до момента выключения питания компьютера.

Доступ к странице установки системного временем осуществляется выбором пункта главного меню **Система** → **Системное время**. Затем на открывшейся странице необходимо выбрать вкладку **Установить время**.

Вид страницы установки системного и аппаратного времени показан на рисунке ниже.



Чтобы изменить системное или аппаратное время, щелкните мышью по соответствующей части времени (часы, минуты, день, месяц или год) и в появившееся текстовое поле введите требуемое значение.

Для сохранения внесенных изменений нажмите кнопку **Сохранить**. Сохранение изменений системного и аппаратного времени выполняется раздельно.

Синхронизация системного и аппаратного времени:

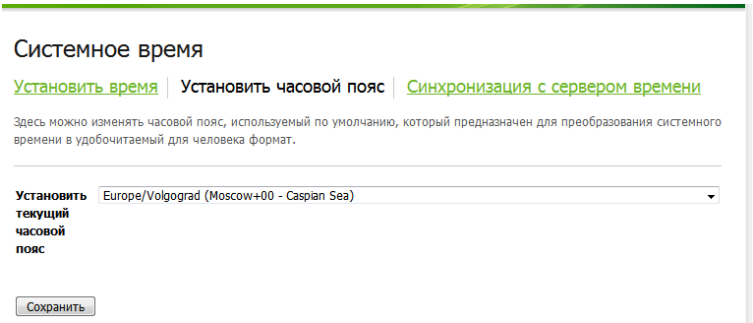
- Нажатие на кнопку **Синхронизировать системное время с аппаратным** устанавливает системное время равным аппаратному.
- Нажатие на кнопку **Синхронизировать аппаратное время с системным** устанавливает аппаратное время равным системному.

Установить часовой пояс

На этой странице можно изменить текущее изменить часовой пояс, используемый по умолчанию, который предназначен для преобразования системного времени во время локальной часовой зоны.

Доступ к странице установки часового пояса осуществляется выбором пункта главного меню **Система → Системное время**. Затем на открывшейся странице необходимо выбрать вкладку **Установить часовой пояс**.

Вид страницы установки системного и аппаратного времени показан на рисунке ниже.



Установка часового пояса

Для того чтобы установить часовой пояс:

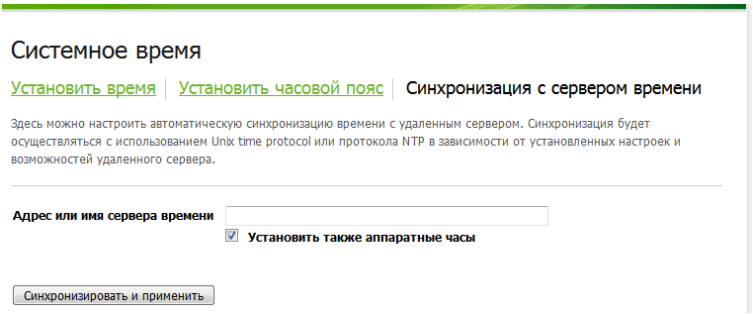
1. Выберите ваш локальный часовой пояс из выпадающего списка.
2. Нажмите на кнопку **Сохранить**.

Настроить синхронизацию с сервером времени

На этой странице можно настроить автоматическую синхронизацию системного времени с удаленным сервером времени. Синхронизация производится с использованием протокола времени UNIX или NTP в зависимости от установленных настроек и возможностей удаленного сервера.

Доступ к странице синхронизации временем с удаленным сервером времени осуществляется выбором пункта главного меню **Система** → **Системное время**. Затем на открывшейся странице необходимо выбрать вкладку **Синхронизация с сервером времени**.

Вид страницы синхронизации времени с удаленным сервером времени показан на рисунке ниже.



Настройка синхронизации с сервером времени

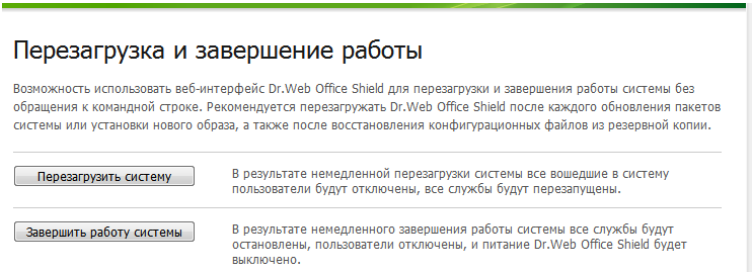
Для того чтобы настроить синхронизацию с сервером времени:

1. Введите IP-адрес или имя сервера времени, который будет использован для синхронизации.
2. Отметьте **Установить также аппаратные часы**, если необходимо синхронизировать не только системное, но и аппаратное время (в противном случае синхронизируется только системное время).
3. Нажмите на кнопку **Синхронизировать и применить**.

