Оглавление

1 Введение

В данном документе описываются основные страницы Web-интерфейса управления ПТК «ТИТАН КОНТРОЛ 1000». Web-интерфейс управления является стандартной (используемой по умолчанию) системой Web-управления для операционной системы OpenWrt (https://openwrt.org/)

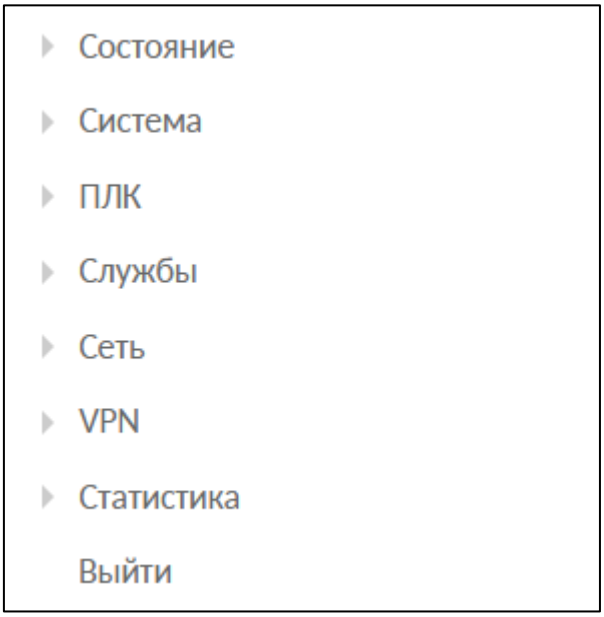


Рисунок 1-1: Главное меню Web-интерфейса управления LuCI

В разделе 2 (раздел меню «Состояние») собраны описания страниц, отображающих различную информацию о системе в целом, и информационные страницы конкретных служб или приложений. В частности, в данном разделе описаны страницы просмотра состояния межсетевого экрана (раздел 2.3), активных маршрутов и правил (раздел 2.2), различных журналов (раздел 2.6), и страницы для просмотра графиков в реальном времени для некоторых системных параметров (раздел 2.5).

В разделе 3 (раздел меню «Система») сконцентрированы описания страниц управления различными системными параметрами. Например, такими, как текущие дата и время, настройки клиента и сервера NTP, управление доступом к системе по SSH протоколу, управление SSH ключами, управление службой сторожевого таймера (watchdog), управление мониторированием разделов, управление резервным копированием. В разделе «Система» также описан функционал обновления прошивки устройства (см.

раздел 4.7) и функционал доступа к терминалу устройства через службу веб-терминала (см. раздел 4.8).

В разделе 4 (раздел меню «ПЛК») описаны страницы для настройки и мониторинга функций ПЛК устройства. В частности, здесь описываются страницы с отображением веб-визуализации пользовательского приложения CODESYS (см. раздел 5.1), настройки CODESYS (см. раздел 5.2), страница просмотра журналов CODESYS (см. раздел 5.5) и также страницы с подробной информацией о запущенном в текущий момент пользовательском приложении CODESYS (см. раздел 5.4).

В разделе 5 (раздел меню «Службы») содержатся страницы настройки различных служб и приложений. Например, HTTP-сервер, служба STP/RSTP, служба DDNS, FTP-сервер.

В разделе 6 (раздел меню «Сеть») описаны страницы управления сетевыми параметрами системы (настройка сетевых интерфейсов, настройка статических маршрутов и т. п.) и такими базовыми сетевыми службами, как DNS и DHCP. Также в данном разделе приводится описание настройки межсетевого экрана и описание использования диагностических сетевых утилит (ping, traceroute, nslookup), для которых в LuCI реализован интерфейс.

В разделе 8 (раздел меню «Статистика») содержатся страницы просмотра графиков службы статистики collectd и RRDtool для их визуализации, а также страницы настройки данных службы.

1.1 Подключение к Web-интерфейсу

При первом подключении к Web-интерфейсу по протоколу HTTP будет отображена страница аутентификации с полями для ввода имени пользователя и пароля, как показано на рисунке 1-2.

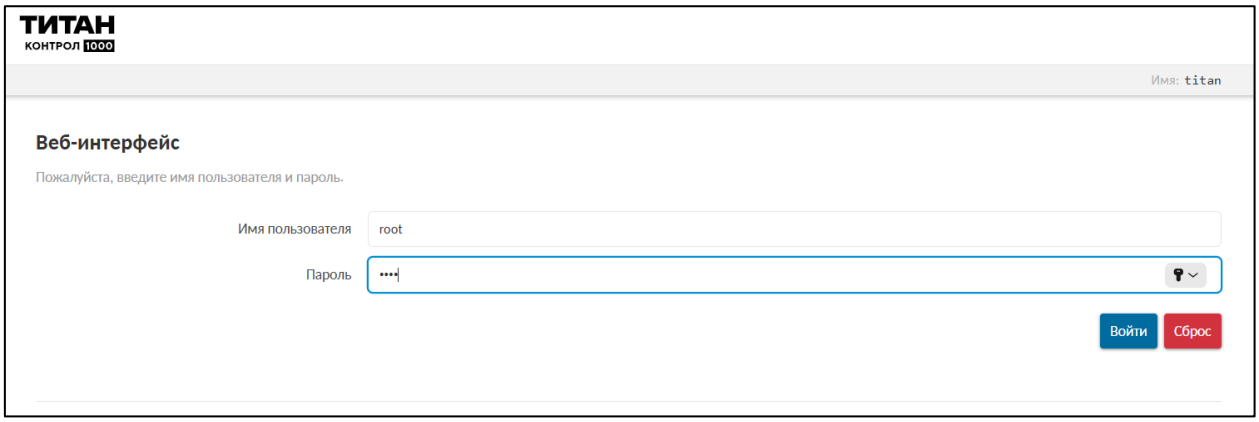


Рисунок 1-2: Страница аутентификации

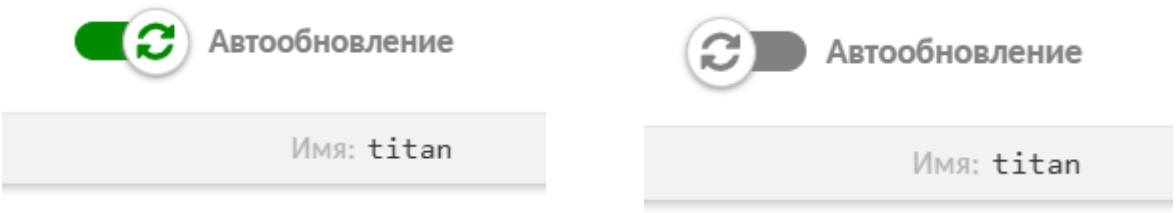
По умолчанию, для аутентификации необходимо использовать следующие учётные данные:

Имя пользователя	root
Пароль	root

Настройка пароля пользователя «root» с использованием Web-интерфейса LuCI рассмотрена в разделе 4.3.1 данного руководства. Кроме того, настройка пароля пользователя «root» может быть выполнена в ходе настройки устройства при помощи мастера настройки, который описывается в разделе 2 данного руководства.

1.2 Автоматическое обновление информации

На многих страницах веб-интерфейса реализована функция автоматического обновления данных в реальном времени. Если на странице используется данная функция, то в заголовке страницы справа от главного меню будет присутствовать надпись «Автообновление» со значком зеленого цвета (см. рисунок 1-3(a)). Автоматическое обновление данных может быть отключено путём нажатия на значок. В этом случае цвет значка изменится на серый, как показано на рисунке 1-3(b).



(а) Автоматическое обновление включено (б) Автоматическое обновление выключено

Рисунок 1-3: Автоматическое обновление данных страницы

Интервал автоматического обновления информации по умолчанию равен 5 секундам и может быть настроен в вкладке «Дополнительные» страницы «Общие настройки» раздела главного меню «Система» (см. раздел 3.1.4).

2 Состояние

2.1 Обзор

На странице «Обзор» раздела «Состояние» отображается сводная информация о текущем состоянии устройства. Внешний вид страницы «Обзор» показан на рисунке 2-1.

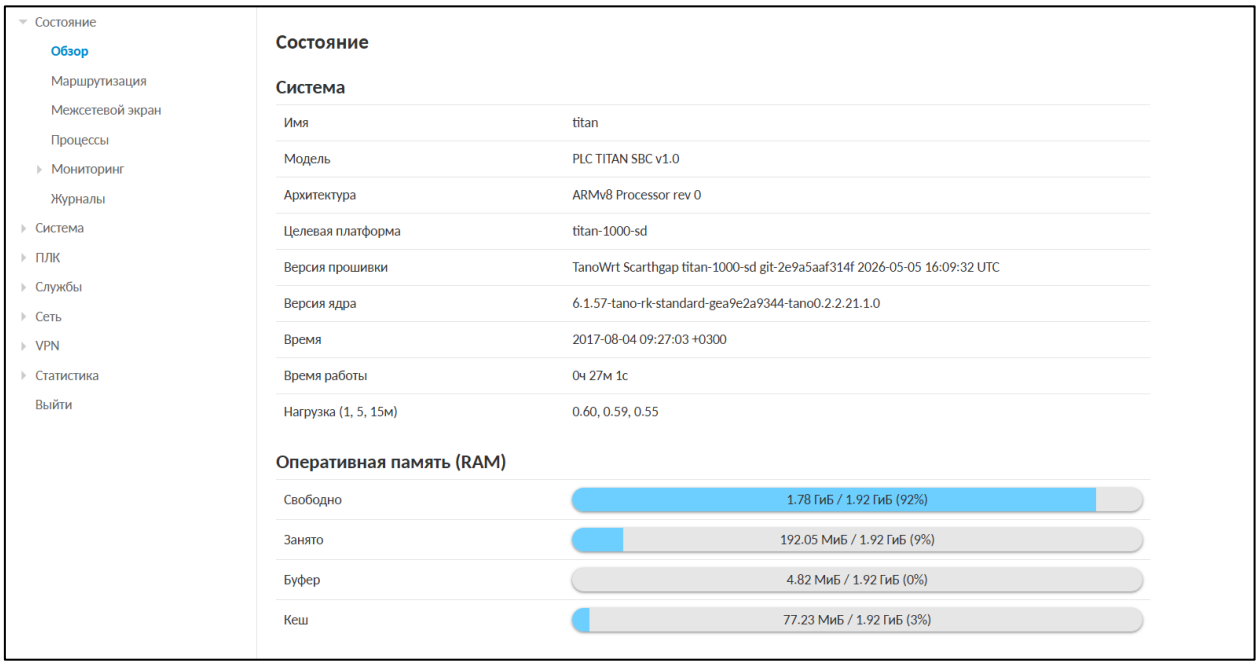


Рисунок 2-1: Страница «Обзор»

Страница «Обзор» разделена на несколько подразделов:

- «Система» (см. раздел 2.1.1);
- «ПЛК» (см. раздел 2.1.2);
- «Оперативная память (RAM)» (см. раздел 2.1.3);
- «Состояние портов сетевых интерфейсов» (см. раздел 2.1.4);
- «Сеть» (см. раздел 2.1.5);
- «Активные DHCP аренды» (см. раздел 2.1.6).

2.1.1 Подраздел «Система»

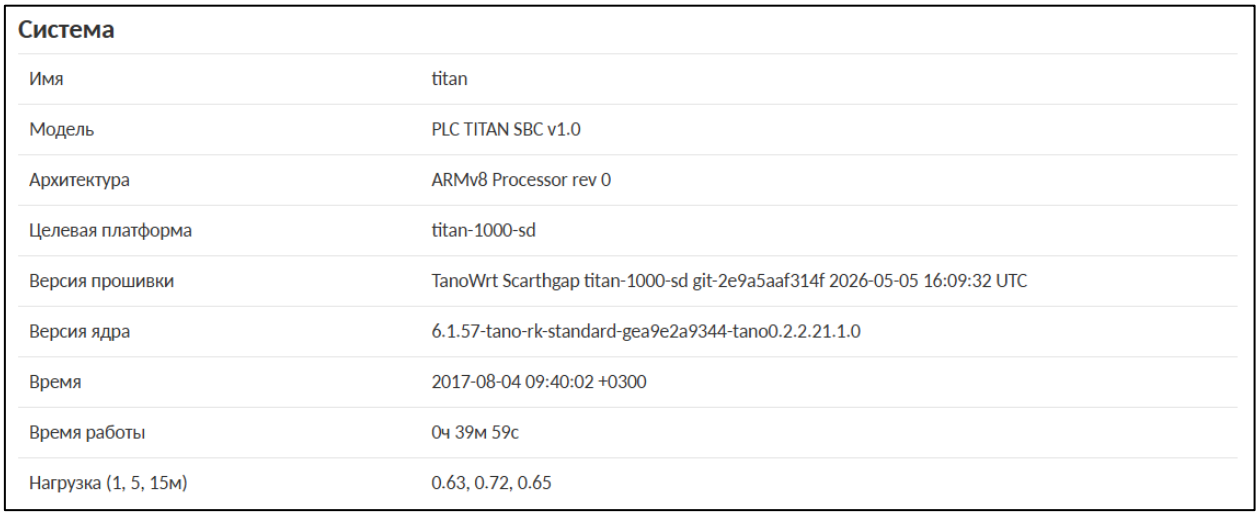


Рисунок 2-2: Состояние. Подраздел «Система»

В подразделе «Система» страницы «Обзор» (см. рисунок 2-2) приводятся основные параметры системы:

- «Имя» — имя системы (имя хоста);
- «Модель» — модель устройства;
- «Архитектура» — модель и архитектура процессора;
- «Целевая платформа» — операционная среда контроллера;
- «Версия прошивки» — версия прошивки;
- «Версия ядра» — версия ядра операционной системы;
- «Время» — текущее дата и время;
- «Время работы» — время работы устройства (с момента включения);
- «Нагрузка» — текущее значение средней нагрузки (средние значения за 1, 5 и 15 минут);

2.1.2 Подраздел «Оперативная память (RAM)»

В подразделе «Оперативная память (RAM)» страницы «Обзор» приводится информация о занятой и свободной оперативной памяти устройства в виде шкалы, как показано на рисунке 2-3.

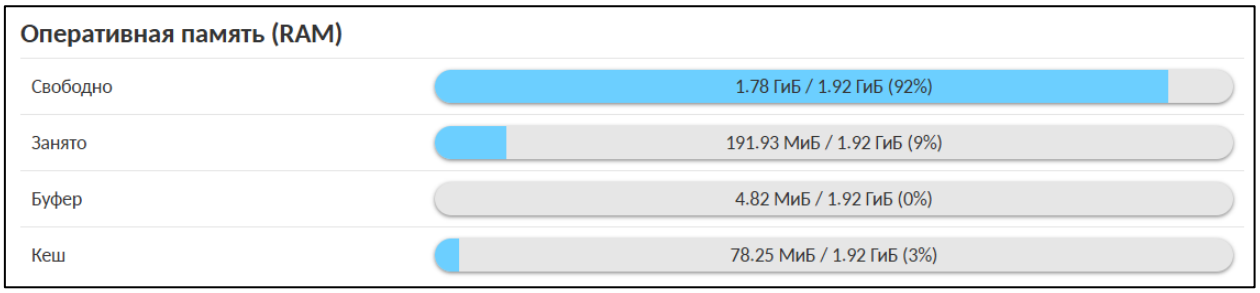


Рисунок 2-3: Состояние. Подраздел «Оперативная память (RAM)»

2.1.3 Подраздел «Состояние портов сетевых интерфейсов»

В подразделе «Состояние портов сетевых интерфейсов» страницы «Обзор» приводится таблица всех портов сетевых интерфейсов в виде таблицы (см. рисунок 2-4).

Рисунок 2-4: Состояние. Подраздел «Состояние портов сетевых интерфейсов»

Каждая строка таблицы соответствует одному физическому сетевому интерфейсу. Таблица имеет следующие столбцы:

– «Имя и MAC-адрес» — имя сетевого порта и MAC-адрес физического интерфейса порта;

– «Состояние подключения» — текущее состояние подключения сетевого интерфейса. Также отображается информация о скорости и дуплексе подключений, если такая информация доступна для данного интерфейса. Дополнительно, в данном столбце отображаются имена портов, которые определяют тип и текущее состояние подключений. Возможные типы и состояния подключений приведены в таблице 3-1.

– «Интерфейс» — имя системного сетевого интерфейса порта. В скобках указывается имя виртуального сетевого интерфейса, к которому

привязан системный интерфейс (если такой интерфейс есть). При этом имя виртуального интерфейса может быть указано в качестве имени сети или в качестве имени узла сети.

– «В составе моста» — имя системного сетевого интерфейса моста, в который включён данный порт. В скобках указывается имя виртуального сетевого интерфейса, к которому привязан системный сетевой интерфейс (если таковой имеется). При нажатии на имя виртуального интерфейса произойдёт переход к странице настройки соответствующего сетевого интерфейса (см. раздел 7.1.1).
– «Зоны межсетевого экрана» — перечисление всех зон межсетевого экрана, в которые включён интерфейс;
– «Получение (RX)» — количество принятых байт (пакетов) через данный интерфейс;
– «Отправка (TX)» — количество отправленных байт (пакетов) через данный интерфейс.

Таблица 3-1: Иконки типов и состояний подключений портов сетевых интерфейсов

Тип подключения	Состояние подключения		
	Отключено	Не подключено	Подключено
Проводное подключение			
Беспроводное Wi-Fi подключение			
Беспроводное LTE/3G/2G подключение			
USB RNDIS подключение			
VPN подключение			
PPP подключение			

2.1.4 Подраздел «Хранилище»

В подразделе «Хранилище» страницы «Обзор приводится информация об использовании дискового пространства и временного хранилища в виде шкалы, как показано на рисунке 2-5.

Рисунок 2-5: Состояние. Подраздел «Хранилище»

2.1.5 Подраздел «Сеть»

В подразделе «Сеть» страницы «Обзор» приводится информация об основных сетевых интерфейсах в виде блоков, как показано на рисунке 3-9.

Рисунок 2-6: Состояние. Подраздел «Сеть»

Кроме того, внизу подраздела «Сеть» страницы «Обзор» отображается текущее и максимально возможное количество сетевых соединений в виде шкалы (см рисунок 2-6).

2.1.6 Подраздел «Активные DHCP аренды»

В подразделе «Активные DHCP аренды» страницы «Обзор» приводится таблица активных арендованных DHCP адресов (см. рисунок 2-7).

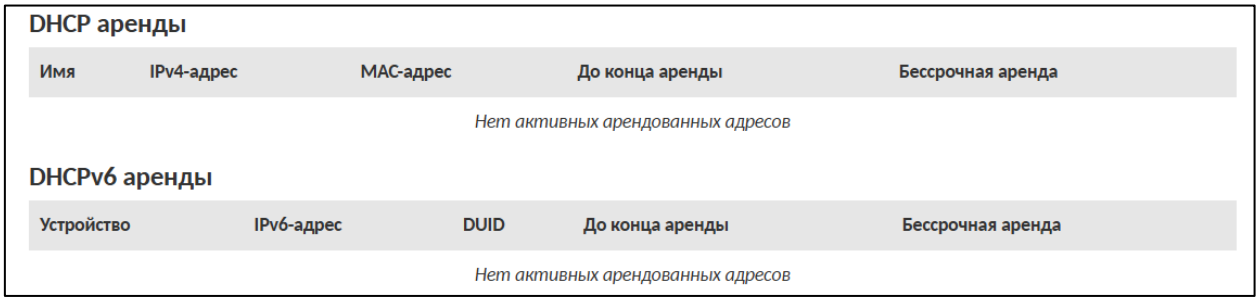


Рисунок 2-7: Состояние. Подраздел «Активные DHCP аренды»

В таблице показаны арендованные IPv4-адреса и IPv6-адреса. Каждая строка таблицы соответствует одному арендованному адресу. Таблица имеет следующие столбцы:

– «Имя» — имя хоста клиента, которому выдан адрес в аренду;
– «IPv4-адрес» — IPv4/IPv6 адрес, выданный клиенту в аренду;
– «MAC-адрес» — аппаратный MAC адрес клиента, получившего адрес в аренду;
– «DUID» — уникальный идентификатор клиента, получившего адрес в аренду;
– «До конца аренды» — оставшееся время аренды выданного адреса;
– «Бессрочная аренда» — столбец активен, если аренда выдана бессрочно.

2.2 Маршрутизация

На странице «Маршрутизация» раздела «Состояние» отображаются текущие IPv4 и IPv6 таблицы маршрутизации. Также на странице приведена текущая ARP таблица (таблица соответствия MAC-адресов IP-адресам). Внешний вид страницы «Маршруты» для IPv4-маршрутизации показан на рисунке 2-8.

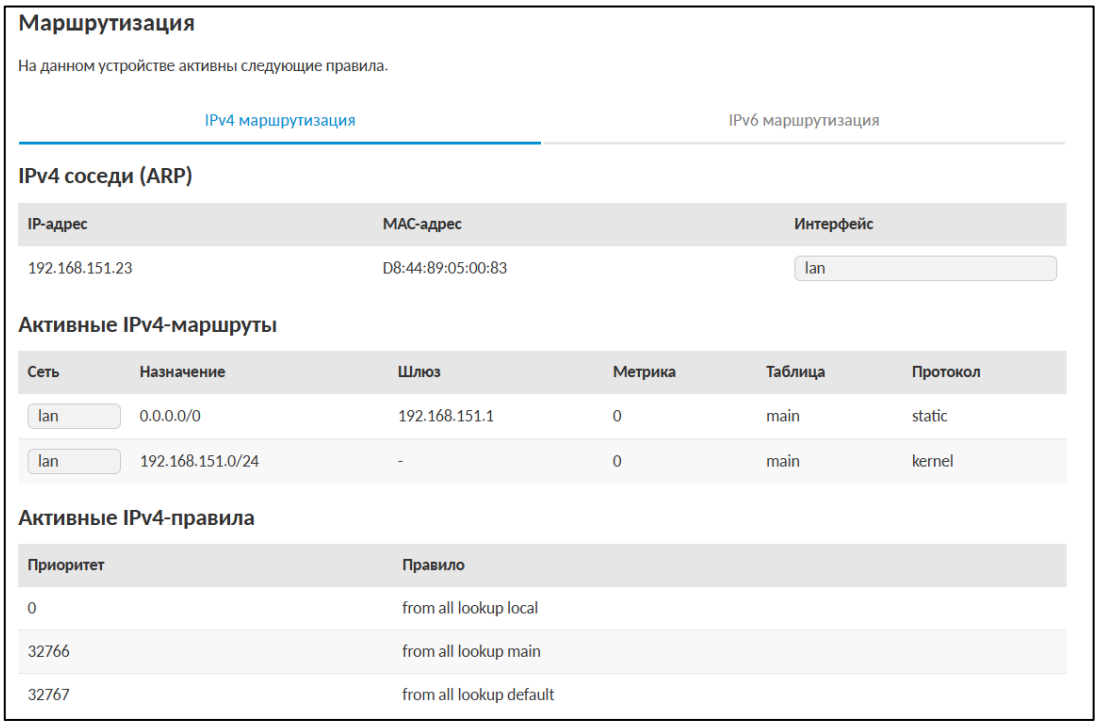


Рисунок 2-8: Страница «Маршруты»

Добавить статические IPv4 или IPv6 маршруты можно на странице «Маршруты» раздела «Сеть» (см. раздел 7.4).

2.3 Межсетевой экран

На странице «Межсетевой экран» раздела «Состояние» отображаются активные правила межсетевого экрана для всех таблиц (Filter, NAT, Mangle) и их цепочек. Внешний вид страницы «Межсетевой экран» показан на рисунке 2-9.