Перезагрузка и завершение работы

Вы можете использовать веб-интерфейс **Dr.Web Office Shield** для перезагрузки и завершения работы системы без обращения к командной строке ОС. Рекомендуется перезагружать **Dr.Web Office Shield** после каждого обновления пакетов системы или установки нового образа, а также после восстановления конфигурационных файлов из резервной копии.

Доступ к странице перезагрузки и завершения работы осуществляется выбором пункта главного меню **Система** → **Перезагрузка и завершение работы**. Вид страницы приведен на рисунке ниже.



Для перезагрузки или завершения работы системы

1. Для немедленной перезагрузки системы нажмите кнопку **Перезагрузить систему**. В результате немедленной перезагрузки системы все вошедшие в систему пользователи будут отключены, все службы на устройстве будут перезапущены.
2. Для немедленного завершения работы системы нажмите кнопку **Завершить работу системы**. В результате немедленного завершения работы системы все службы будут остановлены, пользователи отключены, и питание устройства будет выключено.

Пожалуйста, перед нажатием кнопки **Установить новый образ** убедитесь, что к устройству **Dr.Web Office Shield** **не подключен съемный накопитель USB-flash** (отсоедините его, если это не так)!

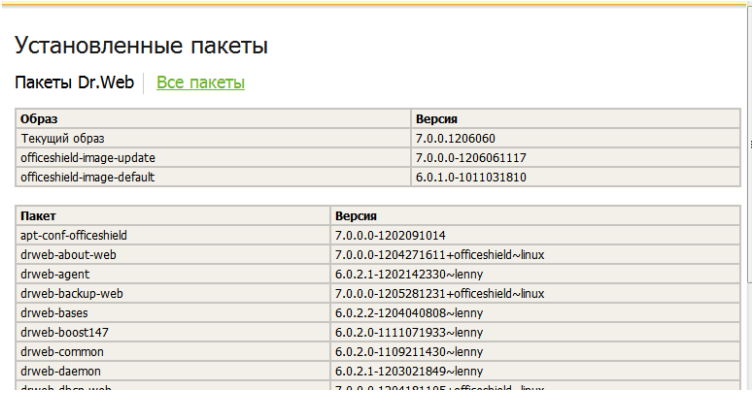
При перезагрузке устройства загрузка операционной системы **Dr.Web Office Shield** может быть остановлена из-за того, что устройство будет пытаться найти загрузчик операционной системы на вставленном съемном накопителе.

В процессе перезагрузки доступ к веб-интерфейсу будет потерян до момента полной загрузки устройства.

Перечень установленных пакетов

На странице **Установленные пакеты** отображается перечень программных пакетов, установленных в системе на текущий момент времени.

Доступ к странице просмотра перечня установленных пакетов осуществляется выбором пункта главного меню **Система** → **Установленные пакеты**. Вид страницы (фрагмент) приведен на рисунке ниже.


Установленные пакеты

Пакеты Dr.Web | Все пакеты

Образ	Версия
Текущий образ	7.0.0.1206060
officeshield-image-update	7.0.0.0-1206061117
officeshield-image-default	6.0.1.0-1011031810

Пакет	Версия
apt-conf-officeshield	7.0.0.0-1202091014
drweb-about-web	7.0.0.0-1204271611+officeshield~linux
drweb-agent	6.0.2.1-1202142330~lenny
drweb-backup-web	7.0.0.0-1205281231+officeshield~linux
drweb-bases	6.0.2.2-1204040808~lenny
drweb-boost147	6.0.2.0-1111071933~lenny
drweb-common	6.0.2.0-1109211430~lenny
drweb-daemon	6.0.2.1-1203021849~lenny

На странице отображается два списка: **список установленных образов системы** и **список установленных в системе пакетов**. В зависимости от выбранного режима просмотра, в списке пакетов отображаются только пакеты программных продуктов **Dr.Web** или все пакеты, включая пакеты системных и сервисных компонентов.