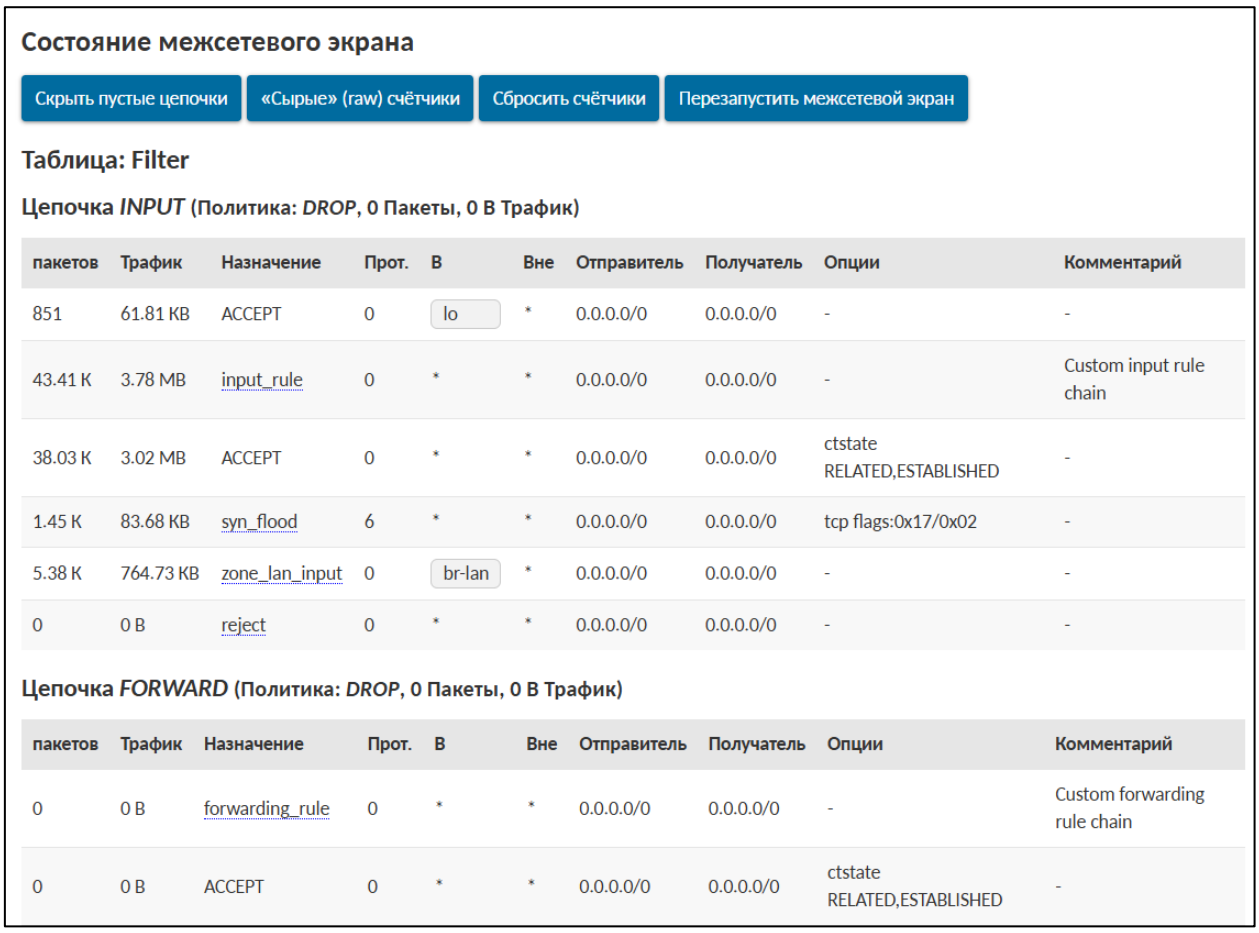


Рисунок 2-9: Страница «Межсетевой экран»

Управление межсетевым экраном (редактирование и добавление правил) осуществляется на странице «Межсетевой экран» раздела «Сеть» (см. раздел 7.5).

2.4 Процессы

Страница «Процессы» раздела «Обзор» (или соответствующего раздела) отображает список работающих в системе процессов и их основные параметры. Внешний вид страницы «Процессы» показан на рисунке 2-10.

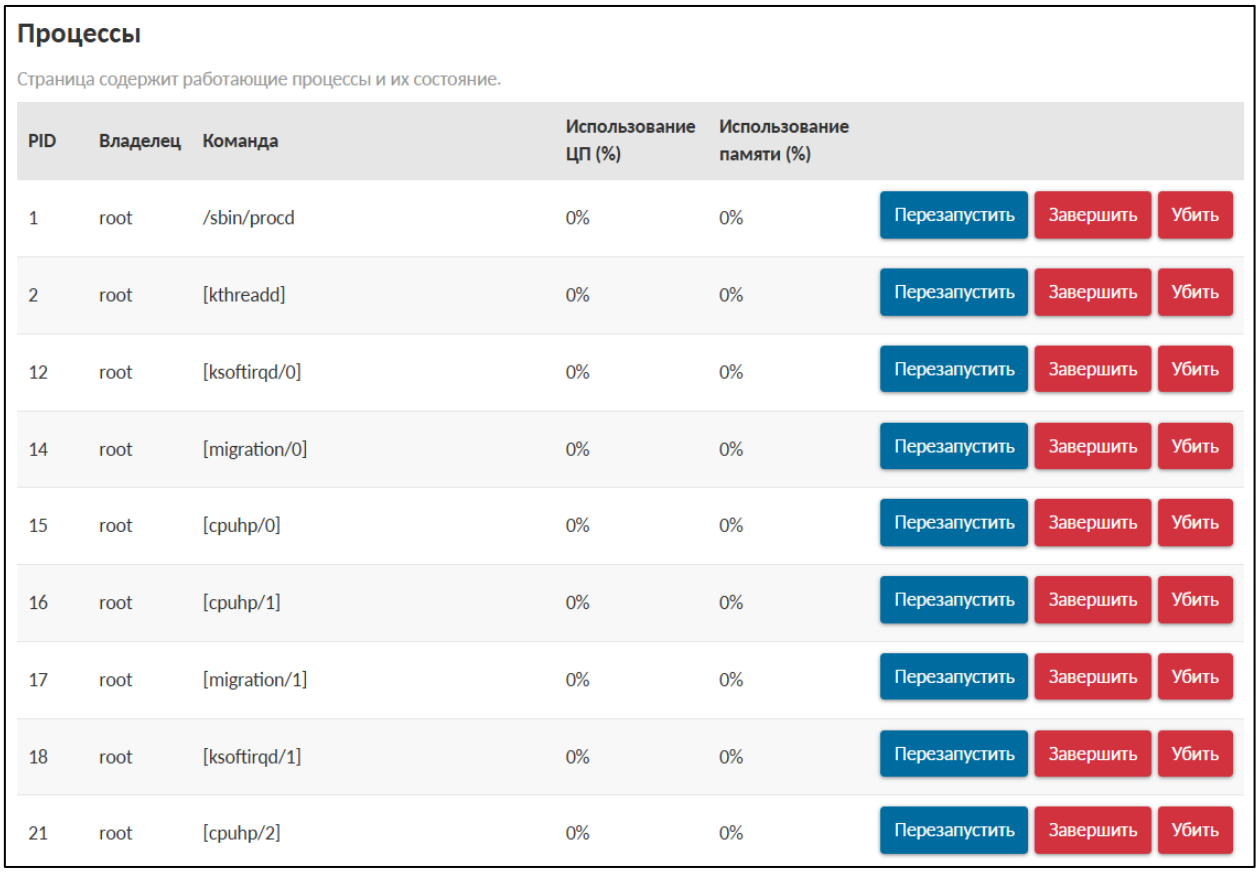


Рисунок 2-10: Состояние. Подраздел «Сеть»

Таблица имеет следующие столбцы:

- «PID» — идентификатор процесса;
- «Владелец» — пользователь, от имени которого запущен процесс;
- «Команда» — имя исполняемого файла или команда, запустившая процесс;
- «Использование ЦП (%)» — процент использования процессорного времени данным процессом;
- «Использование памяти (%)» — процент использования оперативной памяти данным процессом.

В нижней части страницы расположены кнопки управления процессами:

- «Перезапустить» — выполняет перезапуск выбранного процесса;

– «Завершить» — отправляет выбранному процессу сигнал завершения (SIGTERM);
– «Убить» — принудительно завершает выбранный процесс (SIGKILL).

2.5 Мониторинг

Страница «Мониторинг» раздела «Обзор» отображает графики и параметры системной нагрузки, сетевого трафика и активных соединений в реальном времени. Внешний вид страницы показан на рисунках 2-11 и 2-12.

Страница разделена на три подраздела: «Нагрузка», «Трафик» и «Соединения».

2.5.1 Подраздел «Нагрузка»

В подразделе «Нагрузка» отображается график средней загрузки системы за 1, 5 и 15 минут. График построен с временным окном 2 минуты и интервалом обновления 3 секунды.

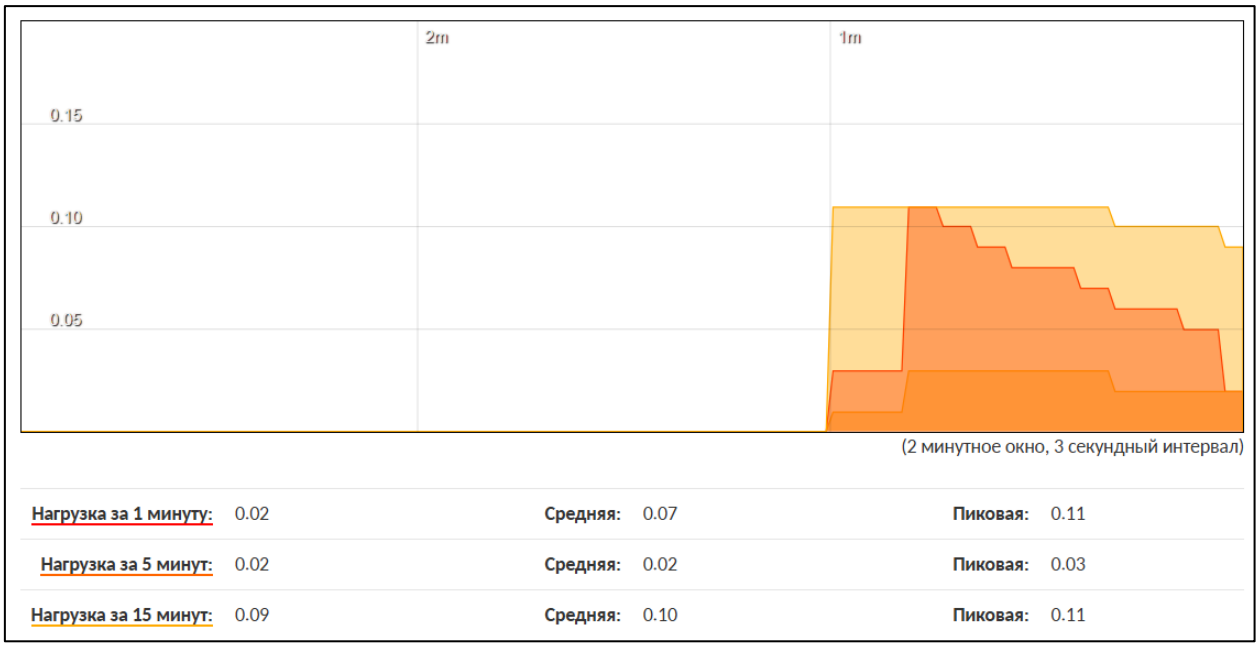


Рисунок 2-11: Мониторинг. Подраздел «Нагрузка»

Ниже графика приводятся числовые значения средней и пиковой нагрузки для каждого из трёх интервалов:

– «Нагрузка за 1 минуту» — текущее значение, среднее и пиковое значение нагрузки за последнюю минуту;

– «Нагрузка за 5 минут» — текущее значение, среднее и пиковое значение нагрузки за последние 5 минут;
– «Нагрузка за 15 минут» — текущее значение, среднее и пиковое значение нагрузки за последние 15 минут.

2.5.2 Подраздел «Трафик»

В подразделе «Трафик» отображается график входящего и исходящего трафика для выбранного сетевого интерфейса (br-lan, can0, eth0, eth1 и др.). График построен с временным окном 2 минуты и интервалом обновления 3 секунды.

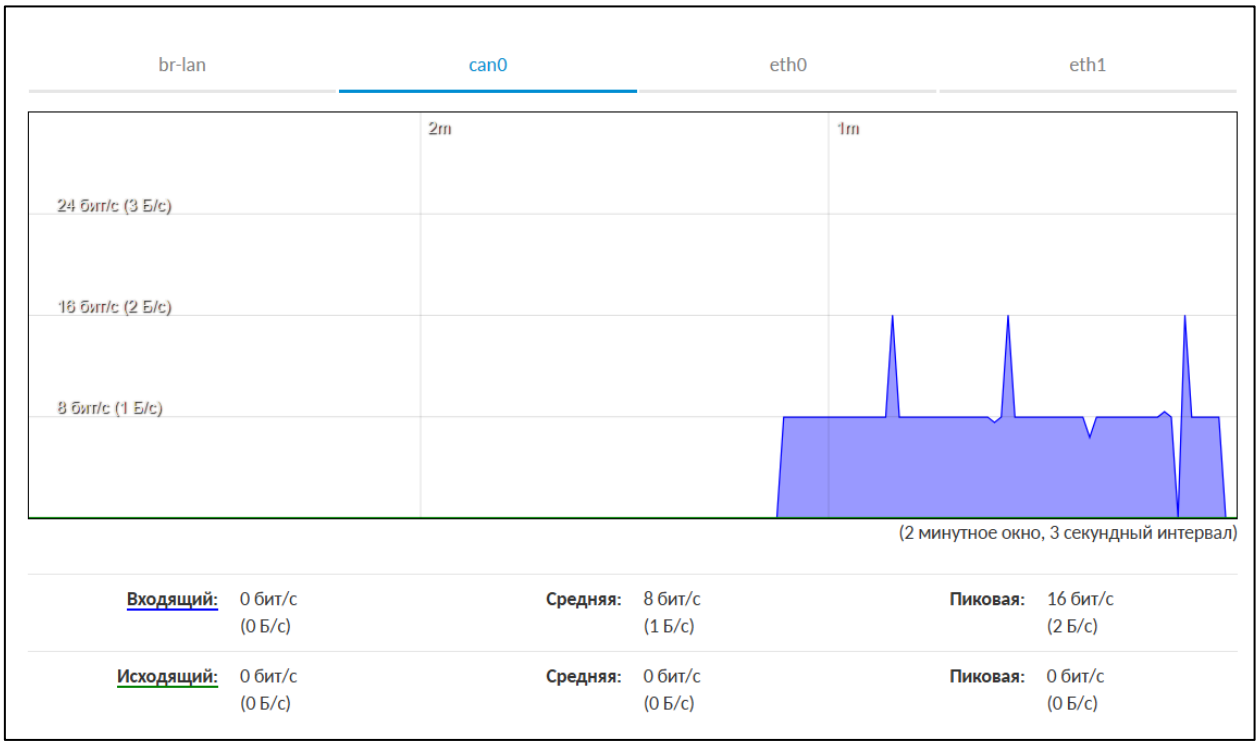


Рисунок 2-12: Мониторинг. Подраздел «Трафик»

Ниже графика приводятся числовые значения для входящего и исходящего трафика:

– «Входящий» — текущая скорость входящего трафика;
– «Средняя» — средняя скорость входящего трафика за период наблюдения;
– «Пиковая» — максимальная скорость входящего трафика за период наблюдения;

Аналогичные значения отображаются для исходящего трафика.

2.5.3 Подраздел «Соединения»

В подразделе «Соединения» (см. рисунок 2.13) отображается график количества активных сетевых соединений с разбивкой по протоколам (UDP, TCP, Другие). График построен с временным окном 2 минуты и интервалом обновления 3 секунды.

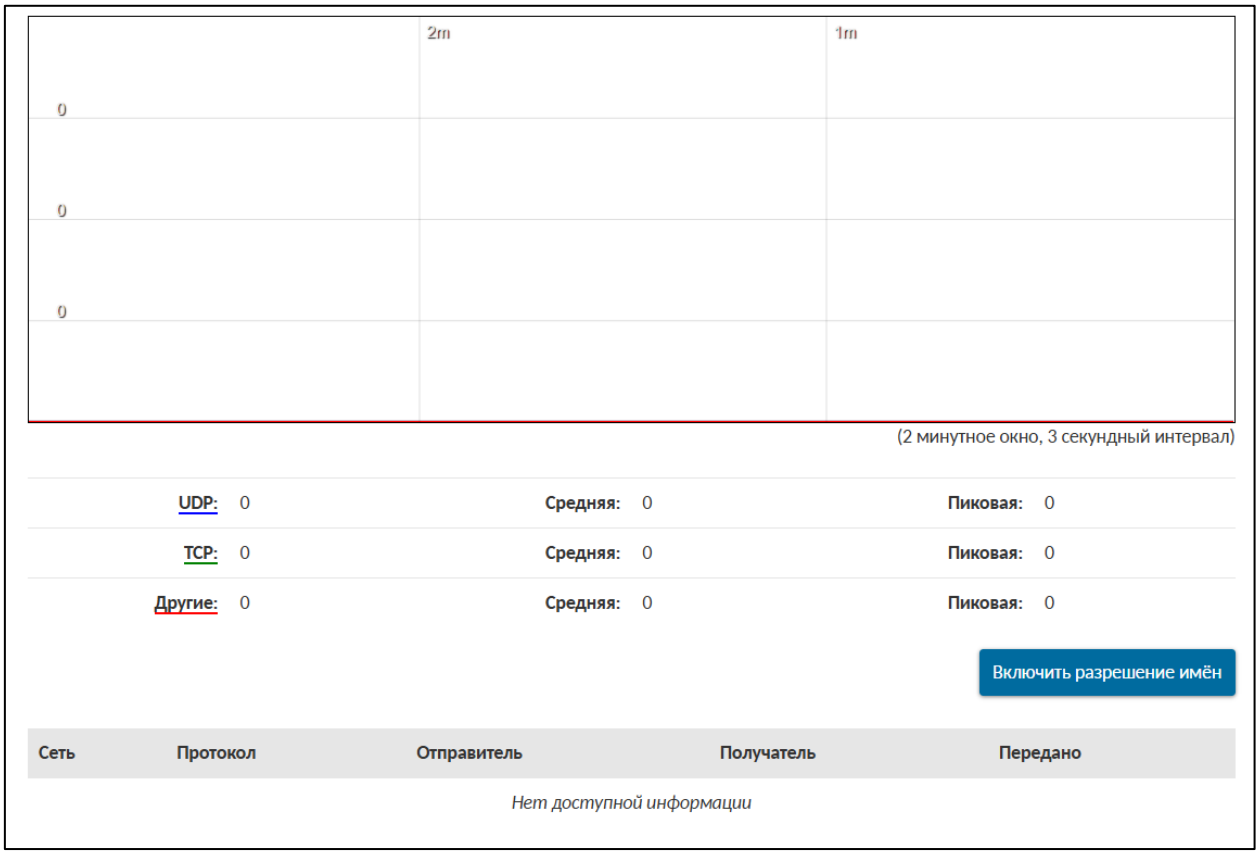


Рисунок 2-13: Мониторинг. Подраздел «Соединения»

Ниже графика приводятся числовые значения для каждого типа соединений:

- «UDP» — текущее, среднее и пиковое количество активных UDP-соединений;
- «TCP» — текущее, среднее и пиковое количество активных TCP-соединений;
- «Другие» — текущее, среднее и пиковое количество активных соединений по прочим протоколам.

Ниже расположена опция «Включить разрешение имён», которая позволяет выполнять обратное DNS-разрешение IP-адресов в таблице активных соединений.

Таблица активных соединений содержит следующие столбцы:

- «Сеть» — тип сети (IPv4/IPv6);
- «Протокол» — транспортный протокол (TCP, UDP и т.д.);
- «Отправитель» — IP-адрес и порт источника;
- «Получатель» — IP-адрес и порт назначения;
- «Передано» — объём переданных данных.

При отсутствии активных соединений в таблице отображается сообщение «Нет доступной информации».

2.6 Журналы

Страница «Журналы» раздела «Состояние» предназначена для просмотра системных журналов различных служб.

Страница содержит подразделы для переключения между различными журналами:

- «Журнал ядра» (см. раздел 2.6.1);
- «Системный журнал» (см. раздел 2.6.2);
- «Запланированные задания (cron)» (см. раздел 2.6.3);
- «SNMP» (см. раздел 2.6.4).

Для каждого журнала доступны следующие элементы управления и настройки отображения:

- «Отображать по убыванию времени (последнее сверху)» — при включении данной опции самые свежие записи отображаются в начале таблицы.
- «Отображать приоритеты» — позволяет фильтровать записи журнала по уровню важности (Info, Notice, Error, Debug, Warning и др.). Рядом с каждым приоритетом указывается количество записей с данным уровнем.

– «Отображать столбцы» — позволяет выбрать, какие колонки будут отображаться в таблице записей. Доступные столбцы могут включать:
  - «№» — порядковый номер записи;
  - «Время» / «Временная метка» — время регистрации события;
  - «Приоритет» — уровень важности события;
  - «Сообщение» — текст события;
– «Фильтр записей» — поле для текстового поиска по записям журнала. Пользователь может ввести строку для фильтрации.

В таблице журнала отображаются записи с соответствующими столбцами.

2.6.1 Подраздел «Журнал ядра»

На странице «Журнал ядра» раздела «Состояние» отображается вывод журнала ядра, в который записываются сообщения работы ядра Linux, начиная с момента загрузки. Внешний вид страницы «Журнал ядра» показан на рисунке 2-14.

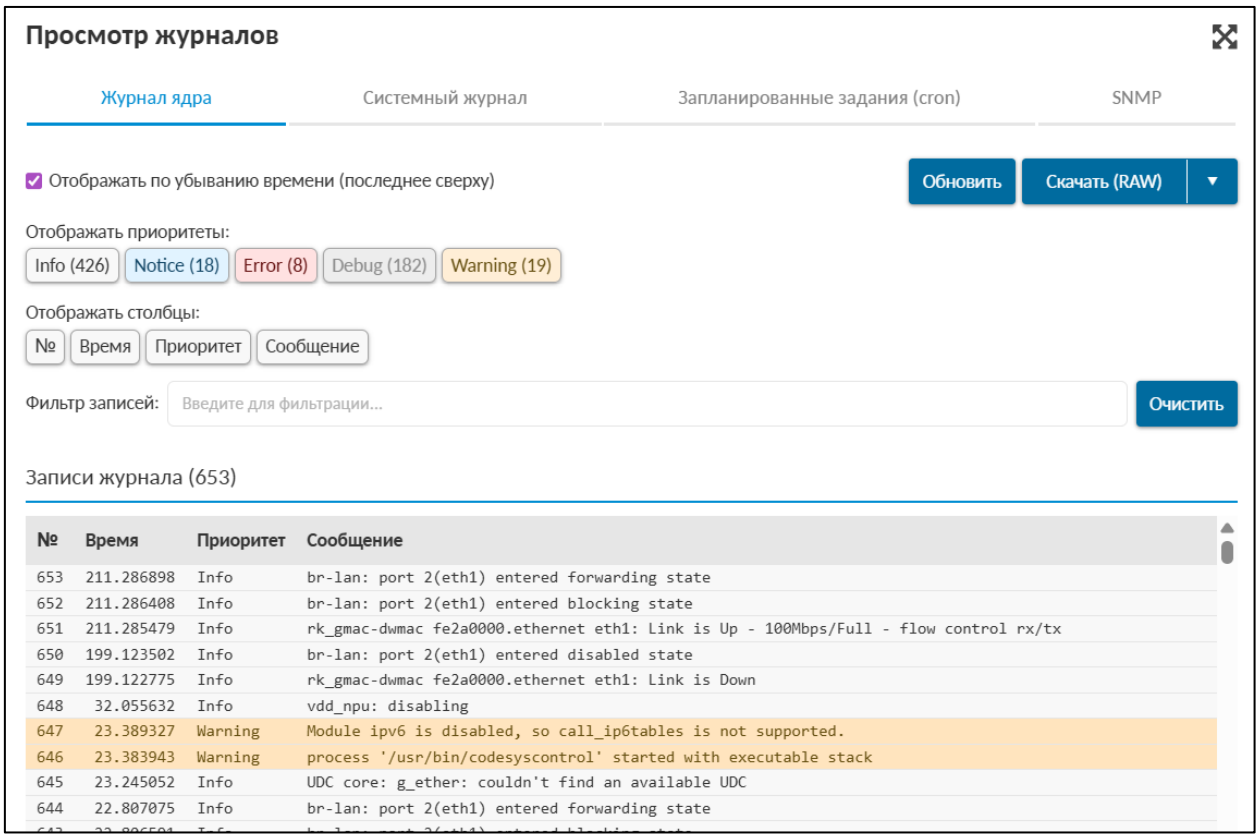


Рисунок 2-14: Страница «Журнал ядра»

В журнале ядра не регистрируются какие-либо события от приложений и служб уровня пользователя.