Для каждого образа и каждого пакета в списке указывается следующая информация:

- Название;
- Версия.

Образы и пакеты в списке всегда выводятся в алфавитном порядке.

Управление составом отображаемого списка пакетов:

- Чтобы вывести в списке пакетов все имеющиеся пакеты, включая пакеты системных и сервисных компонентов, щелкните мышью по вкладке **Все Пакеты**.
- Чтобы вывести в списке пакетов только пакеты, разработанные компанией **«Доктор Веб»**, щелкните мышью по вкладке **Пакеты Dr.Web**.

Обратите внимание, что в номер версии пакетов, поставляемых компанией **«Доктор Веб»**, обязательно входит дата и время их выпуска. Дата и время выпуска пакета задаются строкой вида `YYMMDDHHMM` (год, месяц, число, часы и минуты).

Компоненты

Раздел **Компоненты** главного меню веб-интерфейса **Dr.Web Office Shield** позволяет настроить работу дополнительных компонентов системы. В разделе содержатся следующие ссылки:

- Настройка Webmin — настройка параметров работы Webmin (компонента, отвечающего за функционирование веб-интерфейса **Dr.Web Office Shield**).

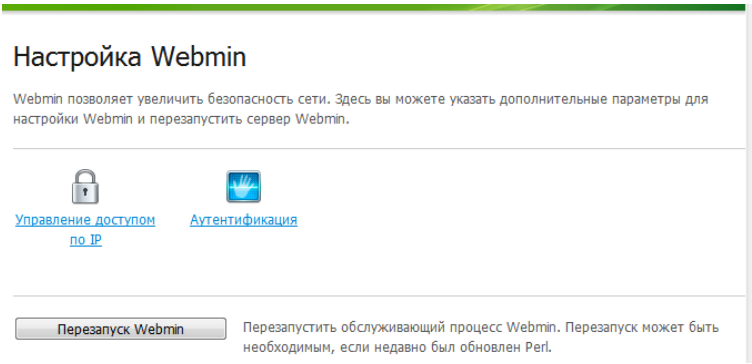
Настройка Webmin

Компонент Webmin (web-интерфейс для системного администратора UNIX) используется для работы веб-интерфейса управления **Dr.Web Office Shield**. Настройки Webmin позволяют определять уровень безопасности доступа пользователей к веб-интерфейсу управления **Dr.Web Office**

Shield.

Перед изменением настроек безопасности Webmin ознакомьтесь, пожалуйста, с Рекомендациями по обеспечению безопасности.

Доступ к странице настройки безопасности Webmin осуществляется выбором пункта главного меню **Компоненты** → **Настройка Webmin**. Вид страницы настройки Webmin приведен на рисунке ниже.



На главной странице настроек Webmin можно выбрать один из следующих разделов:

- Управление доступом по IP – Настройка доступа к интерфейсу управления **Dr.Web Office Shield** с узлов сети.
- Аутентификация – Настройка параметров аутентификации сеансов доступа к интерфейсу управления **Dr.Web Office Shield**.

После внесения изменений в разделах нажмите кнопку **Перезапуск Webmin.** Перезапуск сервера также может быть необходим, если недавно был обновлен интерпретатор Perl.

Управление доступом по IP

На этой странице вы можете ограничить доступ к серверу Webmin (а значит, и к интерфейсу управления **Dr.Web Office Shield**) с определенных узлов сети. Для определения разрешенных (запрещенных) узлов можно указать:

- Имена хостов (например foo.bar.com);
- IP-адреса (например 10.254.3.0);
- Подсети, определяющие диапазон IP-адресов (например 10.254.1.0/255.255.255.128).