2.6.2 Подраздел «Системный журнал»

На странице «Системный журнал» раздела «Состояние» отображается вывод системного журнала, в который записываются все события ядра Linux, приложений и служб, запущенных в системе. Внешний вид страницы «Системный журнал» показан на рисунке 2-15.

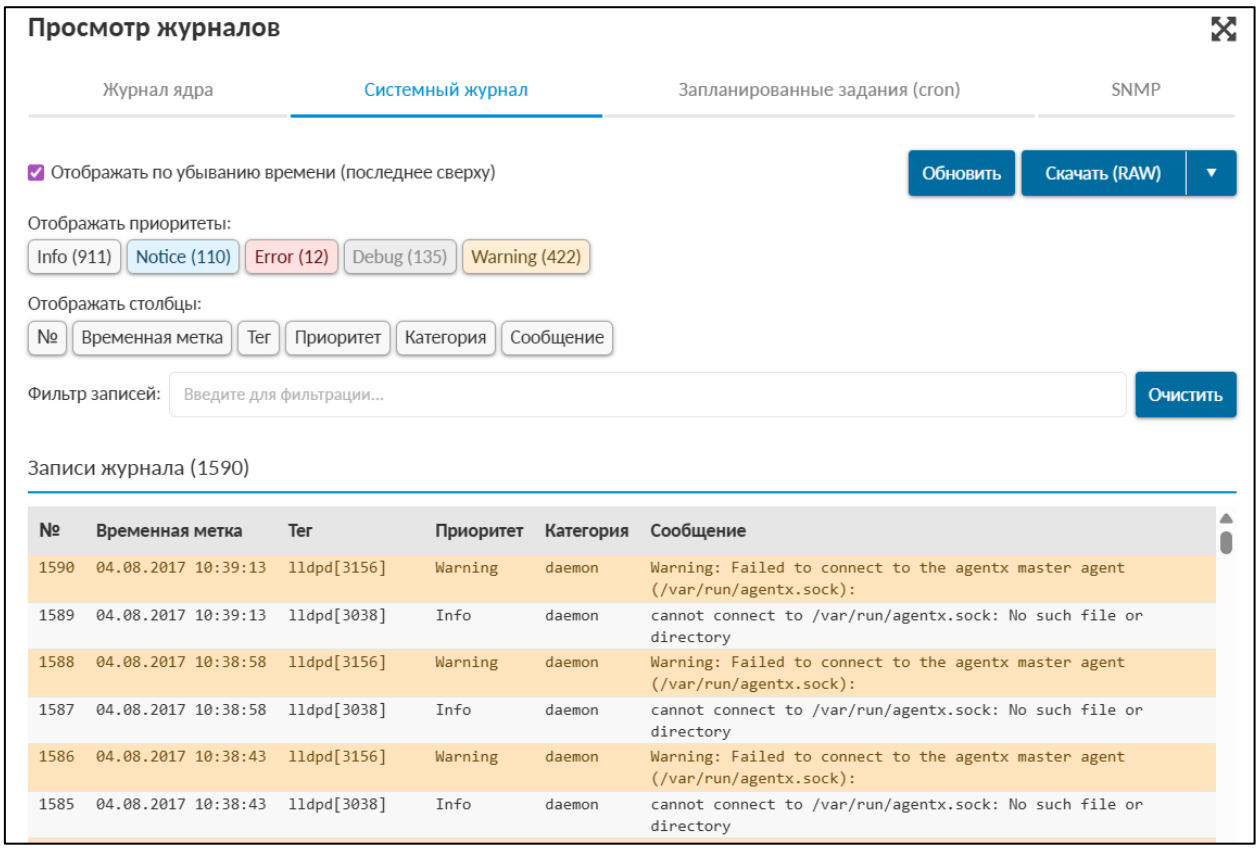


Рисунок 2-15: Страница «Системный журнал»

2.6.3 Подраздел «Запланированные задания (cron)»

В подразделе «Запланированные задания (cron)» отображается журнал службы cron, которая выполняет периодически запускаемые задачи.

Внешний вид страницы «Запланированные задания (cron)» показан на рисунке 2-16.

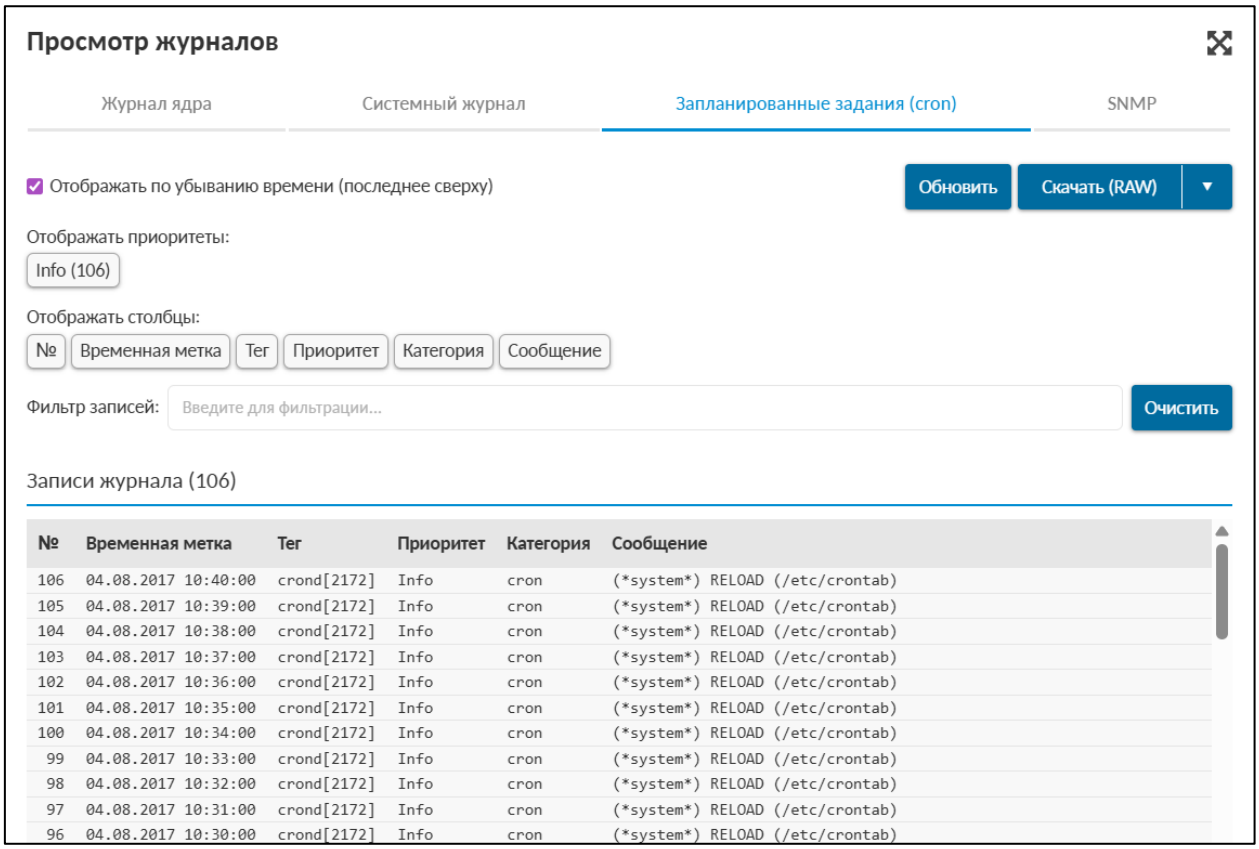


Рисунок 2-16: Страница «Запланированные задания (cron)»

2.6.4 Подраздел «SNMP»

В подразделе «SNMP» отображается журнал работы службы SNMP (Simple Network Management Protocol), предназначенной для управления сетевыми устройствами.

Внешний вид страницы «SNMP» показан на рисунке 2-17.

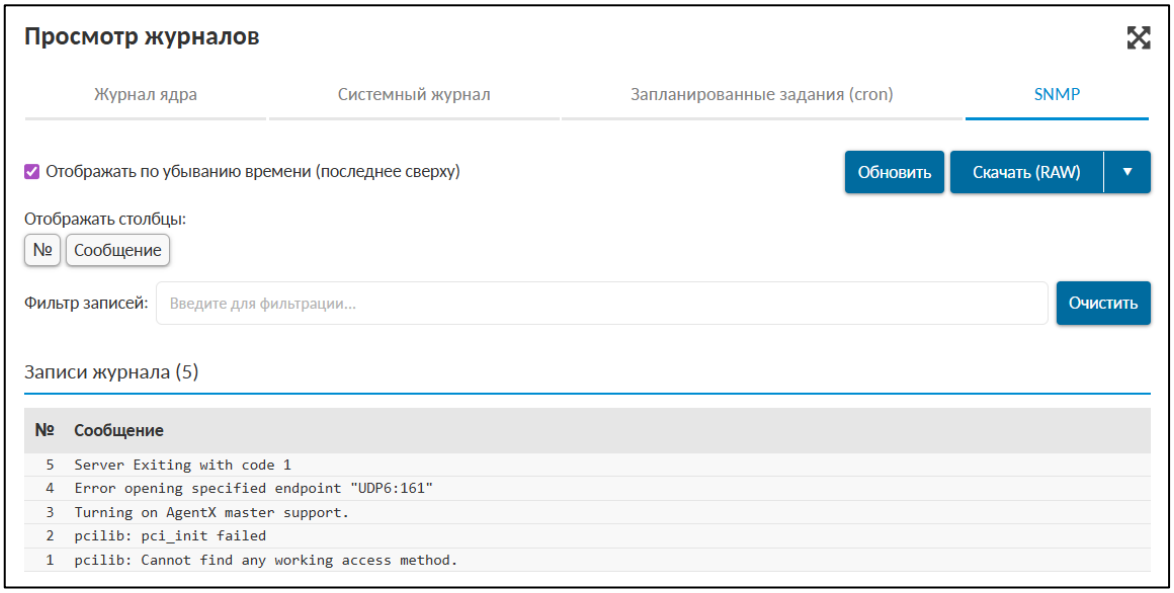


Рисунок 2-17: Страница «SNMP»

3 Система

3.1 Общие настройки

Общие настройки системы размещены на странице «Общие настройки» раздела «Система» и разделены на несколько вкладок:

- «Устройство» (см. раздел 3.1.1);
- «Журналирование» (см. раздел 3.1.2);
- «Язык и тема» (см. раздел 3.1.3);
- «Дополнительные» (см. раздел 3.1.4);
- «Настройки ZRam» (см. раздел 3.1.5).

Внешний вид страницы «Система» показан на рисунке 3-1.

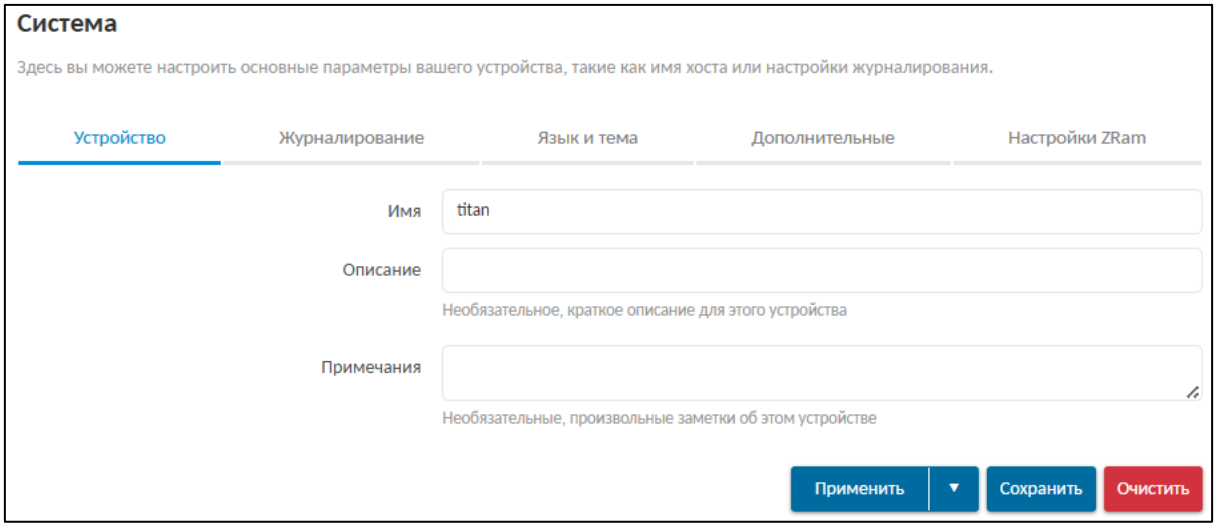


Рисунок 3-1: Страница «Общие настройки»

3.1.1 Вкладка «Устройство»

Вкладка «Устройство» позволяет задать имя хоста системы. Внешний вид вкладки «Устройство» показан на рисунке 3-2.

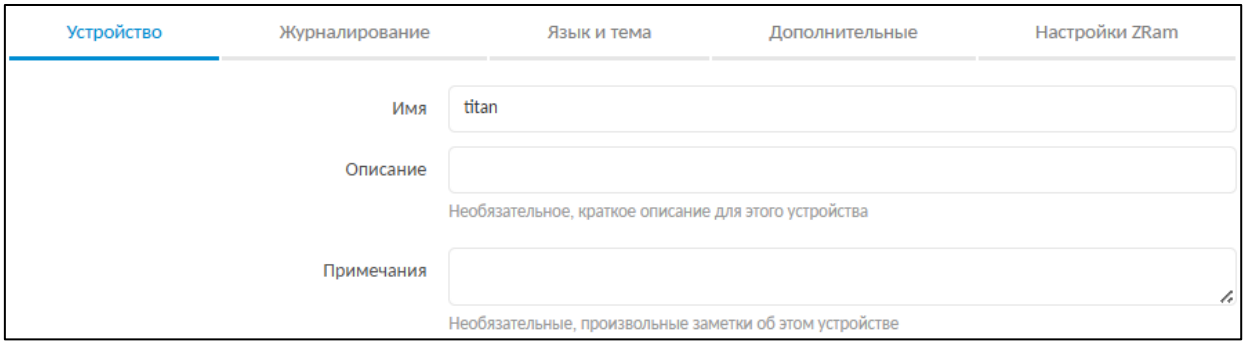


Рисунок 3-2: Страница «Общие настройки». Вкладка «Хост»

3.1.2 Вкладка «Журналирование»

Во вкладке «Журналирование» выполняется настройка системной службы журналирования. Внешний вид вкладки «Журналирование» показан на рисунке 3-3.

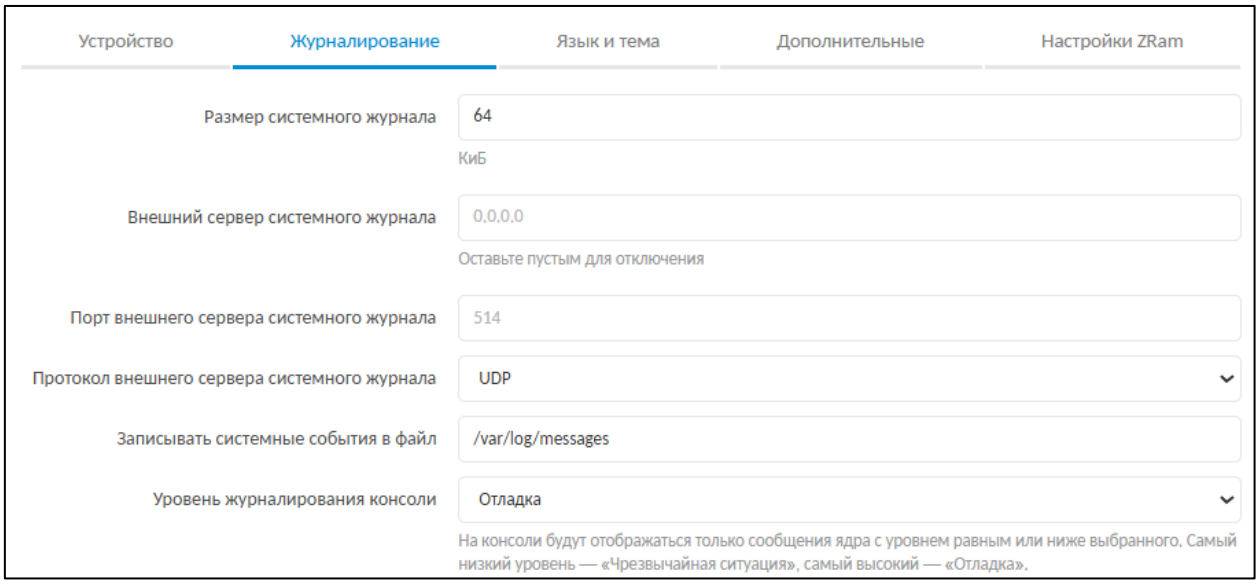


Рисунок 3-3: Страница «Система». Вкладка «Журналирование»

Для конфигурации доступны следующие настройки:

- «Размер системного журнала» — размер хранимого системного журнала в килобайтах. При превышении указанного размера самые старые записи будут удаляться из журнала;
- «Внешний сервер системного журнала» — IP-адрес внешнего сервера системного журнала. При указании адреса внешнего сервера журналирования, события будут дублироваться на него;
- «Порт внешнего сервера системного журнала» — номер порта внешнего сервера журналирования;
- «Протокол внешнего сервера системного журнала» — выбор протокола внешнего сервера журналирования;
- «Записывать системные события в файл» — локальный путь к файлу системного журнала;
- «Уровень журналирования консоли» — выбор уровня событий для журналирования. В системный журнал будут записываться все события

с уровнем выше или равным выбранному. Для выбора доступны следующие уровни:

- отладка (debug);
- информация (information);
- заметка (notice);
- предупреждение (warning);
- ошибка (error);
- критическая ситуация (critical);
- тревога (alarm);
- чрезвычайная ситуация (emergency);

3.1.3 Вкладка «Язык и тема»

Во вкладке «Язык» предоставляется возможность выбора языка и темы оформления интерфейса Web-интерфейса LuCI. Внешний вид вкладки «Язык и тема» показан на рисунке 3-4.

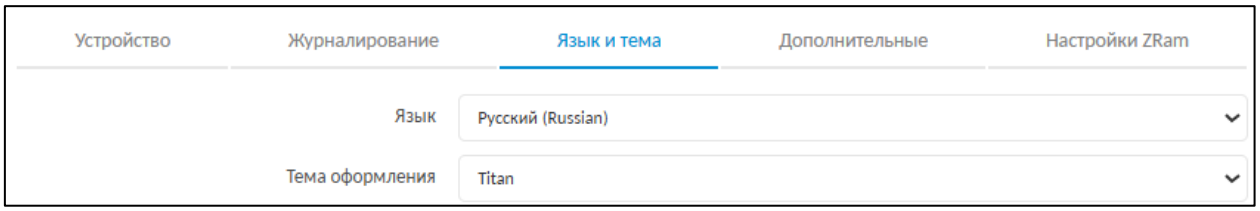


Рисунок 3-4: Страница «Система». Вкладка «Язык»

Помимо списка языков в выпадающем списке «Язык» содержится элемент «автоматически», который позволяет использовать режим автоматического выбора языка интерфейса в зависимости от языка, используемого в браузере клиента.

3.1.4 Вкладка «Дополнительные»

Во вкладке «Дополнительные» предоставлены дополнительные настройки. Внешний вид вкладки «Дополнительные» показан на рисунке 3-5.

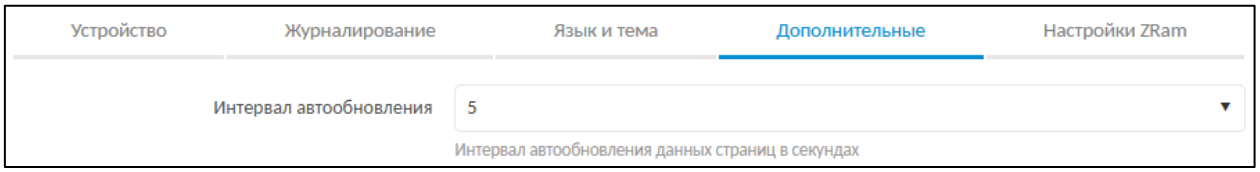


Рисунок 3-5: Страница «Система». Вкладка «Дополнительные»

Настройка «Интервал автообновления» определяет интервал автоматического обновления информации на страницах, поддерживающих данную возможность. Более подробная информация о функции автоматического обновления содержится в разделе 1.2.

3.1.5 Вкладка «Настройки ZRam»

Во вкладке «Настройки ZRam» (см. рисунок 3-6) страницы «Общие настройки» раздела «Система» производится конфигурация объема сжатой оперативной памяти ZRam и алгоритма компрессии.

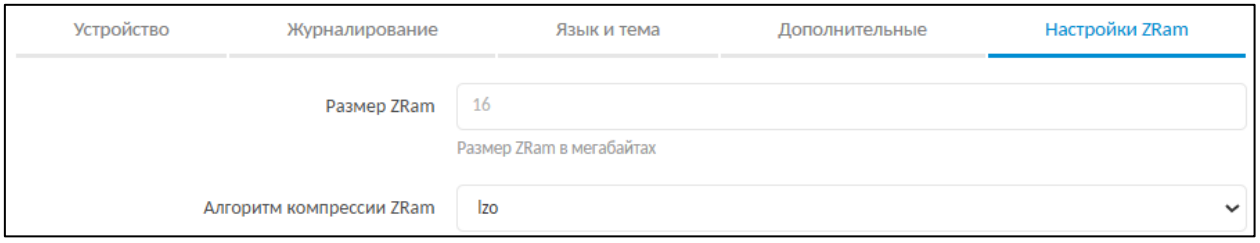


Рисунок 3-6: Страница «Система». Вкладка «Настройки ZRam»

3.2 Время

На странице «Время» раздела «Система» размещены настройки локального времени устройства, а также настройки синхронизации времени при помощи службы NTP. Внешний вид страницы «Время» показан на рисунке 3-7.

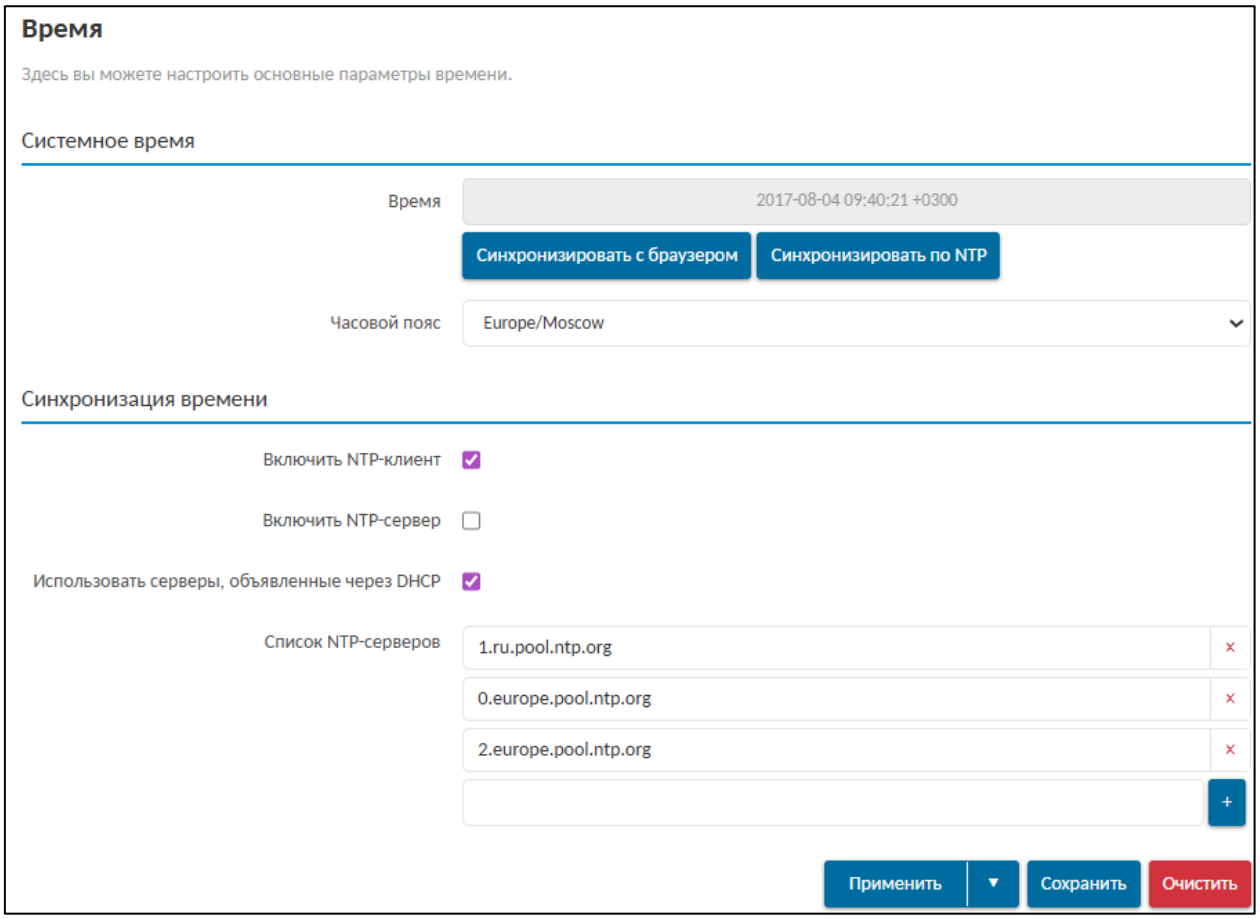


Рисунок 3-7: Страница «Время»

В поле «Системное время» отображается текущее локальное время и дата. Кнопка «Синхронизировать с браузером» выполняет установку локальной даты и времени на устройстве в соответствии с текущей датой и временем, установленными на компьютере клиента (то есть в браузере). При следующем обновлении значения поля «Локальное время», значения даты и времени будут установлены в новые значения.