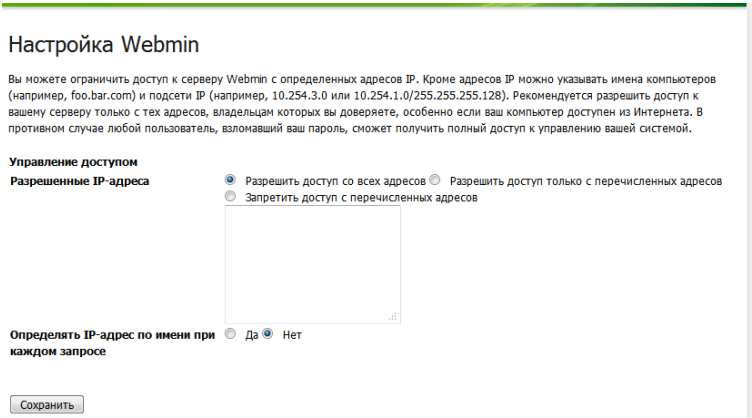
Рекомендуется разрешить доступ к интерфейсу управления **Dr.Web Office Shield** только с тех узлов сети, владельцам которых вы доверяете. В противном случае любой пользователь, взломавший ваш пароль, сможет получить полный доступ к управлению **Dr.Web Office Shield** (включая доступ к консоли ОС через SSH).

Перед изменением настроек безопасности Webmin ознакомьтесь, пожалуйста, с Рекомендациями по обеспечению безопасности.

Для доступа к странице управления доступом по IP следует:

- Выбрать пункт **Настройка Webmin** в разделе **Компоненты** главного меню;
- Перейти по ссылке **Управление доступом по IP**.

Вид страницы настройки управления доступом к Webmin по IP приведен на рисунке ниже.



На странице можно задать следующие настройки доступа:

Параметр	Описание
Разрешенные IP-адреса	Выбирается режим доступности интерфейса для различных узлов сети. Имеется возможность указать следующие режимы: • **Разрешить доступ со всех адресов** – доступ к интерфейсу управления разрешен с любого IP-адреса (*по умолчанию, но не рекомендуется*); • **Разрешить доступ только с перечисленных адресов** – доступ к интерфейсу управления будет разрешен только тем узлам, IP-адреса или имена которых перечислены в списке (*рекомендуется*). • **Запретить доступ с перечисленных адресов** – доступ к интерфейсу управления будет разрешен с любого узла, кроме тех, IP-адреса или имена которых перечислены в списке. Имена хостов, IP-адреса и IP-подсети в списке перечисляются через запятую.
Определять IP-адрес по имени	Определяется, необходимо ли производить проверку IP-адреса клиента при каждом запросе

Параметр	Описание
при каждом запросе	от него: • **Да** – При каждом запросе, поступающем от клиента будет проверяться, принадлежит ли его IP-адрес перечню разрешенных; • **Нет** – IP-адрес клиента будет проверяться только при поступлении от него первого запроса (*по умолчанию*). Включение проверки IP-адресов при каждом запросе замедляет обработку клиентских запросов.

Нажмите кнопку **Сохранить**, чтобы сохранить изменения в политике безопасности сервера.

Аутентификация

Аутентификация – это процесс проверки того, что пользователь является именно тем, за кого он себя выдает. Аутентификация сеансов доступа к интерфейсу управления позволяет следить за всеми вошедшими пользователями и отключать пользователей, неактивных в течение определенного периода времени. На этой странице вы можете изменить параметры аутентификации доступа пользователей к серверу Webmin и настроить защиту от попыток подобрать пароль методом последовательного перебора.

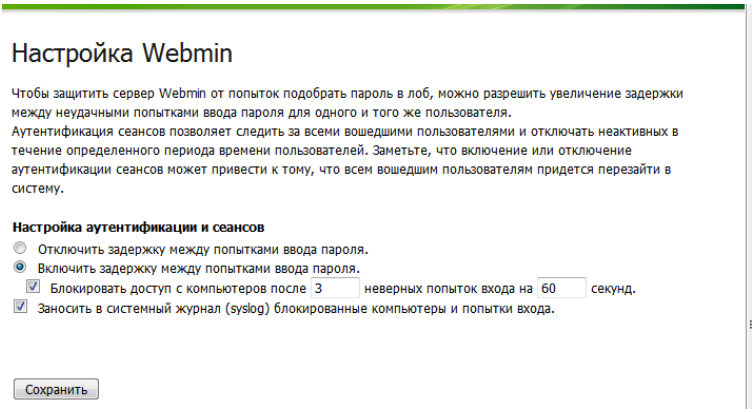
Перед изменением настроек безопасности Webmin ознакомьтесь, пожалуйста, с Рекомендациями по обеспечению безопасности.

Для доступа к странице управления аутентификацией пользователей следует:

- Выбрать пункт **Настройка Webmin** в разделе **Компоненты** главного меню;
- Перейти по ссылке **Аутентификация**.