Кнопка «Синхронизировать по NTP» выполняет синхронизацию времени устройства с NTP-серверами (подробнее см. раздел 4.2.1).

В выпадающем списке «Часовой пояс» выполняется выбор часового пояса локального времени устройства. Для отображения в поле «Локальное время» времени в соответствии с выбранным часовым поясом, необходимо применить изменения, нажав кнопку «Сохранить и применить».

3.2.1 Синхронизация времени

Опция «Включить NTP-клиент» включает синхронизацию времени при помощи NTP-клиента. Синхронизация выполняется с использованием списка NTP-серверов, перечисленных в списке «Список NTP-серверов».

Опция «Включить NTP-сервер» включает службу NTP-сервера. Если данная опция включена, то устройство может быть использовано в качестве NTP-сервера в сети.

Опция «Использовать серверы, объявленные через DHCP» включает использование NTP-серверов, полученных от DHCP-сервера в дополнение к серверам, указанным в списке вручную.

В списке «Список NTP-серверов» указывается список адресов NTP-серверов, используемых для синхронизации локального времени при включенной опции «Включить NTP-клиент».

3.3 Администрирование

Страница «Управление» раздела «Система» содержит настройки локального и удалённого доступа к устройству. На странице «Управление» размещены несколько вкладок:

- «Пароль устройства» (см. раздел 3.3.1);
- «Доступ по SSH» (см. раздел 3.3.2);
- «SSH-ключи» (см. раздел 3.3.3);
- «Доступ HTTP(S)» (см. раздел 3.3.4).

3.3.1 Пароль устройства

Во вкладке «Пароль устройства» страницы «Управление» (см. рисунок 3-8) можно изменить пароль доступа пользователя «root». Указанный пароль используется как для доступа к консоли устройства, так и для доступа к Web-интерфейсу LuCI (см. рисунок 1-2).

Рисунок 3-8: Страница «Управление». Вкладка «Пароль устройства»

3.3.2 Доступ по SSH

Во вкладке «Доступ по SSH» страницы «Управление» (см. рисунок 3-9) размещены настройки сервера Dropbear, который предоставляет доступ к устройствам по протоколам SSH и SFTP.

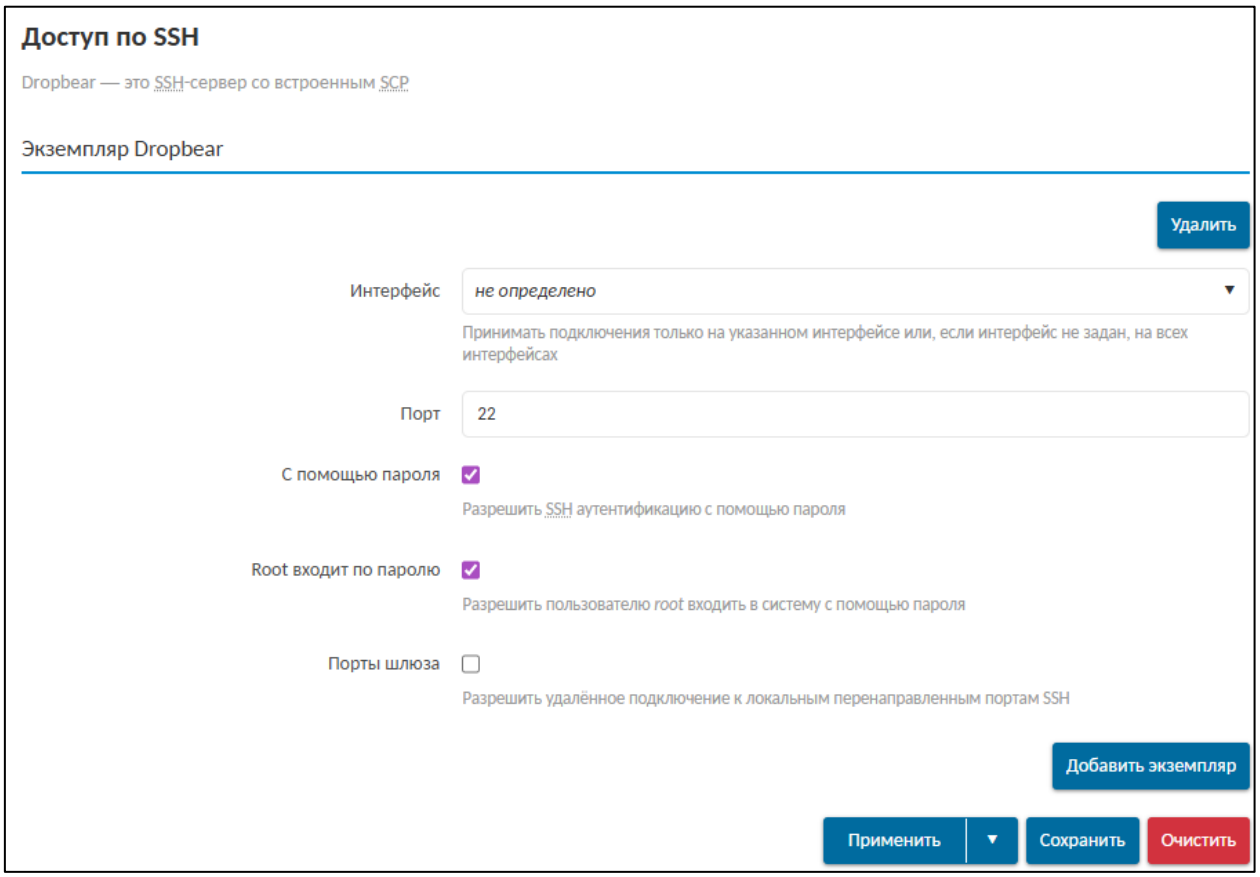


Рисунок 3-9: Страница «Управление». Вкладка «Доступ по SSH»

Кнопки «Добавить экземпляр» и «Удалить» позволяют соответственно добавить или удалить экземпляры сервера Dropbear. По умолчанию в системе запущен только один экземпляр сервера Dropbear, работающий на TCP порту 22 на всех сетевых интерфейсах.

Для каждого экземпляра сервера Dropbear доступны следующие настройки для конфигурации:

- «Интерфейс» — выбор сетевого интерфейса, на котором будут приниматься входящие подключения соответствующего экземпляра сервера Dropbear. Если интерфейс не выбран (значение «не определено»), то соответствующий экземпляр сервера Dropbear будет принимать подключения на всех доступных интерфейсах.
- «Порт» — номер TCP порта для входящих подключений экземпляра сервера Dropbear.
- «С помощью пароля» — разрешает или запрещает аутентификацию при помощи пароля при подключении по SSH. Если аутентификация при помощи пароля запрещена, то вход возможен только по SSH ключам, которые можно добавить в систему в соответствующем подразделе данной страницы.
- «Root входит по паролю» — разрешает или запрещает аутентификацию при помощи пароля для пользователя root. Если аутентификация по паролю запрещена, то вход пользователя root возможен только по ключу.
- «Порты шлюза» — разрешает или запрещает подключение удалённых клиентов к локальным перенаправленным портам.

В приложении А приводится пример выполнения подключения к устройству по протоколу SSH.

3.3.3 SSH-ключи

Во вкладке «SSH-ключи» страницы «Управление» (см. рисунок 3-10) реализована возможность добавления публичных OpenSSH ключей (.pub). Эти SSH ключи используются для выполнения авторизации.

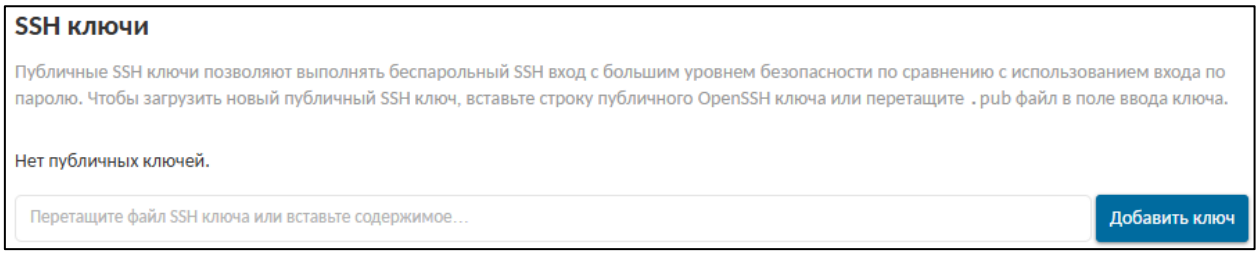


Рисунок 3-10: Страница «Управление». Вкладка «SSH-ключи»

Для добавления нового публичного ключа необходимо вставить строку публичного SSH ключа или перетащить «.pub» файл в поле ввода ключа и нажать кнопку «Добавить». Для удаления ранее добавленного ключа, необходимо нажать кнопку с красным крестиком справа от информации о ключе.

3.3.4 Настройка доступа HTTP(S)

Во вкладке «Доступ HTTP(S)» страницы «Управление» (см. рисунок 3-11) размещены настройки доступf к Web-интерфейсу устройства по протоколам HTTP и HTTPS.

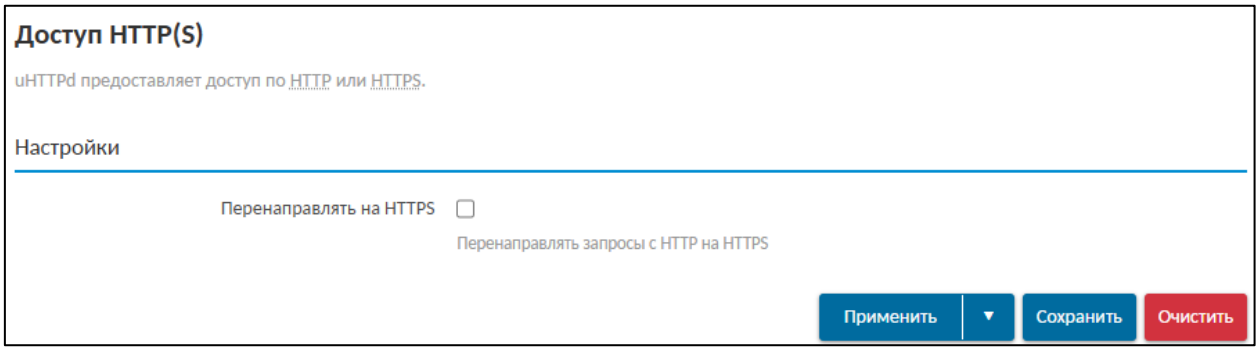


Рисунок 3-11: Страница «Управление». Вкладка «Доступ HTTP(S)»

«Перенаправлять на HTTPS» — при включении данной опции все входящие HTTP-запросы автоматически перенаправляются на защищённое соединение HTTPS. Это обеспечивает шифрование передаваемых данных (логинов, паролей, конфигурации) и повышает безопасность управления устройством.

3.4 Сторожевой таймер

На странице «Сторожевой таймер» раздела «Система» расположены настройки службы сторожевого таймера (watchdog). Внешний вид страницы «Сторожевой таймер» показан на рисунке 3-12.

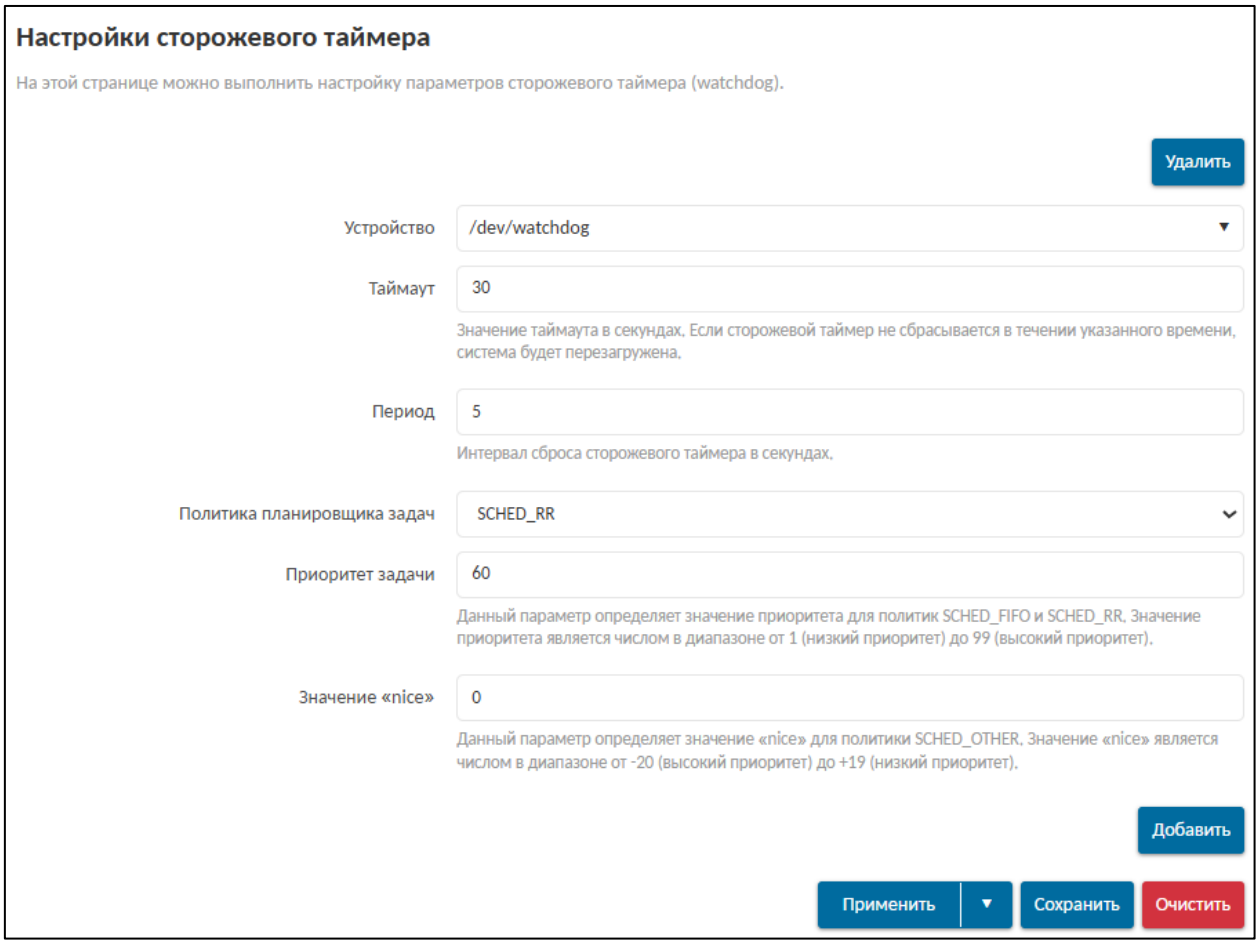


Рисунок 3-12: Страница «Сторожевой таймер»

В поле «Устройство» указывается имя системного устройства аппаратного сторожевого таймера. Служба сторожевого таймера работает в фоновом режиме и автоматически выполняет сброс аппаратного сторожевого таймера с периодом, указанным в поле «Период» (задаётся в секундах). Значение таймаута аппаратного таймера настраивается при помощи поля «Таймаут» (задаётся в секундах).

Настройка «Политика планировщика задач» предназначена для выбора алгоритма диспетчеризации задачи программной службы сторожевого таймера. Доступны следующие алгоритмы:

- SCHED_OTHER — стандартный алгоритм планировщика с разделением времени;
- SCHED_FIFO — планировщик FIFO (First In First Out). Является политикой планирования реального времени. Данный алгоритм планирования не использует никаких интервалов времени. Процесс с алгоритмом «SCHED_FIFO» выполняется до завершения, если он не заблокирован запросом ввода/вывода, вытеснен высокоприоритетным процессом, или он добровольно отказывается от процессорного времени;
- SCHED_RR — циклический (Round-Robin) алгоритм планирования реального времени. Всё, относящееся к алгоритму «SCHED_FIFO», справедливо и для «SCHED_RR» за исключением того, что каждому процессу разрешено работать непрерывно не дольше некоторого времени, называемого карусельным квантом.

Настройки «Приоритет задачи» и «Значение nice» являются параметрами алгоритма диспетчеризации:

3.5 Автозапуск

На странице «Автозапуск» раздела «Система» производится управление скриптами инициализации (службами и пакетами), которые запускаются автоматически при включении устройства. Также здесь можно добавить пользовательские команды для выполнения при загрузке.

Страница разделена на два подраздела: «Скрипты инициализации» и «Запуск пакетов и служб пользователя при включении устройства».

3.5.1 Скрипты инициализации

В подразделе «Скрипты инициализации» отображается таблица всех установленных скриптов инициализации с их параметрами. Вид подраздела представлен на рисунке 3-13.

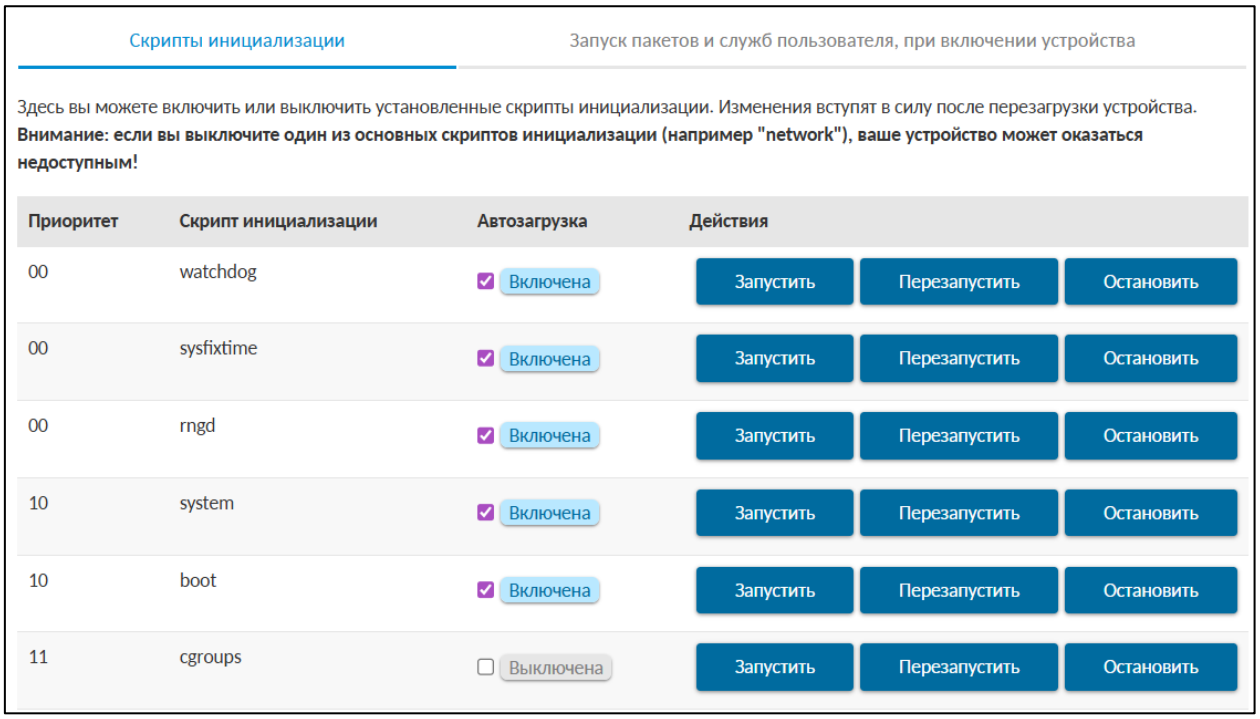


Рисунок 3-13: Страница «Автозапуск». Скрипты инициализации

Таблица имеет следующие столбцы:

- «Приоритет» — числовое значение, определяющее порядок запуска скриптов (чем меньше число, тем раньше выполняется скрипт);
- «Скрипт инициализации» — имя службы или скрипта (например, «watchdog», «sysfixtime», «rngd»);
- «Автозагрузка» — флаг, указывающий, включён ли автоматический запуск данного скрипта при загрузке устройства (отмеченный чекбокс «Включена» означает, что скрипт будет запускаться автоматически);
- «Действия» — кнопки управления службой:
  - «Запустить» — запускает службу немедленно;
  - «Перезапустить» — перезапускает службу;
  - «Остановить» — останавливает службу.

3.5.2 Запуск пакетов и служб пользователя при включении устройства

В подразделе «Запуск пакетов и служб пользователя при включении устройства» отображается содержимое конфигурационного файла «/etc/rc.local». Вид подраздела представлен на рисунке 3-14.

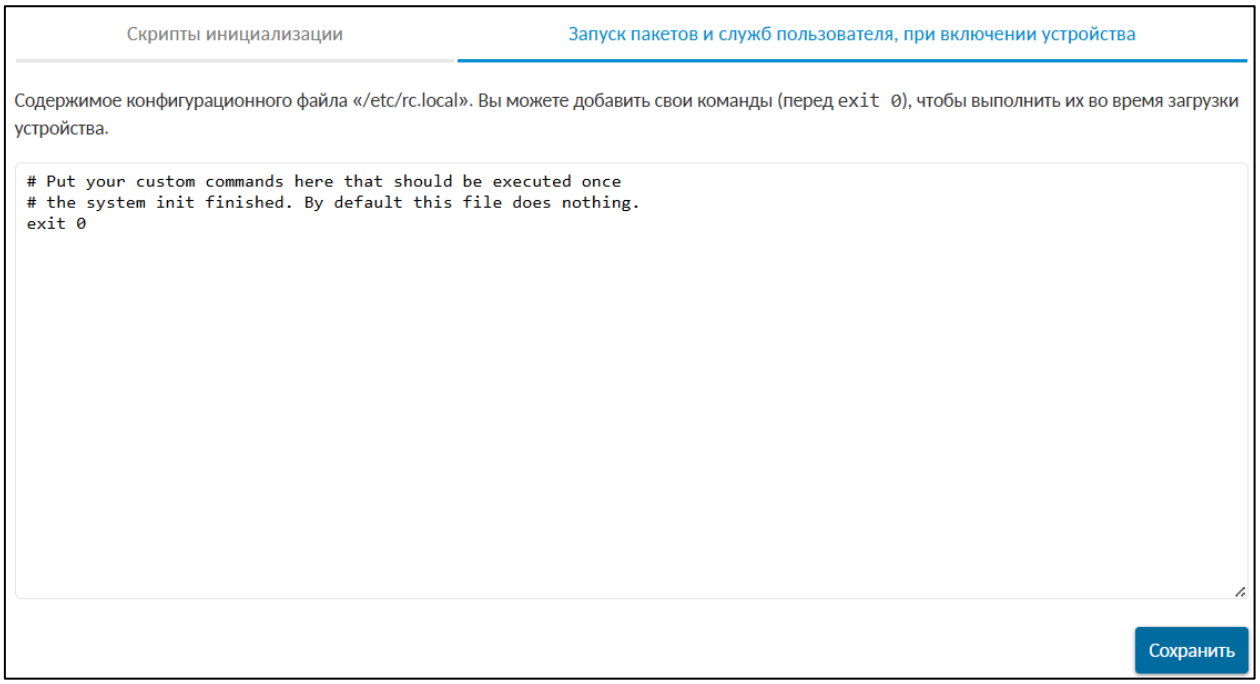


Рисунок 3-14: Страница «Автозапуск». Пользовательские настройки

Для добавления пользовательских команд необходимо разместить их перед строкой exit 0. Для сохранения изменений предназначена кнопка «Сохранить».

3.6 Планировщик

На странице «Планировщик» раздела «Система» производится настройка запланированных задач с использованием службы cron. Здесь можно просматривать и редактировать конфигурационный файл crontab, в котором определяются задачи, выполняемые периодически по расписанию.

Внешний вид страницы показан на рисунке 3-15.

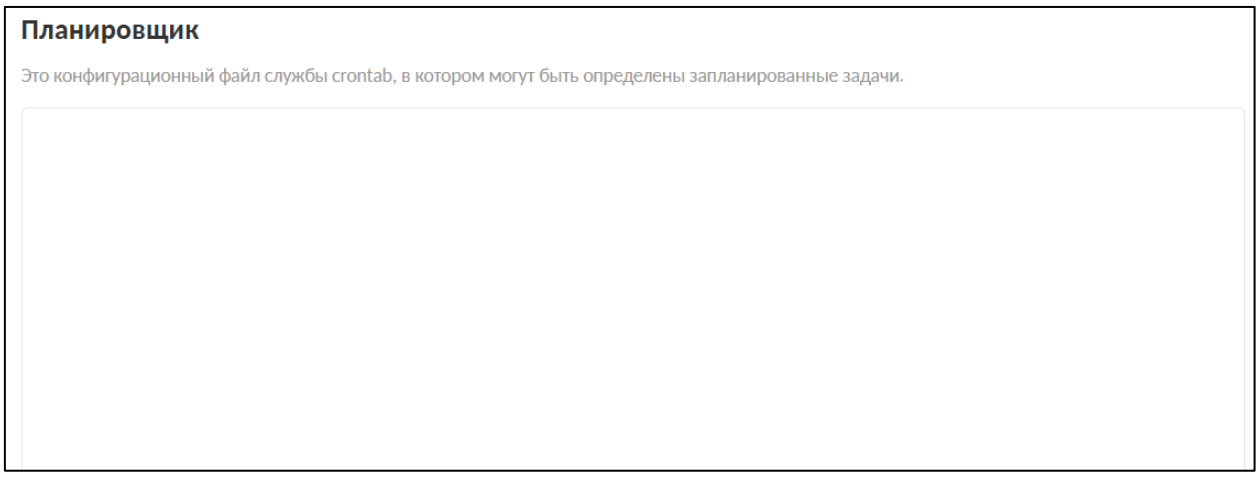


Рисунок 3-15: Страница «Планировщик»

3.7 Точки монтирования

Управление монтированием разделов осуществляется на странице «Точки монтирования» раздела «Система».

Монтирование разделов осуществляется утилитой block на основе конфигурационного файла /etc/config/fstab. Все настройки, представленные на странице «Точки монтирования» хранятся в конфигурационном файле /etc/config/fstab.

Все настройки на странице «Монтирование разделов» разделены на три подраздела:

- «Основные настройки» (см. раздел 3.7.1);
- «Смонтированные разделы» (см. раздел 3.7.2);
- «Точки монтирования» (см. раздел 3.7.3);
- «Разделы подкачки (swap)» (см. раздел 3.7.4).

3.7.1 Подраздел «Основные настройки»

В разделе «Глобальные настройки» страницы «Монтирование разделов» (см. рисунок 3-16) представлены глобальные настройки монтирования:

- Кнопка «Создать конфигурационный файл» — позволяет создать (переписать) конфигурационный файл «/etc/config/fstab» на основе обнаруженных в системе разделов.
- Кнопка «Монтировать подключенные устройства» — при включённой опции система будет пытаться автоматически монтировать сконфигурированные точки монтирования для подключаемых устройств.
- «Неизвестный swap» — при включении данной опции будет выполняться монтирование (активация) не сконфигурированных разделов подкачки (swap). Если опция выключена, неизвестные swap-разделы игнорируются.
- «Неизвестный раздел» — автоматическое монтирование разделов, даже если эти разделы явно не указаны в конфигурации подраздела «Точки

монтирования» (см. раздел 3.7.3). Если опция включена, то неизвестные разделы будут автоматически смонтированы в папку «/mnt/<имя_устройства>».

- «Hotplug раздела подкачки» — автоматическое монтирование (активация) раздела подкачки при его подключении к системе во время её работы (без выключения питания и остановки системы).
- «Hotplug раздела» — автоматическое монтирование разделов при подключении (hotplug). Автоматическое монтирование осуществляется только для разделов, которые указаны в таблице подраздела «Монтирование разделов» (см. раздел 4.5.3). Если подключённый раздел не перечислен в таблице подраздела «Монтирование разделов», то такой раздел будет смонтирован только если включена опция «Неизвестный раздел». Точкой монтирования в таком случае будет папка «/mnt/<имя_устройства>».
- «Проверка файловых систем перед монтированием» — выполнение проверки файловой системы раздела перед монтированием. Для проверки применяются следующие утилиты в зависимости от типа файловой системы:
    - VFAT — /usr/sbin/dosfsck;
    - F2FS — /usr/sbin/fscK.f2fs;
    - Btrfs — /usr/bin/btrfsck;
    - ext2, ext3, ext4 — /usr/sbin/e2fsck.

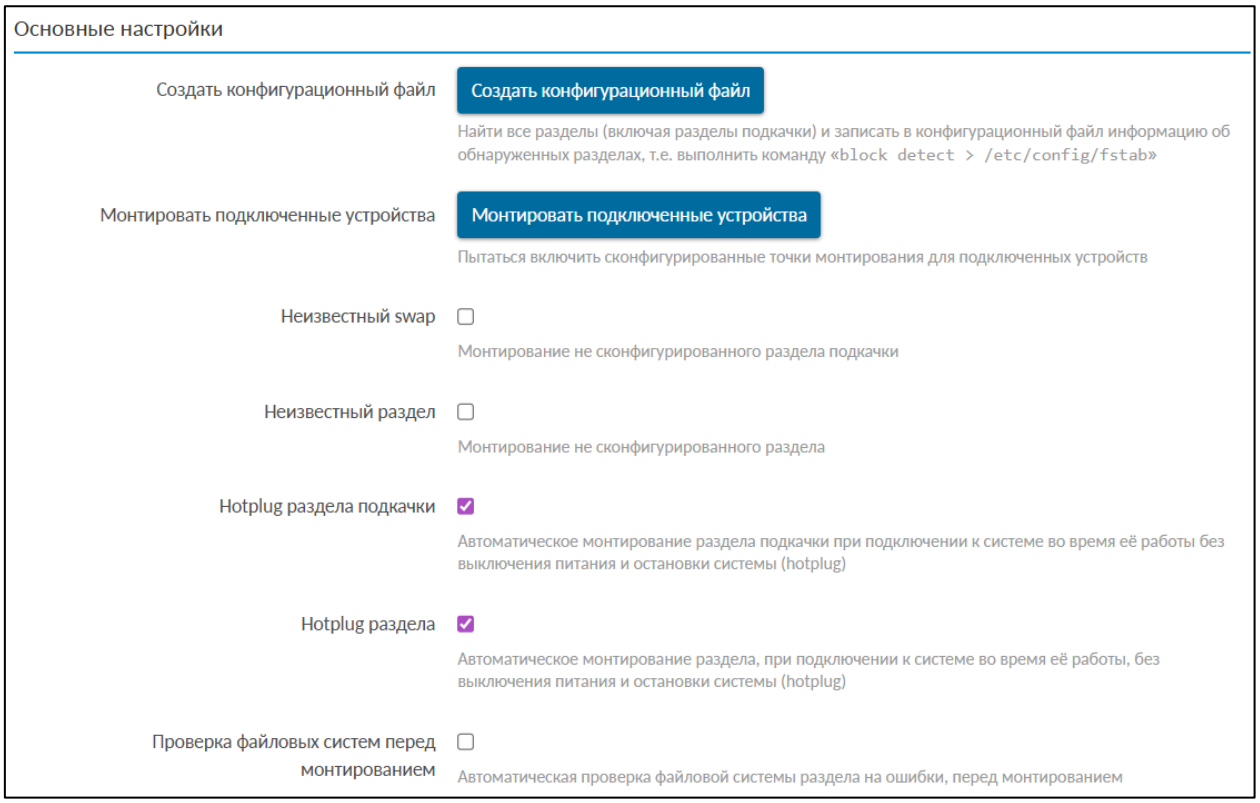


Рисунок 3-16: Точки монтирования. Основные настройки

3.7.2 Подраздел «Смонтированные разделы»

В подразделе «Смонтированные разделы» страницы «Монтирование разделов» приведена текущая таблица монтирования (см. рисунок 3-17).

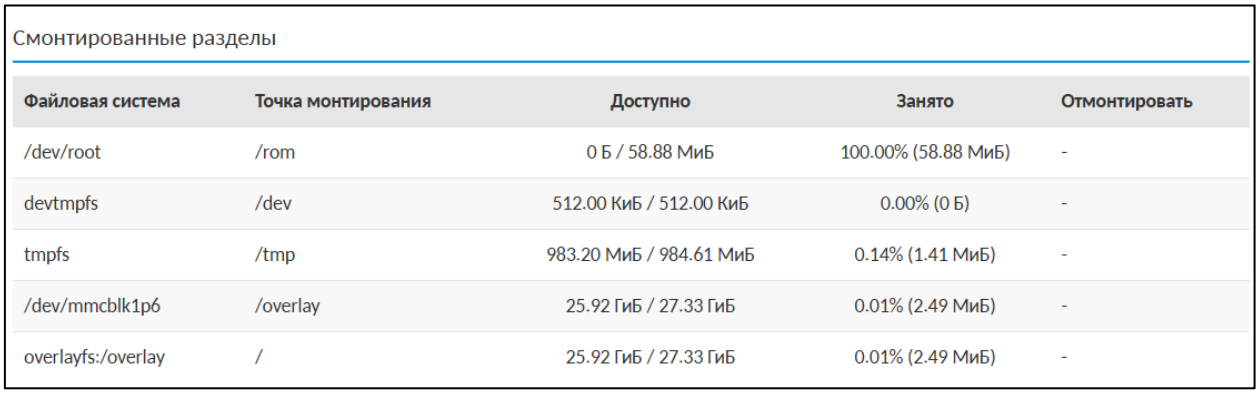


Рисунок 3-17: Страница «Монтирование разделов». Текущая таблица монтирования

В таблице перечислены все смонтированные разделы, их точки монтирования и объём доступного пространства. Имеется возможность ручного размонтирования пользовательских разделов при помощи кнопки «Отмонтировать».

3.7.3 Подраздел «Точки монтирования»

Управление точками монтирования осуществляется в разделе «Точки монтирования» (см. рисунок 3-18). В данном разделе можно добавить точки монтирования для пользовательских разделов (например, для USB-накопителей).

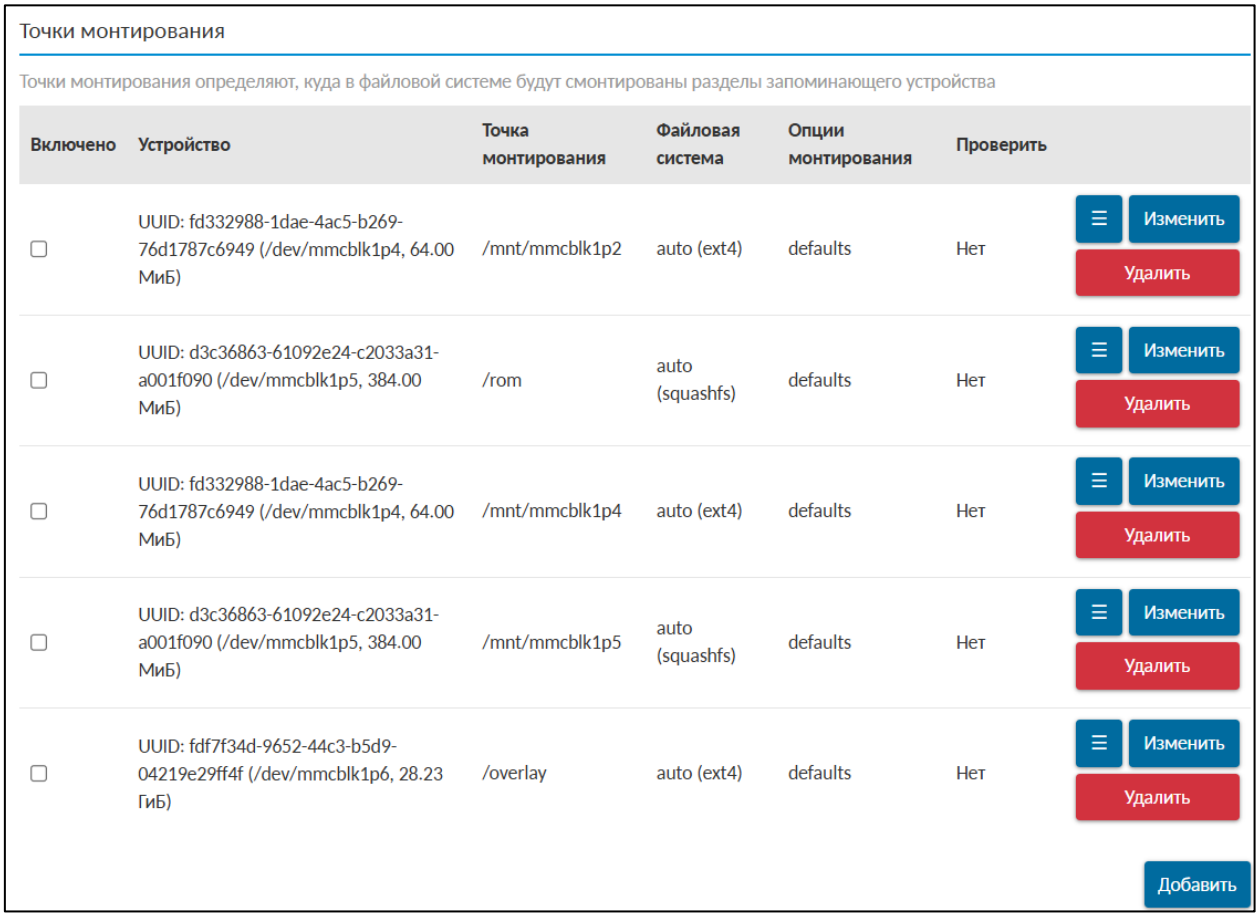


Рисунок 3-18: Страница «Монтирование разделов». Управление монтированием пользовательских разделов

В разделе приведена таблица уже созданных точек монтирования пользовательских разделов с их параметрами. Таблица содержит следующие столбцы:

- «Включено» — определяет включена ли данная точка монтирования.
- «Устройство» — параметры устройства и признак, по которому устройство идентифицируется для монтирования (UUID, метка устройства или файл устройства).
- «Точка монтирования» — точка монтирования раздела.

– «Файловая система» — файловая система смонтированного раздела.
– «Опции монтирования» — дополнительные опции, передаваемые утилите mount при монтировании.
– «Проверить» — признак проверки файловой системы перед монтированием.

3.7.3.1 Редактирование точки монтирования

Для редактирования точки монтирования пользовательского раздела необходимо нажать кнопку «Изменить», расположенную в строке соответствующего раздела таблицы точек монтирования (см. рисунок 3-18). При этом откроется страница редактирования параметров точки монтирования раздела, как показано на рисунке 3-19.

Страница редактирования параметров точки монтирования раздела разделена на вкладки «Общие настройки» (см. рисунок 3-19) и «Дополнительные настройки» (см. рисунок 3-20).

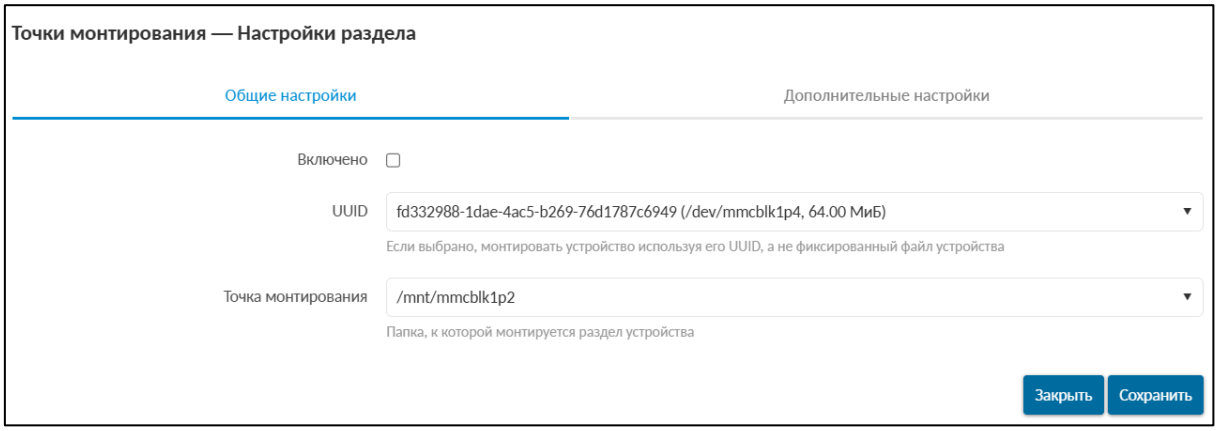


Рисунок 3-19: Общие настройки точки монтирования раздела

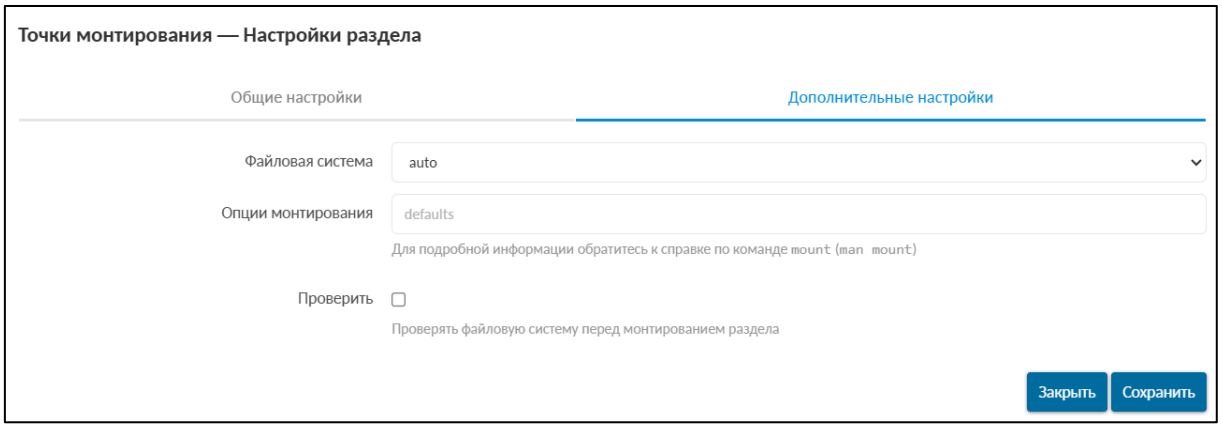


Рисунок 3-20: Дополнительные настройки точки монтирования раздела

Во вкладке «Общие настройки» размещены следующие настройки:

- «Включено» — определяет включена ли данная точка монтирования.
- «UUID» — если выбрана данная опция, то монтируемый раздел будет идентифицироваться по выбранному UUID. Возможен ручной ввод UUID или выбор из списка UUID всех подключённых разделов на момент загрузки страницы.
- «Точка монтирования» — определяет точку монтирования раздела. Возможен ручной ввод точки монтирования раздела или выбор из предложенных вариантов.

Во вкладке «Дополнительные настройки» расположены следующие настройки:

- «Файловая система» — выбор файловой системы монтируемого раздела.
- «Опции монтирования» — дополнительные опции, передаваемые утилите mount при монтировании раздела. Для корректного отображения имен файлов и каталогов с использованием символов кириллицы, необходимо указать следующие опции монтирования:

```
codepage=1251, iocharset=utf8
```

- «Проверить» — проверка файловой системы перед монтированием.

3.7.3.2 Добавление точки монтирования

Для добавления новой точки монтирования пользовательского раздела необходимо нажать кнопку «Добавить», расположенную под таблицей точек монтирования (см. рисунок 3-18).

При добавлении новой точки монтирования откроется такая же страница редактирования параметров точки монтирования, как и при редактировании уже существующей точки монтирования. Редактирование существующих точек монтирования рассмотрено в разделе 3.7.3.1 данного руководства.

3.7.3.3 Удаление точки монтирования

Для удаления точки монтирования пользовательского раздела необходимо нажать кнопку «Удалить», расположенную в строке соответствующего раздела таблицы точек монтирования (см. рисунок 3-18).

3.7.4 «Разделы подкачки (swap)»

В подразделе «Разделы подкачки (swap)» (см. рисунок 3-21) страницы «Монтирование разделов» производится настройка и управление swap-разделами, используемыми для временного хранения данных при недостатке оперативной памяти.

Если физической памяти недостаточно, неиспользуемые данные могут быть временно перемещены в раздел подкачки, что позволяет увеличить объём доступной свободной RAM. Однако следует учитывать, что перемещение данных на swap-раздел — это достаточно медленный процесс, так как устройство, на котором располагается раздел подкачки (например, flash-накопитель или SD-карта), работает гораздо медленнее, чем оперативная память.

В подразделе отображается таблица уже созданных swap-разделов. Таблица имеет следующие столбцы:

- «Включено» — флаг, указывающий, активирован ли данный swap-раздел;
- «Устройство» — имя системного устройства, используемого в качестве swap-раздела (например, /dev/sda2 или путь к swap-файлу).

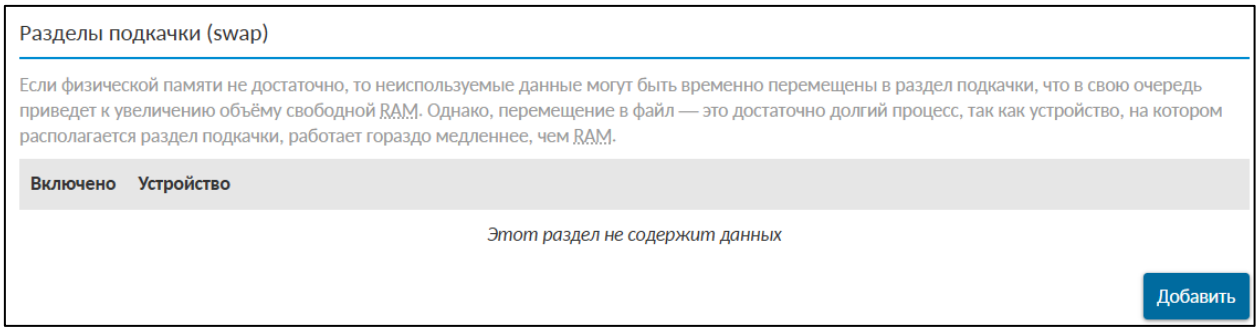


Рисунок 3-21: Точки монтирования. Разделы подкачки

3.8 Индикаторы

На странице «Настройка LED индикации» раздела «Система» производится настройка поведения светодиодных индикаторов (LED) устройства.

Внешний вид страницы показан на рисунке 3-22.