Вид страницы настройки аутентификации пользователей

приведен на рисунке ниже.



На странице можно задать следующие настройки аутентификации:

Параметр	Описание
Включение задержки между попытками ввода пароля	Будет ли производиться задержка между попытками ввода пароля от одного и того же пользователя. Имеется возможность указать следующие режимы: • **Отключить задержку между попытками ввода пароля** – задержки между попытками ввода пароля от одного и того же пользователя; • **Включить задержку между попытками ввода пароля** – между попытками ввода пароля одним и тем же пользователем будет введена задержка в несколько секунд, что ограничит возможности по подбору пароля методом слепого перебора (*рекомендуется*).
Блокировать доступ с компьютеров	Включение блокировки доступа с IP-адресов на указанный преиод (в секундах), если с них было выполнено подряд указанное число неудачных попыток входа. Необходимо указать число неудачных попыток и величину задержки в секундах.

Параметр	Описание
Заносить в системный журнал (syslog) блокированные компьютеры и попытки входа	Будут ли неудачные попытки входа, и IP-адреса, с которых они совершались, заноситься в системный журнал (syslog) устройства **Dr.Web Office Shield**

Нажмите кнопку **Сохранить**, чтобы сохранить внесенные изменения в политику безопасности сервера.

Включение или отключение аутентификации сеансов может привести к тому, что всем вошедшим пользователям придется зайти в систему еще раз.

Доступ к настройке системы

В случае возникновения проблем с конфигурированием **Dr.Web Office Shield** посредством веб-интерфейса (например, забыт пароль или сбились сетевые настройки и веб-страницы интерфейса управления более недоступны) имеется возможность получить доступ к файлам программного комплекса через консоль операционной системы.

Для настройки компонентов через консоль операционной системы требуется обладать соответствующими навыками. Если вы не обладаете навыками работы с консолью UNIX-систем, обратитесь к системному администратору или в службу технической поддержки компании **«Доктор Веб»**.

Обратите внимание, что службе технической поддержки для устранения возникших неисправностей может потребоваться удаленный доступ к вашему устройству. В этом случае вы должны быть готовы сообщить следующую информацию:

1. Имя устройства (доступно на странице настройки подключений);
2. IP-адрес устройства в зоне LAN, а также его IP-адрес в зоне WAN (со стороны Интернета), если не используется DHCP (доступно на странице настройки подключений);
3. Заданный вами пароль для входа в веб-интерфейс управления;
4. Дополнительно может потребоваться, чтобы вы включили службу VPN и сообщили имя и пароль заданной учетной записи PPP.

Имеется два основных способа доступа к консоли операционной системы, установленной на устройстве **Dr.Web Office Shield**.

1. Непосредственное подключение к устройству

Для получения доступа к консоли операционной системы необходимо подключить к разъемам, расположенным на задней панели устройства **Dr.Web Office Shield**, монитор и клавиатуру. В случае если устройство уже загружено, на экране выведется приглашение стандартной консоли UNIX-систем. В противном случае включите устройство. При этом на экране появится меню загрузчика **GRUB**, имеющее следующие пункты:

- **Dr.Web Office Shield** – производится обычная загрузка системы.
- **Load system defaults** – позволяет восстановить и запустить образ операционной системы с заводскими (начальными) настройками всех компонентов, включая **Dr.Web Enterprise Server**. Выберите данный вариант, если система работает ошибочно, а также для восстановления пароля, если пароль был забыт.

После восстановления исходного образа операционной системы в качестве пароля администратора будет установлено `drweb`, а настройки всех компонентов будут установлены в изначально заводские. Кроме того, обновления также будут утрачены. После выполнения восстановления исходного образа ОС необходимо:

- Загрузить лицензионные ключи;
- Сменить пароль;
- Восстановить настройки из резервной копии;
- Выполнить обновление компонентов.

Если вы настроили **Антивирусную сеть Dr.Web** предприятия при помощи **Dr.Web Enterprise Server**, входящего в состав комплекса, то сброс устройства в заводское состояние приведет к тому, что **Антивирусная сеть Dr.Web** окажется недоступной!

В случае если восстановления заводских настроек избежать не удается, после выполнения возврата к заводским настройкам выполните восстановление **Антивирусной сети Dr.Web**.