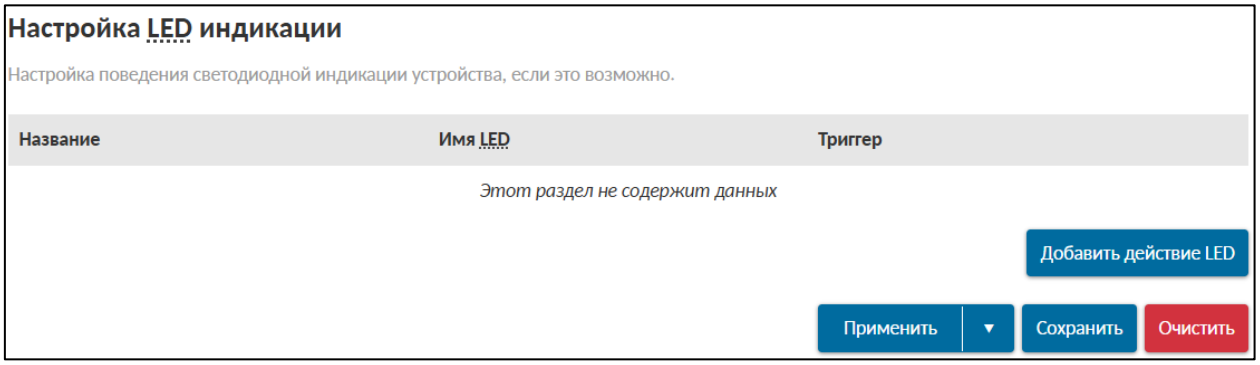


Рисунок 3-22: Страница «Индикаторы»

В подразделе отображается таблица уже созданных правил управления светодиодами. Таблица имеет следующие столбцы:

– «Название» — символьное имя для данного правила;
– «Имя LED» — системное имя светодиода, поведение которого настраивается;
– «Триггер» — событие или условие, при котором светодиод будет активирован.

Кнопка «Добавить действие LED» используется для создания нового правила управления светодиодом. При её нажатии открывается страница (см. рисунок 3-23) для выбора светодиода, настройки триггера и дополнительных параметров.

Рисунок 3-23: Страница «Индикаторы». Добавление действия LED

3.9 Резервное копирование

На странице «Резервное копирование» раздела «Система» расположены настройки, связанные с созданием и восстановлением резервной копии файлов конфигурации устройства. Настройка списка сохраняемых файлов описана в разделе 3.9.1. Кроме того, на данной странице можно выполнить сброс устройства к заводским настройкам (factory reset).

Внешний вид страницы «Резервное копирование» показан на рисунке 3-24.

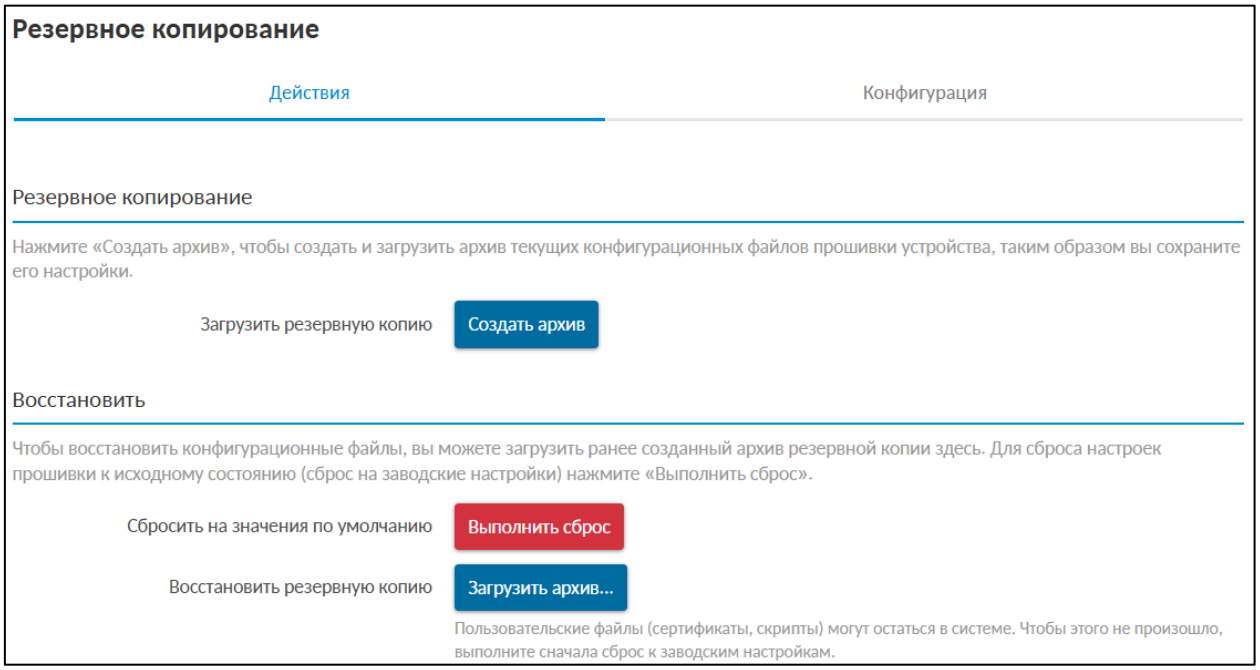


Рисунок 3-24: Страница «Резервное копирование»

На странице «Резервное копирование» во вкладке «Действия» (см. рисунок 3-24) представлены следующие элементы управления:

– Кнопка «Создать архив» — позволяет создать (скачать) tar-архив текущих конфигурационных файлов прошивки устройства;

Кнопка «Загрузить архив» — позволяет выбрать на локальном компьютере tar-архив резервной копии для последующего восстановления. При выполнении восстановления резервной копии настроек будет выполнена перезагрузка устройства;

– Кнопка «Выполнить сброс» — выполняет сброс устройства к заводским настройкам (factory reset);

При выполнении сброса к заводским настройкам будут уничтожены все пользовательские файлы и потерянные пользовательская конфигурация устройства.

При выполнении сброса к заводским настройкам будет выполнена перезагрузка устройства.

3.9.1 Настройка списка файлов резервной копии

На вкладке «Конфигурация» страницы «Резервное копирование» можно выполнить настройку списка файлов, которые будут сохраняться в резервной копии. Внешний вид вкладки «Конфигурация» показан на рисунке 3-25.

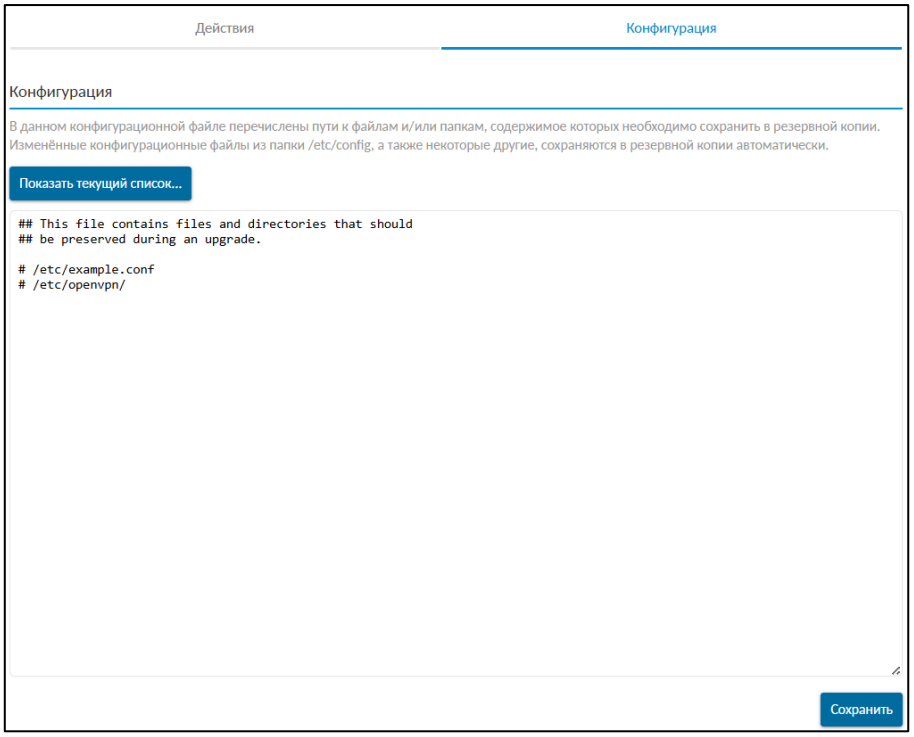


Рисунок 3-25: Страница «Резервное копирование». Вкладка «Конфигурация»

Здесь представлено содержимое конфигурационного файла «/etc/sysupgrade.conf», в котором указываются дополнительные пути к файлам и/или папкам, которые необходимо сохранять в резервной копии (по одной записи на строку). Строки, начинающиеся с символа «#», являются комментариями и игнорируются при выполнении резервного копирования.

При нажатии кнопки «Показать текущий список...» будет отображён полный список файлов, которые будут сохранены в резервную копию с учётом конфигурационного файла «/etc/sysupgrade.conf» (см. рисунок 3-26).

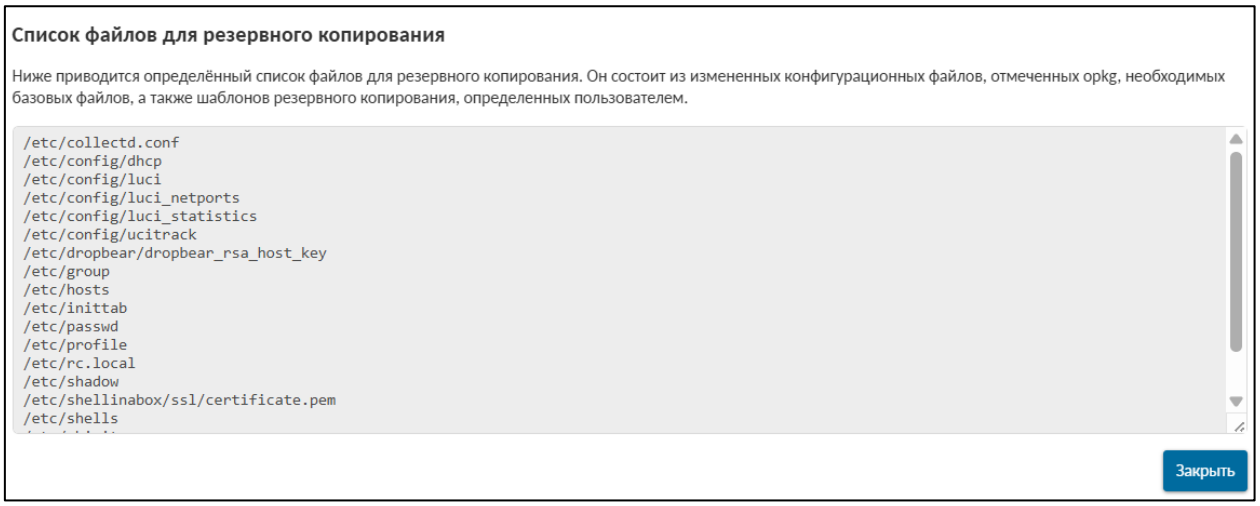


Рисунок 3-26: Страница «Резервное копирование». Вкладка «Настройка config файла». Список файлов

Возврат к редактированию конфигурационного файла «/etc/sysupgrade.conf» осуществляется при помощи кнопки «Закрыть».

3.10 Обновление прошивки

На странице «Обновление прошивки» раздела «Система» расположен функционал обновления прошивки устройства. Внешний вид страницы «Обновление прошивки» показан на рисунке 3-27.

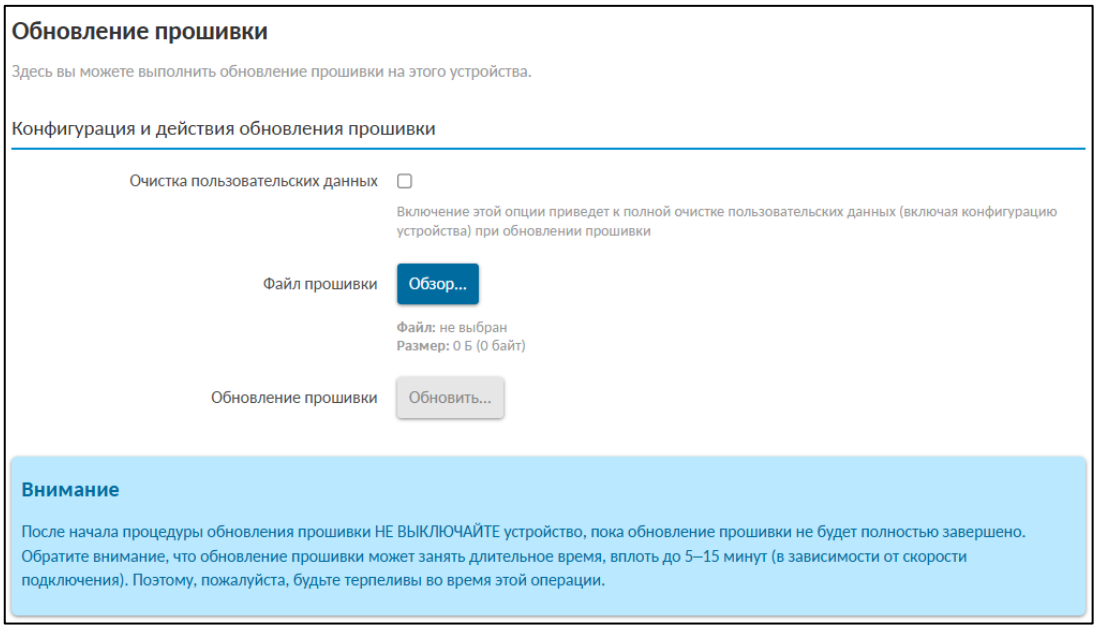


Рисунок 3-27: Страница «Обновление прошивки»

При выполнении обновления прошивки устройства можно выполнить автоматический сброс всех настроек к заводскому состоянию. Для выполнения сброса предназначена настройка «Очистка пользовательских

данных» (см. рисунок 3-27). Если данная настройка включена, то при выполнении обновления прошивки все пользовательские настройки и данные на устройстве будут уничтожены.

Процедуры ручного создания и восстановления резервной копии подробно рассматриваются в разделе 3.9 данного документа. При обновлении прошивки устройства, для создания и восстановления резервной копии используются те же возможности.

Для обновления прошивки необходимо выбрать новый файл образа прошивки для загрузки на устройство при помощи кнопки «Обзор...».

При наличии на внешнем устройстве корректного файла образа прошивки кнопка «Обновить…» становится активна. Нажатие этой кнопки начинает процедуру обновления прошивки устройства.

3.11 Терминал

На странице «Терминал» раздела «Система» можно получить доступ к терминалу устройства непосредственно через браузер, без использования какого-либо дополнительного программного обеспечения.

Внешний вид страницы «Терминал» показан на рисунке 3-28.

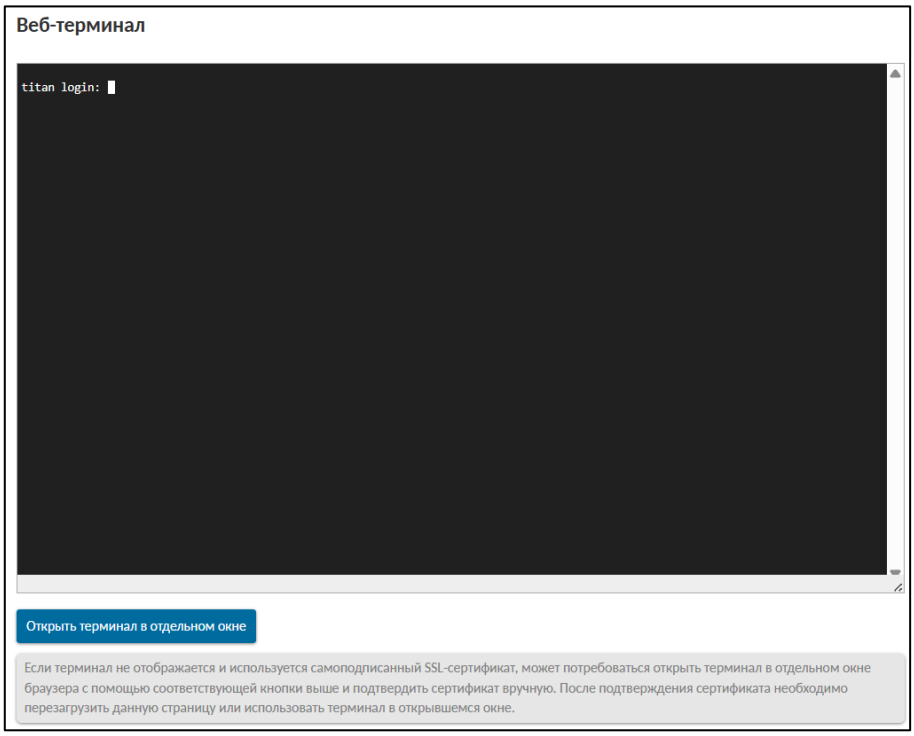


Рисунок 3-28: Страница «Терминал»

3.11.1 Настройки терминала

Страница настроек терминала показана на рисунке 3-29.

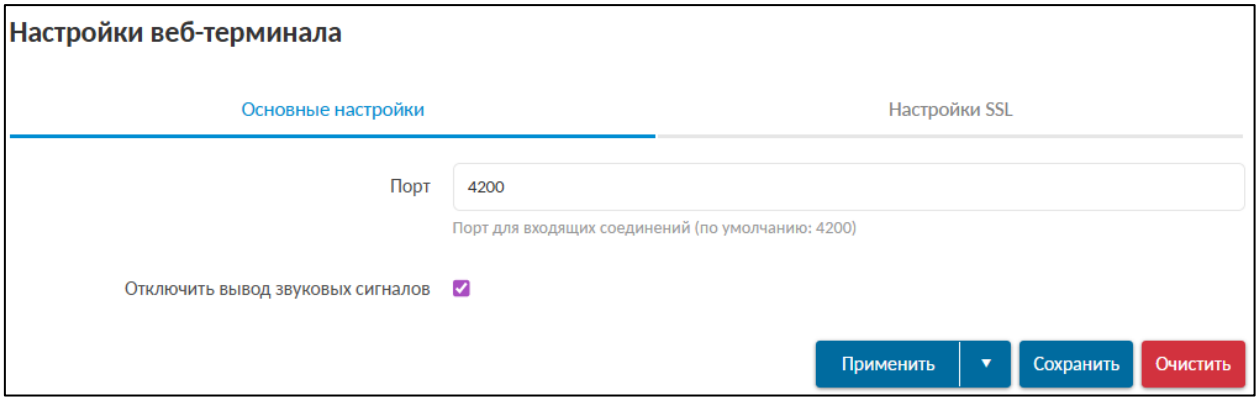


Рисунок 3-29: Страница основных настроек терминала

В поле «Порт» указывается значение TCP порта службы веб-терминала. По умолчанию, службой веб-терминала используется порт TCP 4200.

Настройка «Отключить вывод звуковых сигналов» отключает воспроизведение браузером звуковых сигналов, которые могут быть сгенерированы в терминале, например при выводе специального символа ASCII BEL (код 7).

На вкладке «Настройки SSL» расположены настройки шифрования SSL. Внешний вид вкладки «Настройки SSL» показан на рисунке 3-30.

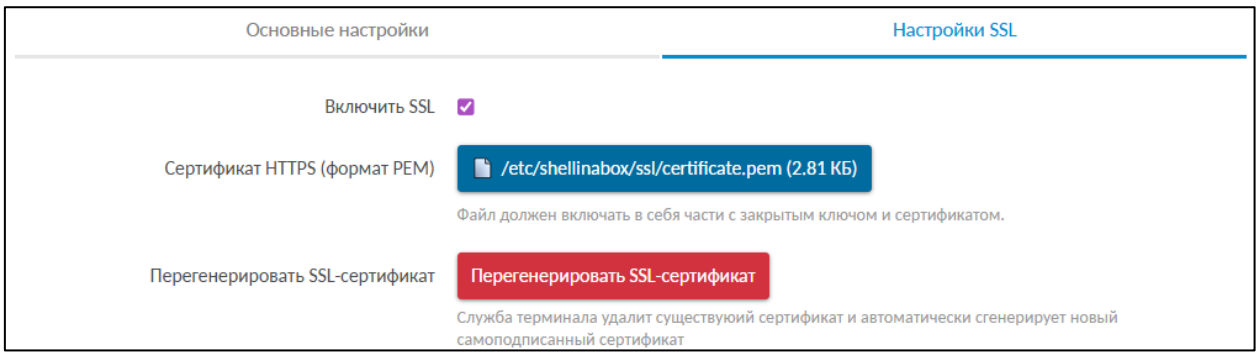


Рисунок 3-30: Страница SSL настроек терминала

Настройка «Включить SSL» позволяет включить или отключить использование SSL при работе терминала.

Не рекомендуется использовать службу терминалов без включённого SSL шифрования. В этом случае, все данные по сети передаются в открытом виде, в том числе логин и пароль.

Настройка «Сертификат HTTPS (формат PEM)» позволяет указать путь к SSL сертификату на файловой системе устройства или выполнить загрузку нового сертификата в формате PEM при помощи кнопки.

При нажатии кнопки «Перегенерировать SSL сертификат» происходит удаление текущего SSL сертификата и автоматическая генерация нового самоподписанного сертификата.

3.12 Перезагрузка

Страница «Перезагрузка» раздела «Система» предназначена для выполнения программной перезагрузки устройства. Данная функция аналогична выполнению в консоли команды gboot. Внешний вид страницы «Перезагрузка» раздела «Система» показан на рисунке 3-31.

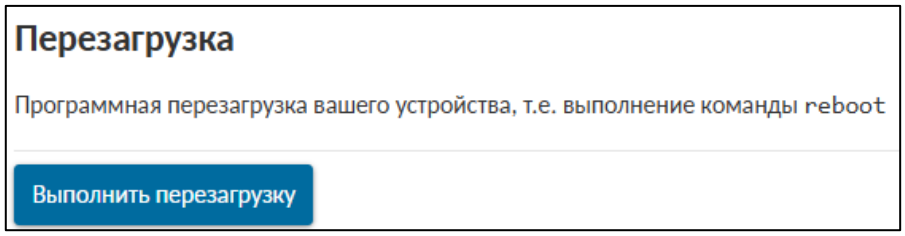


Рисунок 3-31: Страница «Перезагрузка»

Перезагрузка устройства выполняется при нажатии кнопки «Выполнить перезагрузку».

4 ПЛК

Раздел «ПЛК» главного меню Web-интерфейса содержит страницы для настройки и мониторинга функций программируемого логического контроллера (ПЛК) устройства. В данном разделе описываются страницы, связанные с работой ядра CODESYS, пользовательским приложением, загрузками, журналами и другими параметрами.

4.1 Веб-визуализация

Примечание**:** на момент подготовки документации страница веб-визуализации пользовательского приложения CODESYS не функционирует («не работает»). При попытке доступа к ней отображается сообщение об ошибке или пустая страница. Функциональность будет добавлена в следующих версиях прошивки.

4.2 Настройки CODESYS

На странице «Настройки CODESYS» производится конфигурация параметров ядра CODESYS, включая сетевые настройки веб-визуализации, обработку исключений, параметры трендов и тревог, а также дополнительные возможности.

Страница разделена на следующие подразделы.

- «Сетевые настройки веб-интерфейса» (см. раздел 4.2.1);
- «Исключения» (см. раздел 4.2.2);
- «Тренды и тревоги» (см. раздел 4.2.3);
- «Разное» (см. раздел 4.2.4).

4.2.1 Сетевые настройки веб-визуализации

В данном подразделе (см. рисунок 4-1) настраиваются параметры доступа к веб-визуализации пользовательского приложения.