В качестве логина/ пароля доступа к **Центру управления Dr.Web** при заводских настройках устройства задано `admin/root`.

Дополнительные сведения об управлении **Антивирусной сети Dr.Web** содержатся в Руководстве администратора **Антивирусной сети Dr.Web**, которое доступно по адресу: http://support.drweb.com/esuite/doc_ru.

- **Load updates** – позволяет установить и запустить последний обновленный образ системы, загруженный на устройство ранее (аналогично обновлению образа системы через веб-интерфейс).

Предупреждение! После установки обновленого образа системы все конфигурационные файлы будут перезаписаны! Перед установкой образа настоятельно рекомендуется сохранить конфигурационные файлы на странице Сохранение и восстановление, сохранив их на съемный USB-накопитель или локальный компьютер.

Обратите внимание, что после обновления образа системы ранее сохраненные настройки могут оказаться несовместимы. В этом случае их загрузка будет невозможной.

По умолчанию после ожидания (3 секунды) система выбирает и запускает 1 пункт меню (обычная загрузка). После загрузки системы на экране выведется приглашение стандартной консоли UNIX-систем.

Для начала работы вам требуется ввести пароль суперпользователя.

Пароль суперпользователя (`root`) в операционной системе, установленной в устройстве **Dr.Web Office Shield**, совпадает с паролем, используемым в веб-интерфейсе управления (по умолчанию, а также после сброса настроек – `drweb`).

2. Подключение к устройству по сети через SSH

Если настройки межсетевого экрана **Dr.Web Office Shield** не нарушены, то по умолчанию к консоли ОС, установленной на устройстве, можно подключиться через SSH. Подключение разрешено как из зоны WAN (через Интернет), так и из зоны LAN.

Для подключения к консоли устройства воспользуйтесь любым SSH-клиентом:

- в среде Windows можно воспользоваться утилитой **PuTTY** (скачать ее можно по адресу http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).
- в среде UNIX-систем воспользуйтесь командой:

  ```
  ssh <IP-address> -l root
  ```

  где `root` – имя суперпользователя, а `<IP-address>` – IP-

адрес устройства **Dr.Web Office Shield** в сети.

Для удаленного подключения к консоли операционной системы по SSH требуется знать IP-адрес устройства **Dr.Web Office Shield** в сети. Он различается для зон WAN и LAN. По умолчанию в зоне LAN устройство имеет IP-адрес `192.168.1.100`.

В случае успешного подключения к консоли устройства вам будет предложено указать пароль суперпользователя.

3. Подключение к устройству по сети с использованием VPN

Если настройки межсетевого экрана **Dr.Web Office Shield** не нарушены и включена служба частных сетей VPN, то можно создать VPN-подключение к сети. Подключение разрешено как из зоны WAN (через Интернет), так и из зоны LAN.

Для подключения к устройству выполните следующие шаги:

- Создайте VPN-подключение на клиентской машине. В качестве имени пользователя и пароля используйте логин и пароль учетной записи PPP по умолчанию (`vpn_user` и `drweb`), а в качестве IP-адреса – IP-адрес устройства **Dr.Web Office Shield** в той сети, из которой вы подключаетесь (WAN или LAN).
- После установления соединения откройте в браузере веб-интерфейс управления **Dr.Web Office Shield**. Для этого введите в адресную строку браузера адрес вида:

  ```
  https://<LAN IP-address>:10000/
  ```

  где `<LAN IP-address>` – IP-адрес устройства **Dr.Web Office Shield** в зоне LAN.

Для удаленного подключения по VPN требуется знать IP-адрес устройства **Dr.Web Office Shield** в сети. Он различается для зон WAN и LAN. По умолчанию в зоне LAN устройство имеет IP-адрес `192.168.1.100`.

В случае успешного подключения в браузере откроется страница авторизации, на которой вам будет предложено указать пароль

для доступа к веб-интерфейсу.

Дополнительно к устройству можно попытаться подключиться, используя подключение через кросс-кабель, например, при первоначальной настройке, если IP-адрес устройства, заданный по умолчанию (192.168.1.100), не входит в диапазон IP-адресов сети или если этот адрес занят другим устройством.

Рекомендации по обеспечению безопасности

В данном разделе даются рекомендации по обеспечению сетевой безопасности при использовании **Dr.Web Office Shield**.

1. При первом заходе в систему (а также после восстановления ее к заводским настройкам) смените пароль доступа.

   Помните, что этот же пароль используется для доступа к системе через консоль и по SSH. Никогда не используйте простых паролей, которые могут быть подобраны угадыванием.

2. Без необходимости не оставляйте включенной службу виртуальных частных сетей VPN. По умолчанию при поставке устройства эта служба отключена.
   - При использовании службы VPN обязательно настройте перечень учетных записей, которые могут подключаться через VPN.
   - Используйте аутентификацию подключений VPN.
   - Для разных учетных записей задавайте разные пароли и перечень разрешенных адресов.

3. Ограничьте доступ к интерфейсу управления **Dr.Web Office Shield**, разрешив его только для определенных узлов сети.

   Рекомендуется разрешить доступ к интерфейсу управления только для тех узлов сети, владельцам которых вы доверяете.

4. Защитите сервер интерфейса управления от попыток подобрать пароль методом последовательного перебора, задав задержку между неудачными попытками ввода пароля.

Техническая поддержка

Страница службы технической поддержки компании **«Доктор Веб»** находится по адресу http://support.drweb.com/.

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу http://download.drweb.com/;
- прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com/;
- попытаться найти ответ в **базе знаний Dr.Web** по адресу http://wiki.drweb.com/;
- посетить **форумы Dr.Web** по адресу http://forum.drweb.com/.

Если после этого вам не удалось решить проблему, то вы можете заполнить веб-форму вопроса в соответствующей секции раздела http://support.drweb.com/.

Найти ближайшее к вам представительство компании **«Доктор Веб»** и всю информацию, необходимую пользователю, вы можете по адресу http://company.drweb.com/contacts/moscow.

Обратите внимание, что службе технической поддержки для устранения возникших неисправностей может потребоваться удаленный доступ к вашему устройству. В этом случае вы должны быть готовы сообщить следующую информацию:

1. Имя устройства (доступно на странице настройки подключений);
2. IP-адрес устройства в зоне LAN, а также его IP-адрес в зоне WAN (со стороны Интернета), если не используется DHCP (доступно на странице настройки подключений);
3. Заданный вами пароль для входа в веб-интерфейс управления;
4. Дополнительно может потребоваться, чтобы вы включили службу VPN и сообщили имя и пароль заданной учетной записи PPP.

Лицензирование

Лицензия на использование программно-аппаратного комплекса **Dr.Web Office Shield** управляет возможностями использования следующих компонентов обеспечения безопасности, входящих в состав **Dr.Web Office Shield**:

- **Dr.Web Enterprise Server**. Обеспечивает централизованную защиту рабочих станций, файловых серверов и компьютеров корпоративной локальной сети.
- **Dr.Web Веб-прокси**. Защищает доступ пользователей внутренней интранет-сети к ресурсам сети Интернет.
- **Dr.Web Почтовый прокси**. Обеспечивает антивирусную и антиспам-защиту почтового трафика.

Лицензии определяют следующие параметры:

- Перечень доступных компонентов обеспечения безопасности;
- Срок действия услуги защиты;
- Количество защищаемых серверов и рабочих станций.

Лицензия может быть приобретена на определенный срок (например на 1, 2 или 3 года), на использование только отдельных компонентов безопасности (например, только на проверку почтового трафика при помощи **Dr.Web Почтовый прокси**), а также различаться по количеству файловых серверов и рабочих станций организации, для которых обеспечивается защита. Кроме того, существуют также условно-безлимитные лицензии, при приобретении которых количество обслуживаемых клиентов ограничивается только аппаратными возможностями устройства.

- Минимально приобретаемая лицензия для **Dr.Web Enterprise Security Suite** — на 1 файловый сервер и 10 пользователей.
- Минимально приобретаемые лицензии для **Dr.Web Веб-прокси** и **Dr.Web Почтовый прокси** — на 10 пользователей.

При покупке лицензии клиент получает возможность в течение всего срока ее действия получать обновления с серверов **Всемирной системы обновлений Dr.Web** (**ВСО Dr.Web**), а также получать стандартную техническую поддержку компании и ее партнеров.

Обратите внимание, что при истечении срока действия лицензии соответствующие компоненты безопасности (**Dr.Web Enterprise Server**, **Веб-прокси** и **Почтовый прокси**) запускаться не будут. Не забывайте своевременно продлевать действие лицензии, чтобы не оставлять рабочие станции локальной сети без антивирусной защиты.