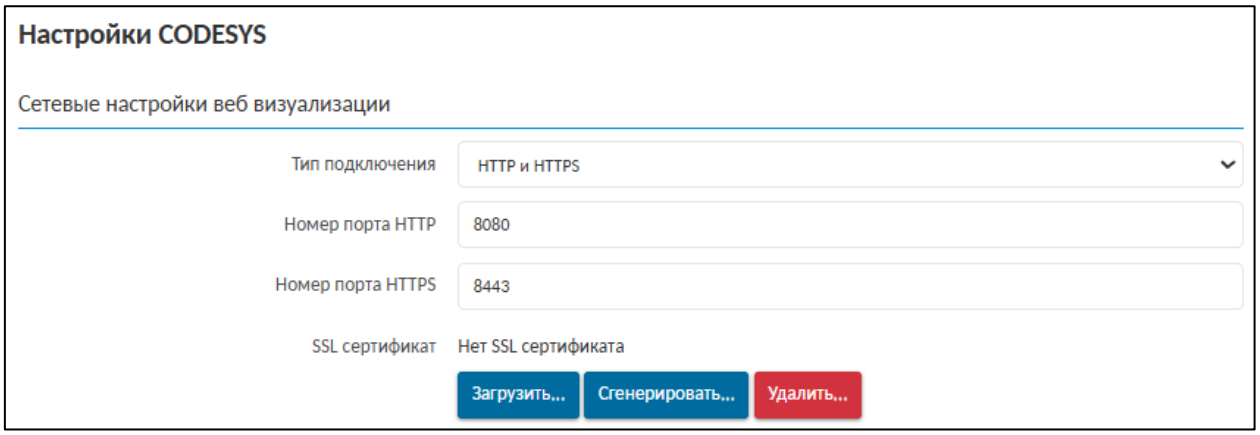


Рисунок 4-1: Страница «Настройки CODESYS». Сетевые настройки веб-визуализации

В подразделе настраиваются следующие параметры:

– «Тип подключения» — выбор протокола для доступа к веб-визуализации;
– «Номер порта HTTP» — TCP-порт для входящих HTTP-соединений. По умолчанию: 8080;
– «Номер порта HTTPS» — TCP-порт для входящих HTTPS-соединений. По умолчанию: 8443;
– «SSL сертификат» — информация о текущем SSL-сертификате для HTTPS.

4.2.1.1 Загрузка SSL-сертификата

При нажатии на кнопку «Загрузить...» в подразделе «Сетевые настройки веб-визуализации» открывается диалоговое окно «Загрузка SSL сертификата». Внешний вид окна показан на рисунке 4-2.

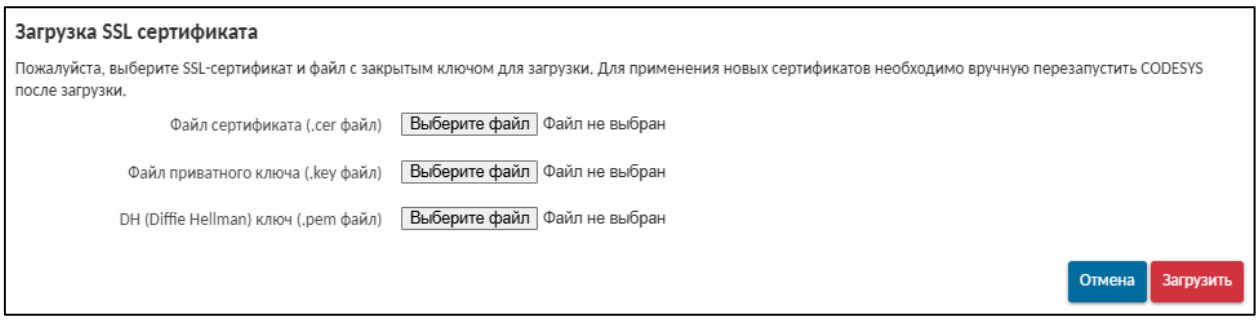


Рисунок 4-2: Страница «Настройки CODESYS»

Диалоговое окно позволяет загрузить SSL-сертификат и соответствующий закрытый ключ для использования службой веб-визуализации CODESYS по протоколу HTTPS.

Параметры загрузки

- «Файл сертификата (.cer файл)» — выбор файла сертификата в формате .cer.
- «Файл приватного ключа (.key файл)» — выбор файла закрытого ключа в формате .key.
- «DH (Diffie Hellman) ключ (.pem файл)» — выбор файла параметров Diffie-Hellman в формате .pem

4.2.1.2 Генерация SSL сертификата

При нажатии на кнопку «Сгенерировать...» в подразделе «Сетевые настройки веб-визуализации» (см. раздел 4.2.1) открывается диалоговое окно подтверждения генерации нового SSL-сертификата. Внешний вид окна показан на рисунке 4-3.

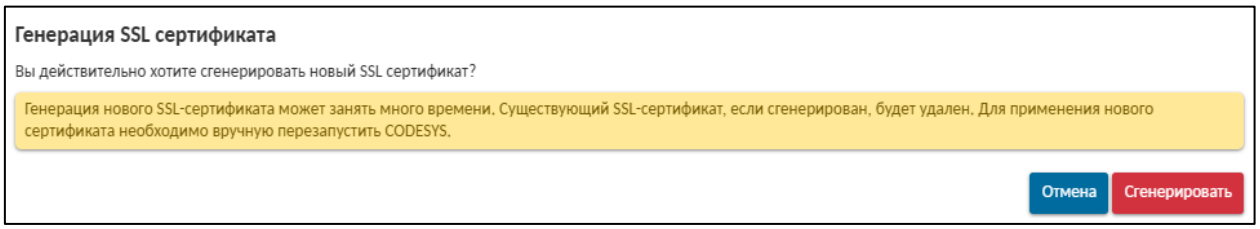


Рисунок 4-3: Диалоговое окно «Генерация SSL сертификата»

4.2.2 Исключения

Подраздел «Обработка исключений» (см. рисунок 4-4) определяет поведение ядра CODESYS при возникновении исключения. Значение «Отваливается CODESYS» означает, что при критической ошибке ядро ПЛК будет остановлено.

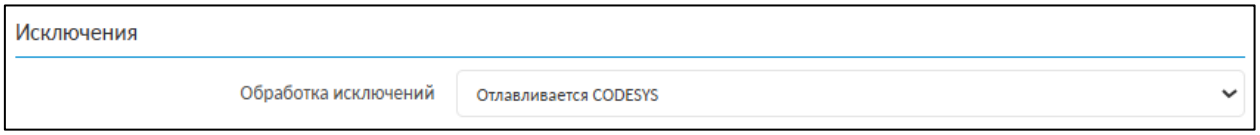


Рисунок 4-4: Страница «Настройки CODESYS». Исключения

4.2.3 Тренды и тревоги

В подразделе «Тренды и тревоги» (см. рисунок 4-5) настраиваются параметры хранения и обработки данных о ходе технологического процесса (тренды) и аварийных событиях (тревоги).

- «Каталог трендов» — путь к директории для хранения файлов трендов (истории изменения параметров).
- «Каталог тревог» — путь к директории для хранения файлов тревог (аварийных событий).
- «Объем оперативной памяти, используемый memsys5, Мб» — объём оперативной памяти (в мегабайтах), выделяемый для системы управления памятью memsys5.
- «Период диагностики, сек.» — интервал (в секундах) сбора диагностической информации.

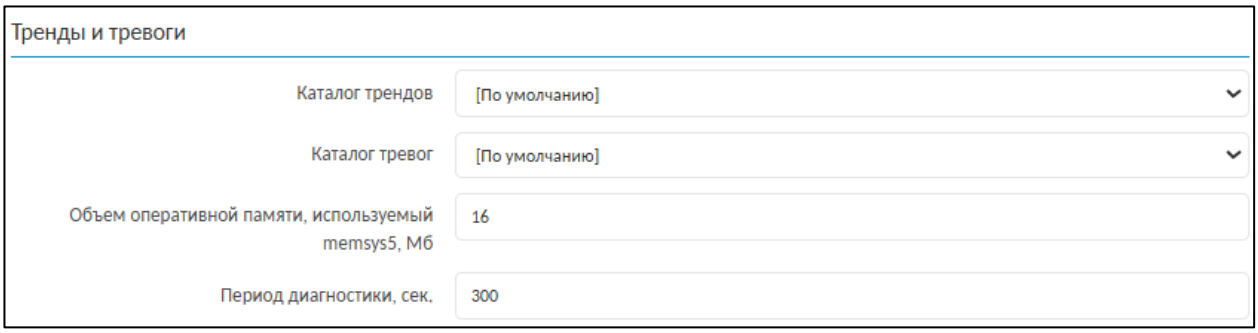


Рисунок 4-5: Страница «Настройки CODESYS». Тренды и тревоги

4.2.4 Разное

В подразделе «Разное» (см. рисунок 4-6) размещены дополнительные кнопки для управления ядром CODESYS и пользовательским проектом.

- «Очистить retain память...» — кнопка для очистки retain-памяти (энергонезависимой памяти, сохраняющей значения переменных при перезагрузке).
- «Перезапустить CODESYS...» — кнопка для перезапуска ядра CODESYS.

– «Удалить проект...» — кнопка для удаления загруженного пользовательского проекта.

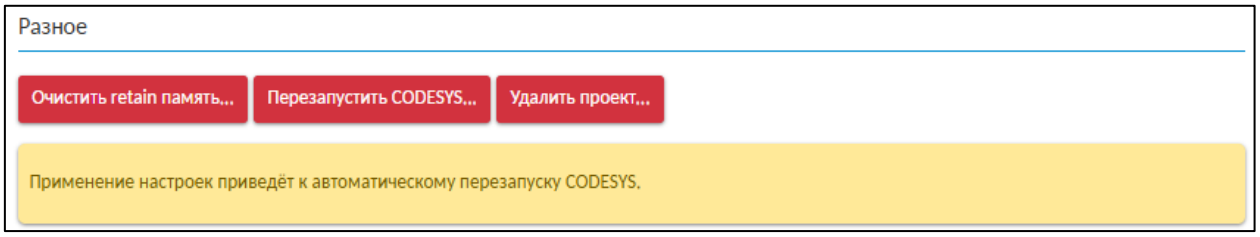


Рисунок 4-6: Страница «Настройки CODESYS». Разное

4.3 Загрузки

На странице «Загрузки» (см. рисунок 4-7) представлены ссылки для скачивания файлов, необходимых для работы с устройством.

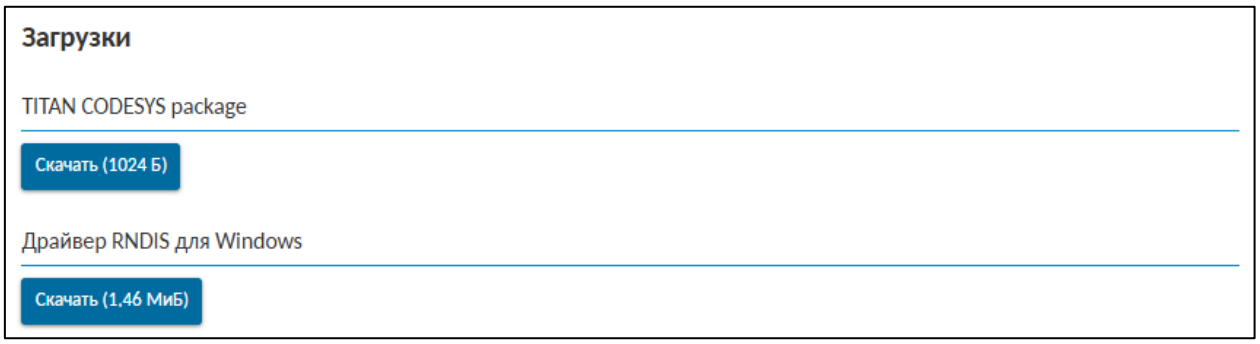


Рисунок 4-7: Страница «Загрузки»

«TITAN CODESYS package» — пакет для работы с CODESYS. Кнопка «Скачать (1024 Б)» активирует загрузку пакета.

«Драйвер RNDIS для Windows» — драйвер для организации сетевого подключения через USB (RNDIS). Кнопка «Скачать (1,46 МБ)» активирует загрузку драйвера.

4.4 Приложение

На странице «Приложение» (см. рисунок 4-8) отображается информация о загруженном пользовательском приложении CODESYS, а также монитор задач с параметрами выполнения.

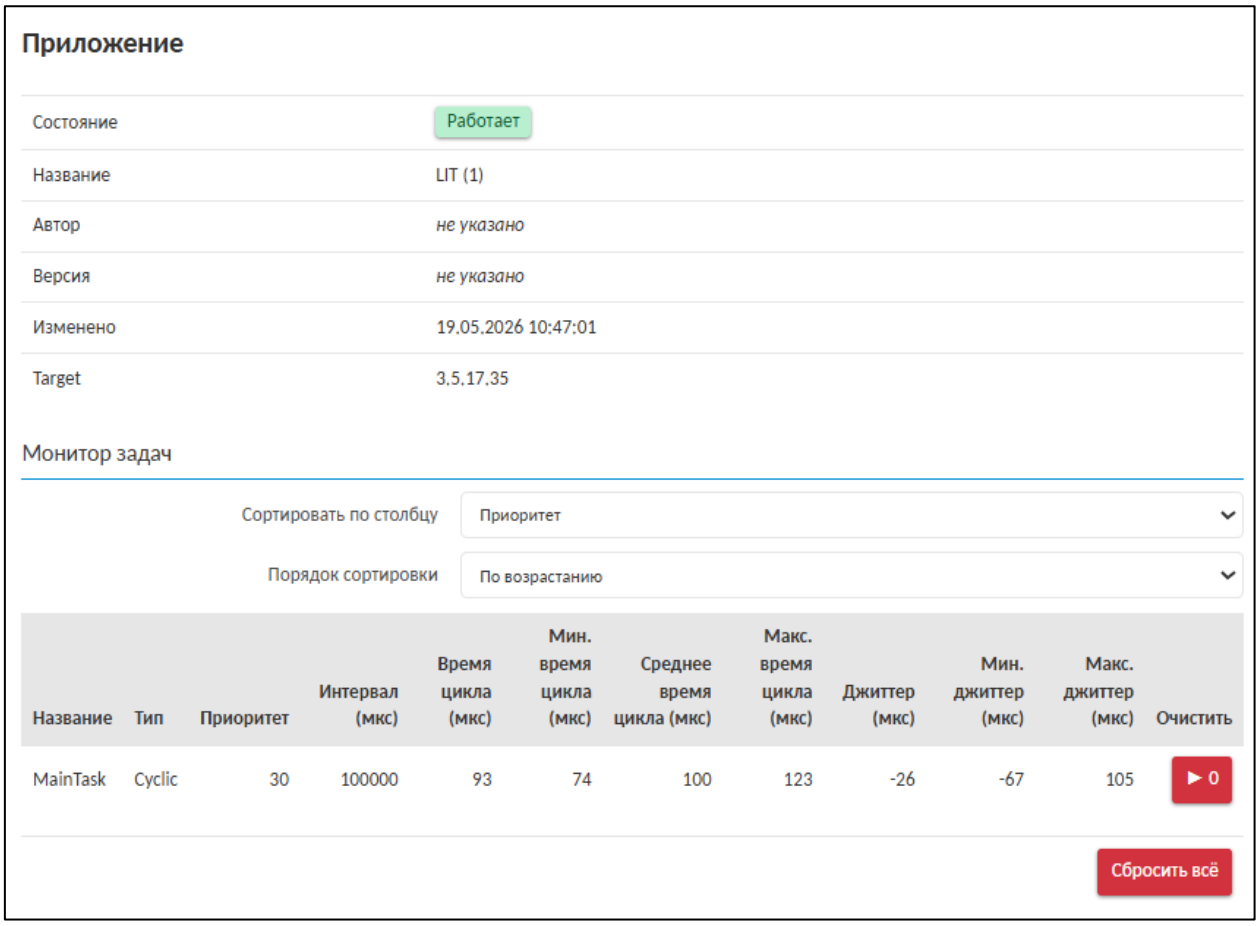


Рисунок 4-8: Страница «Приложение»

Страница содержит следующие элементы:

«Состояние» — текущее состояние приложения;

«Название» — имя загруженного приложения;

«Автор» — автор приложения (если указан);

«Версия» — версия приложения (если указана);

«Изменено» — дата и время последнего изменения приложения;

«Target» — версия target-файла CODESYS.

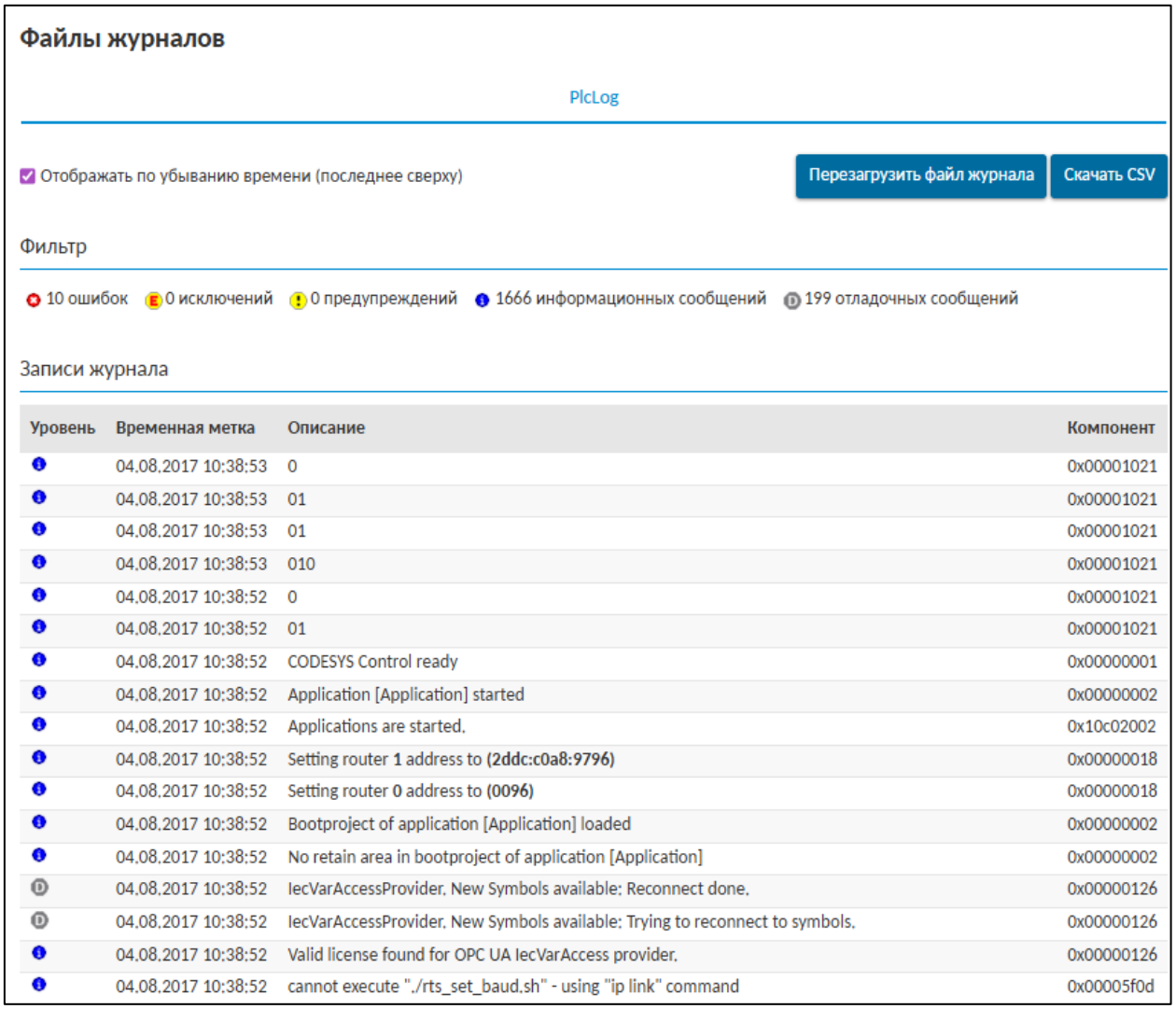
В подразделе «Монитор задач» отображается таблица задач реального времени, выполняемых в приложении. Доступна сортировка:

– «Сортировать по столбцу» — выбор столбца для сортировки (например, «Приоритет»).
– «Порядок сортировки» — выбор направления сортировки («По возрастанию» или «По убыванию»).

В нижней части страницы расположена кнопка «Сбросить всё», которая сбрасывает статистику для всех задач.

4.5 Файлы журналов

На странице «Файлы журналов» (см. рисунок 4-9) отображается журнал работы ядра CODESYS (PlcLog). Страница позволяет просматривать, фильтровать и экспортировать записи журнала.



Уровень	Временная метка	Описание	Компонент
	04.08.2017 10:38:53	0	0x00001021
	04.08.2017 10:38:53	01	0x00001021
	04.08.2017 10:38:53	01	0x00001021
	04.08.2017 10:38:53	010	0x00001021
	04.08.2017 10:38:52	0	0x00001021
	04.08.2017 10:38:52	01	0x00001021
	04.08.2017 10:38:52	CODESYS Control ready	0x00000001
	04.08.2017 10:38:52	Application [Application] started	0x00000002
	04.08.2017 10:38:52	Applications are started.	0x10c02002
	04.08.2017 10:38:52	Setting router **1** address to **(2ddc:c0a8:9796)**	0x00000018
	04.08.2017 10:38:52	Setting router **0** address to **(0096)**	0x00000018
	04.08.2017 10:38:52	Bootproject of application [Application] loaded	0x00000002
	04.08.2017 10:38:52	No retain area in bootproject of application [Application]	0x00000002
	04.08.2017 10:38:52	IecVarAccessProvider. New Symbols available: Reconnect done.	0x00000126
	04.08.2017 10:38:52	IecVarAccessProvider. New Symbols available: Trying to reconnect to symbols.	0x00000126
	04.08.2017 10:38:52	Valid license found for OPC UA IecVarAccess provider.	0x00000126
	04.08.2017 10:38:52	cannot execute "./rts_set_baud.sh" - using "ip link" command	0x00005f0d

Рисунок 4-9: Страница «Файлы журналов»

В верхней части страницы расположены следующие элементы управления:

– «Отображать по убыванию времени (последнее сверху)» — при включении данной опции самые свежие записи отображаются в начале таблицы.
– «Перезагрузить файл журнала» — кнопка для принудительного обновления содержимого журнала.
– «Скачать CSV» — кнопка для экспорта журнала в формате CSV (значения, разделённые запятыми).
– Фильтр по уровню — при нажатии на соответствующий элемент отображаются только записи выбранного уровня.

Ниже на странице находятся записи журнала. Таблица журнала имеет следующие столбцы:

– «Уровень» — уровень важности события (Error, Warning, Info, Debug).
– «Временная метка» — дата и время регистрации события.
– «Описание» — текстовое описание события или код ошибки.
– «Компонент» — идентификатор компонента, сгенерировавшего событие.

5 Службы

5.1 DDNS

На странице «Динамический DNS» раздела «Службы» производится настройка автоматического обновления DNS-записей для доменных имён при изменении IP-адреса устройства.

Страница разделена на вкладки:

– «Информация» (см. раздел 5.1.1);
– «Глобальные настройки» (см. раздел 5.1.2);
– «Службы» (см. раздел 5.1.3).

5.1.1 Вкладка «Информация»

На вкладке «Информация» (см. рисунок 5-1) отображается общая информация о состоянии и версии DDNS-клиента, а также элементы управления для его запуска и обновления.