В случае отсутствия или истечения срока действия лицензии на компоненты безопасности **Dr.Web Office Shield** может работать в качестве сетевого шлюза, отделяющего локальные сети организации от сети Интернет, если его подключить и настроить соответствующим образом.

Приобрести, продлить и изменить лицензию на использование компонентов **Dr.Web Office Shield** вы можете у наших партнеров или через интернет-магазин.

Конкретные предложения по срокам, а также по другим количественным возможностям и ограничениям, могут варьироваться для отдельных региональных партнеров компании **«Доктор Веб»**, а также могут быть в будущем пересмотрены компанией **«Доктор Веб»**. Для уточнения всех вопросов лицензирования следует обращаться к конкретному партнеру компании **«Доктор Веб»**. Контактные данные партнеров можно найти по адресу http://partners.drweb.com/.

Файлы лицензионных ключей

Права пользователя на использование **Dr.Web Office Shield** в соответствии с имеющейся лицензией регулируются при помощи набора специальных файлов, называемых файлами лицензионных ключей или *ключевыми файлами*. В зависимости от вида лицензии, клиенту может предоставляться различное

количество ключевых файлов (от 1 до 3).

Содержимое ключевого файла, регулирующие права пользователя, устанавливается в соответствии с лицензией. Файл содержит следующую информацию:

- перечень компонентов программного-аппаратного комплекса, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование компонентов;
- другие ограничения (например, количество пользователей, которые будут использовать продукт);
- сведения о пользователе и продавце продукта.

Ключевой файл **Dr.Web Office Shield** является *действительным* при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится *недействительным*, при этом выдается соответствующее предупреждение, и использование соответствующего компонента безопасности из комплекта **Dr.Web Office Shield**, регулируемое данным ключевым файлом, становится невозможным.

Ключевой файл имеет формат, защищенный от редактирования при помощи механизма электронной подписи. Редактирование файла делает его недействительным. Поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.

Также обратите внимание, что компания **«Доктор Веб»** может *заблокировать* любой ключевой файл в случае его дискредитации, то есть при выявлении факта его незаконного распространения. Блокировка осуществляется на серверах обновлений, поэтому при блокировке ключевого файла вы не

сможете получать обновления вирусных баз и компонентов **Dr. Web Office Shield**. В случае блокировки вашего ключевого файла свяжитесь с технической поддержкой компании **«Доктор Веб»**.

Дополнительную информацию о лицензировании и ключевых файлах можно найти на официальном сайте компании **«Доктор Веб»** по адресу http://www.drweb.com.

Получение файлов лицензионных ключей

Поскольку ключевые файлы обеспечивают предоставление услуг в соответствии с действующим лицензионным соглашением, для получения ключевых файлов требуется серийный номер лицензии.

Для получения файлов лицензионных ключей необходимо:

1. После получения лицензионного сертификата зарегистрируйте указанный в нем серийный номер на сайте компании **«Доктор Веб»**: http://products.drweb.com/register. В результате для данного серийного номера будет создан набор необходимых лицензионных ключевых файлов.
2. Архив с набором созданных ключевых файлов будет выслан на указанный вами при регистрации адрес электронной почты.
3. Полученный набор ключевых файлов необходимо разархивировать и сохранить на локальный диск или съемный накопитель USB.

Отсчет срока действия лицензии начинается с момента регистрации серийного номера и получения ключевого файла.

Рекомендуется сохранять полученные файлы лицензионных ключей до истечения срока действия лицензии. В случае

утраты ключевых файлов можно использовать ту же процедуру, что и при активации лицензии: повторно ввести регистрационный серийный номер и адрес электронной почты, на который будет выслан набор ключевых файлов, соответствующий лицензии.

Регистрация с одним и тем же регистрационным серийным номером допускается **не более 25 раз**!

При необходимости восстановить утерянный лицензионный ключевой файл после 25 регистраций следует разместить по адресу в Интернете http://support.drweb.com/request запрос на восстановление ключевого файла, указать данные, введенные при регистрации, адрес электронной почты и подробно описать ситуацию.

Запрос будет рассмотрен специалистами службы технической поддержки, и в случае положительного решения ключевой файл будет либо выдан через автоматизированную систему поддержки пользователей, либо выслан по электронной почте.