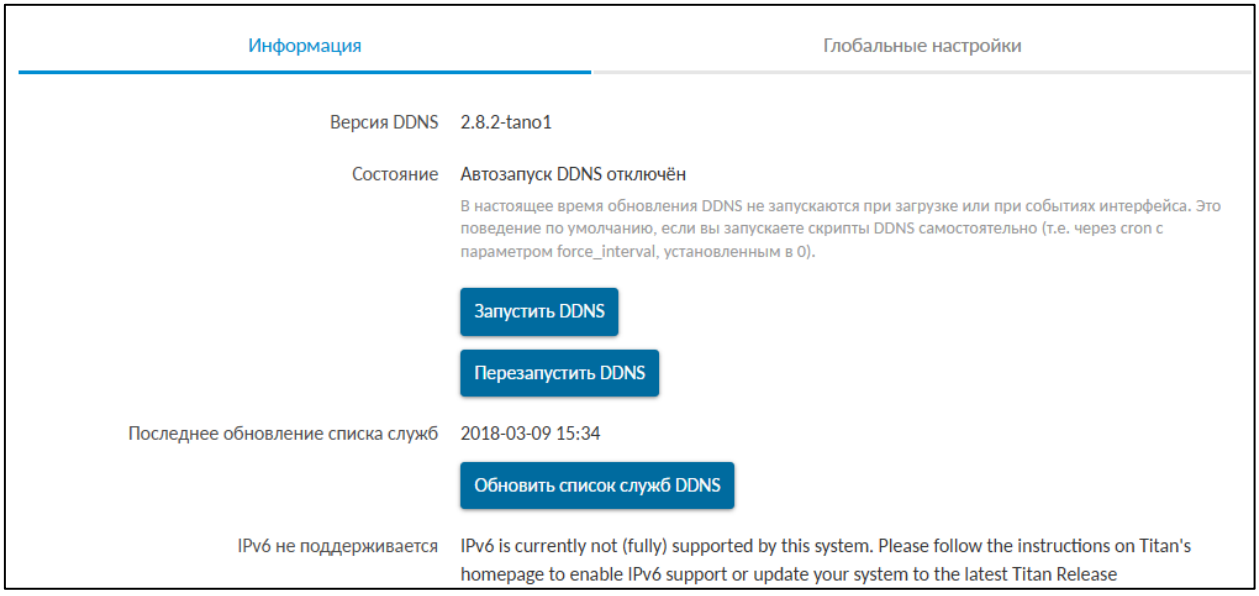


Рисунок 5-1: Страница «Динамический DNS». Вкладка «Информация»

На вкладке доступны следующие элементы:

– «Версия DDNS» — версия установленного пакета DDNS $
– «Состояние» — текущее состояние DDNS-клиента. Сообщает, включён ли автозапуск DDNS при загрузке и при событиях интерфейса;

– «Запустить DDNS» — кнопка для немедленного запуска всех настроенных DDNS-служб;
– «Перезапустить DDNS» — кнопка для перезапуска всех настроенных DDNS-служб;
– «Последнее обновление списка служб» — дата и время последнего обновления встроенного списка поддерживаемых DDNS-провайдеров;
– «Обновить список служб DDNS» — кнопка для принудительного обновления списка поддерживаемых DDNS-провайдеров из внешнего источника.

IPv6 в данной системе не поддерживается.

5.1.2 Вкладка «Глобальные настройки»

На вкладке «Глобальные настройки» (см. рисунок 5-2) расположены общие параметры DDNS-клиента, влияющие на поведение всех служб.

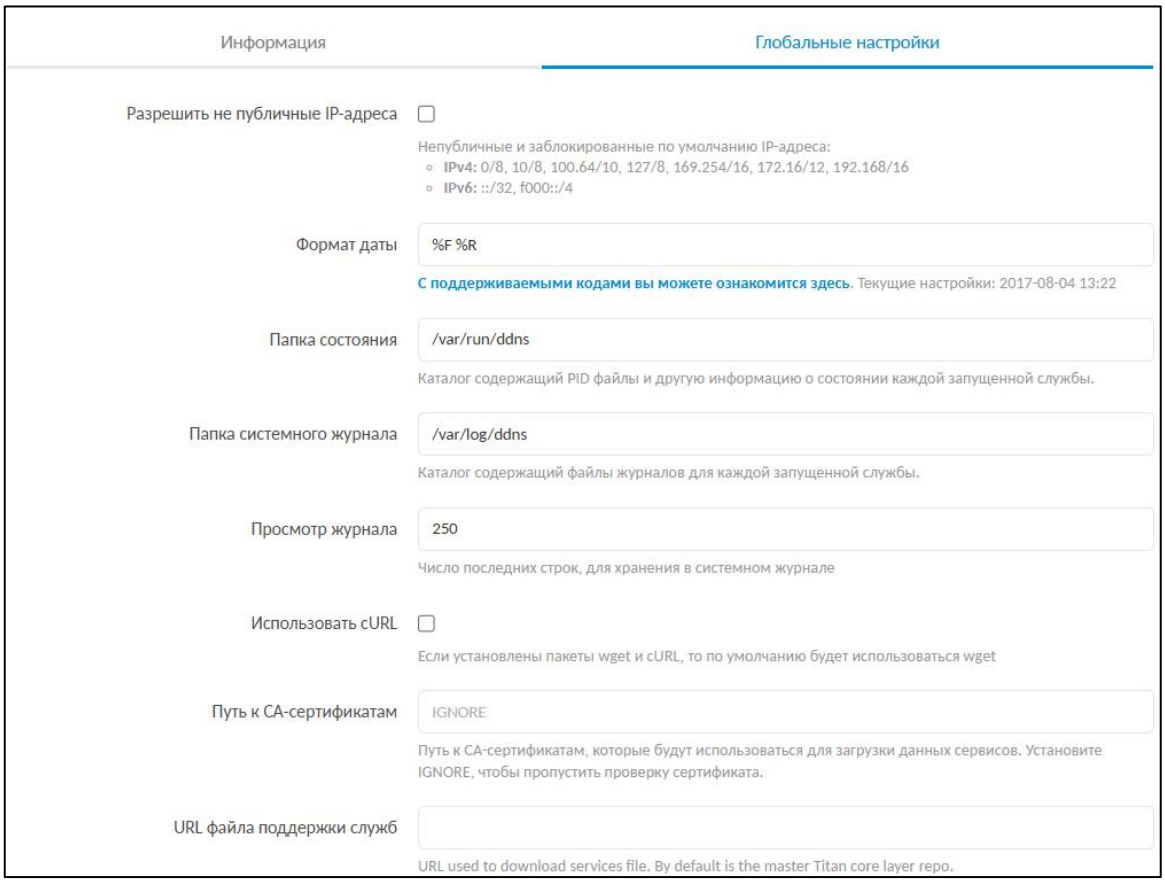


Рисунок 5-2: Страница «Динамический DNS». Вкладка «Глобальные настройки»

На вкладке доступны следующие настройки:

– «Разрешить не публичные IP-адреса» — при включении данной опции разрешается использование приватных IP-адресов для обновления DDNS.
– «Формат даты» — определяет формат отображения даты и времени в интерфейсе DDNS.
– «Папка состояния» — путь к директории, в которой хранятся PID-файлы и другая информация о состоянии каждой запущенной DDNS-службы.
– «Папка системного журнала» — путь к директории, в которой хранятся файлы журналов для каждой запущенной DDNS-службы.
– «Просмотр журнала» — число сохраняемых строк журнала для каждой службы.
– «Использовать cURL» — выбор предпочтительного инструмента для HTTP-запросов.
– «Путь к CA-сертификатам» — путь к CA-сертификатам, используемым для проверки сертификатов при загрузке данных сервисов.
– «URL файла поддержки служб» — URL-адрес для загрузки файла со списком поддерживаемых DDNS-провайдеров.

5.1.3 Подраздел «Службы» (список DDNS-сервисов)

В подразделе «Службы» (см. рисунок 5-3) отображается таблица всех настроенных DDNS-служб.

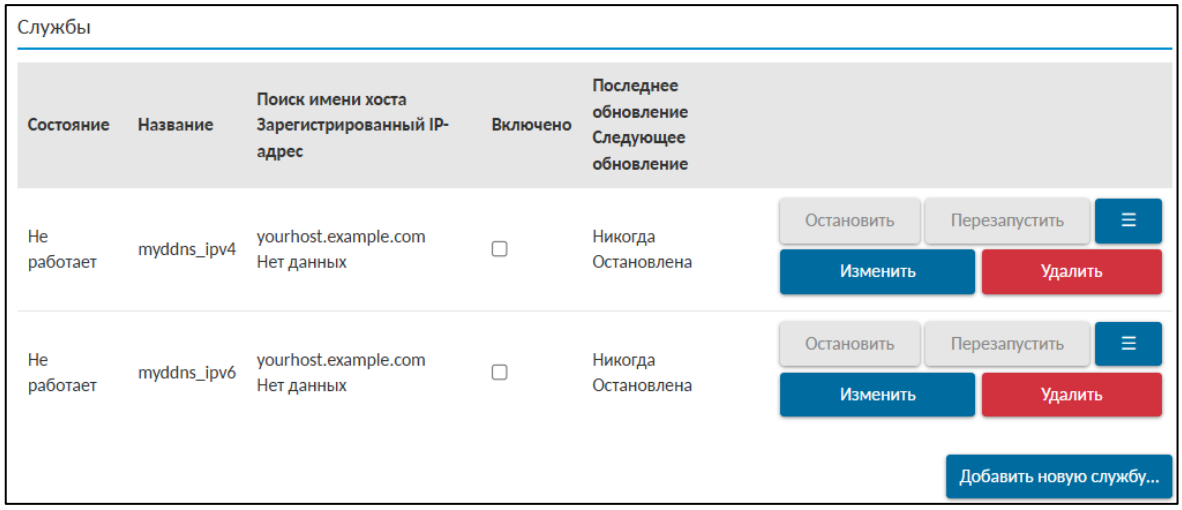


Рисунок 5-3: Страница «Динамический DNS». Подраздел «Службы»

Таблица имеет следующие столбцы:

- «Состояние» — текущее состояние службы;
- «Название» — пользовательское имя;
- «Поиск имени хоста / Зарегистрированный IP-адрес» — доменное имя, которое будет обновляться, и текущий зарегистрированный IP-адрес;
- «Включено» — флаг, указывающий, активна ли данная DDNS-служба;
- «Последнее обновление / Следующее обновление» — дата и время последнего успешного обновления, а также время следующей запланированной попытки обновления.

5.1.3.1 Редактирование параметров DDNS-службы

Страница редактирования параметров DDNS-службы открывается при нажатии кнопки «Изменить» в строке соответствующей службы (см. раздел 5.1.3). Внешний вид страницы показан на рисунке 5-4.

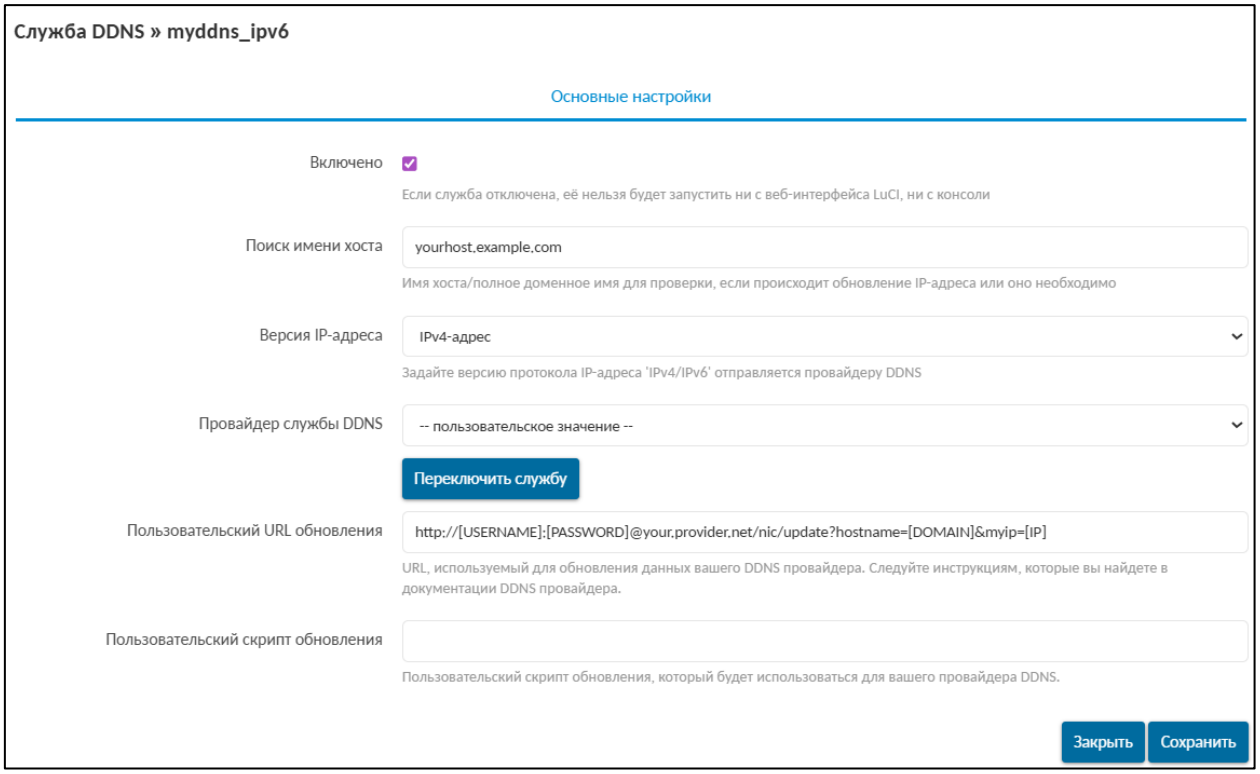


Рисунок 5-4: Страница редактирования DDNS-службы (на примере «myddns_ipv6»)

На странице доступны следующие настройки:

- «Включено» — флаг, включающий или отключающий данную DDNS-службу.

– «Поиск имени хоста» — имя хоста или полное доменное имя (FQDN), которое будет использоваться для проверки необходимости обновления IP-адреса.
– «Версия IP-адреса» — выбор версии протокола IP-адреса, который будет отправляться провайдеру DDNS.
– «Провайдер службы DDNS» — выбор провайдера DDNS-услуг из выпадающего списка.
– Кнопка «Переключить службу» меняет провайдера DDNS.
– «Пользовательский URL обновления» — URL-адрес, используемый для обновления данных у DDNS-провайдера.
– «Пользовательский скрипт обновления» — путь к пользовательскому скрипту обновления, который будет использоваться для вашего провайдера DDNS.

5.1.3.2 Добавление новой DDNS-службы

Для добавления новой DDNS-службы предназначена кнопка «Добавить новую службу...», расположенная в подразделе «Службы» (см. раздел 5.1.3). При её нажатии открывается диалоговое окно создания новой службы, внешний вид которого показан на рисунке 5-5.

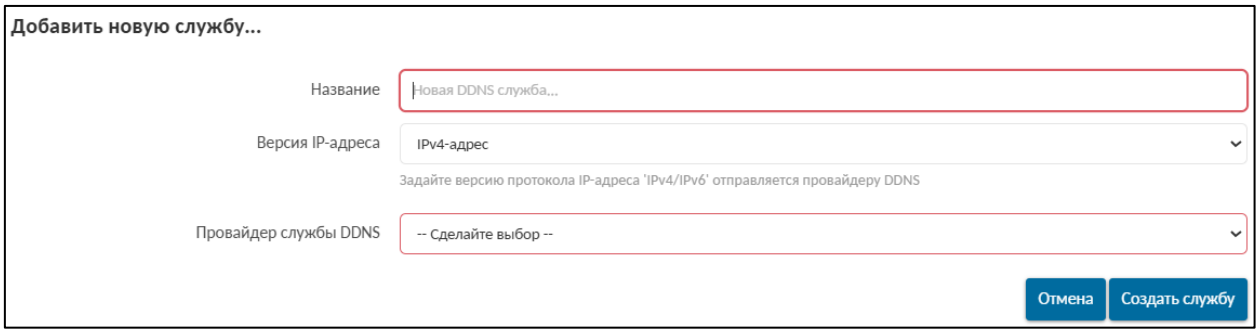


Рисунок 5-5: Добавление новой DDNS-службы

В диалоговом окне необходимо указать следующие параметры:

– «Название» — уникальное символьное имя создаваемой DDNS-службы (например, «Новая DDNS служба...»).
– «Версия IP-адреса» — выбор версии протокола IP-адреса, который будет отправляться провайдеру DDNS.

– «Провайдер службы DDNS» — выпадающий список для выбора провайдера DDNS-услуг

5.2 LLDP

LLDP (Link Layer Discovery Protocol) — это стандартизированный протокол канального уровня, позволяющий сетевым устройствам объявлять о себе и обнаруживать соседние устройства. В данном разделе описываются страницы просмотра информации о соседях и настройки службы LLDPd.

5.2.1 Состояние LLDP

Страница «Состояние LLDP» позволяет просмотреть информацию о локальном шасси, обнаруженных соседях и статистику интерфейсов.

5.2.1.1 Локальное шасси

В подразделе «Локальное шасси» (см. рисунок 5-6) отображается информация о самом устройстве:

– «Название» — имя устройства;
– «Описание» — описание системы;
– «ID» — идентификатор шасси;
– «Тип ID» — тип идентификатора;
– «IP-адреса» — IP-адреса устройства, используемые для управления.
– «Возможности» — поддерживаемые и включенные возможности устройства.

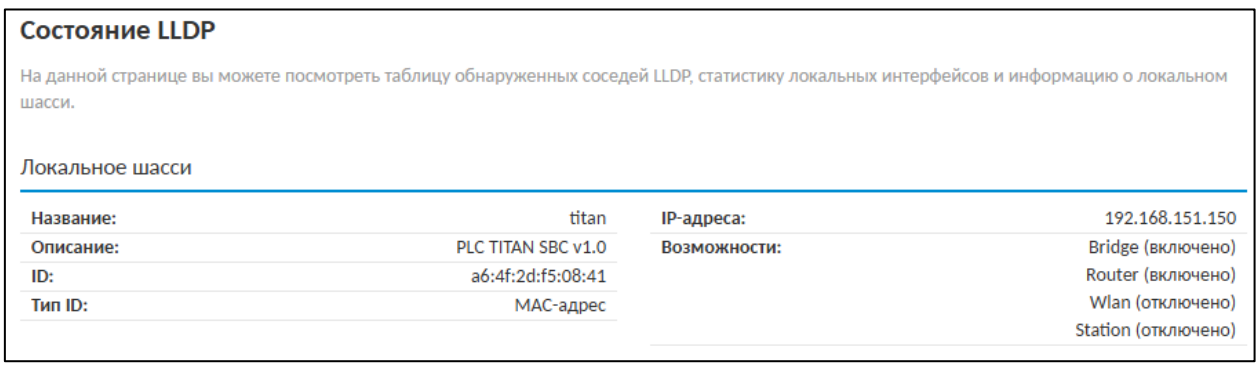


Рисунок 5-6: Страница «Состояние LLDP»

5.2.1.2 Обнаруженные соседи

В подразделе «Обнаруженные соседи» (см. рисунок 5-7) отображается таблица соседних устройств, обнаруженных по протоколам LLDP, CDP и другим. Для каждого обнаруженного соседа приводятся следующие сведения:

Локальный интерфейс:

- «Название» — имя сетевого интерфейса устройства, на котором обнаружен сосед;
- «Возраст» — время с момента последнего получения LLDP-пакета от данного соседа.

Протокол:

- «Протокол» — протокол, с помощью которого обнаружен сосед.

Обнаруженное шасси:

- «Название» — имя соседнего устройства;
- «Описание» — текстовое описание соседнего устройства;
- «ID» — идентификатор шасси соседнего устройства;
- «Тип ID» — тип идентификатора;
- «IP-адреса» — IP-адреса соседнего устройства;
- «Возможности» — поддерживаемые и включенные возможности соседнего устройства.

Обнаруженный порт:

- «ID порта» — идентификатор порта соседнего устройства, к которому подключено данное устройство;
- «Тип ID порта» — тип идентификатора порта;
- «Описание порта» — текстовое описание порта соседнего устройства;
- «TTL» — время жизни (Time To Live) полученной информации в секундах (например, «120»). По истечении этого времени запись о соседе удаляется, если не получен новый пакет.

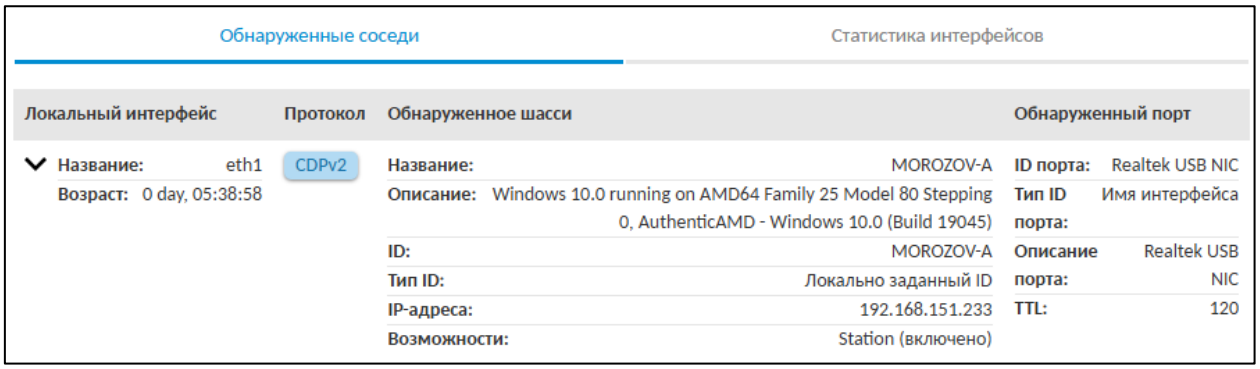


Рисунок 5-7: Страница «Состояние LLDP». Подраздел «Обнаруженные соседи»

5.2.1.3 Статистика интерфейсов

В подразделе «Статистика интерфейсов» (см. рисунок 5-8) отображается сводная информация по каждому интерфейсу: количество переданных и принятых LLDP-пакетов, ошибки, устаревшие записи и т.д.

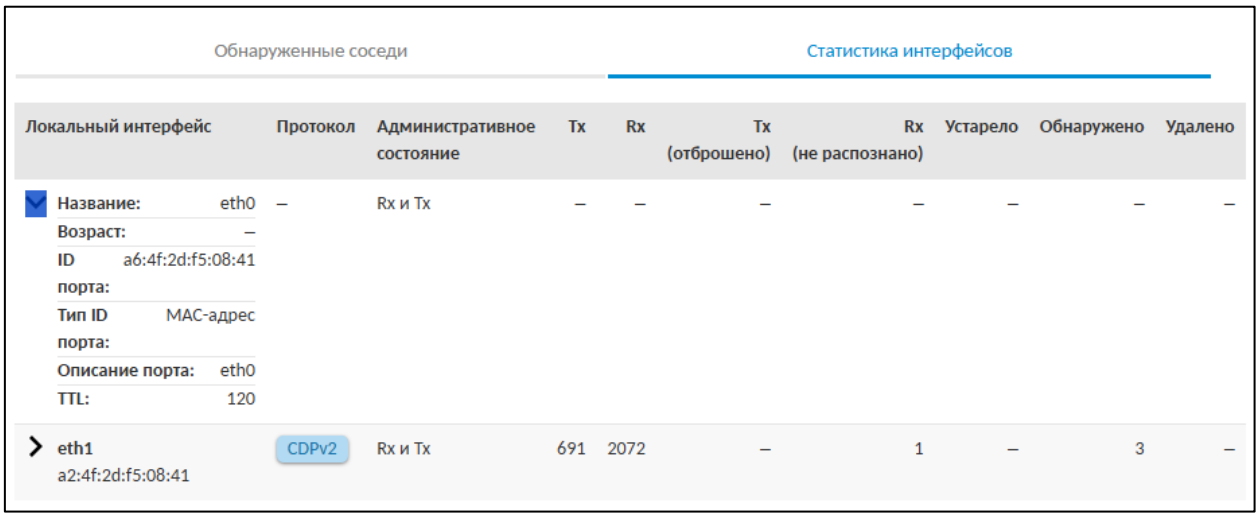


Рисунок 5-8: Страница «Состояние LLDP». Статистика интерфейсов

Таблица имеет следующие столбцы:

– «Локальный интерфейс» — имя сетевого интерфейса (например, «eth0», «eth1»), а также дополнительная информация об интерфейсе: идентификатор (ID), тип ID, описание порта, TTL (время жизни) и т.д;
– «Протокол» — протокол обнаружения, для которого ведётся статистика;
– «Административное состояние» — режим работы протокола на интерфейсе;
– «Tx» — количество переданных пакетов;
– «Rx» — количество принятых пакетов;

– «Tx (отброшено)» — количество переданных пакетов, отброшенных по различным причинам;
– «Tx (не распознано)» — количество переданных пакетов, которые не были распознаны;
– «Устарело» — количество записей о соседях, удалённых по истечении TTL;
– «Обнаружено» — количество обнаруженных соседей на данном интерфейсе;
– «Удалено» — количество удалённых записей о соседях (по любой причине);

5.2.2 Настройки LLDPd

Страница «Настройки LLDPd» (см. рисунок 5-9) позволяет сконфигурировать параметры службы LLDPd. Страница разделена на вкладки: «Основные настройки», «Сетевые интерфейсы», «Дополнительные настройки», «Поддержка протоколов».

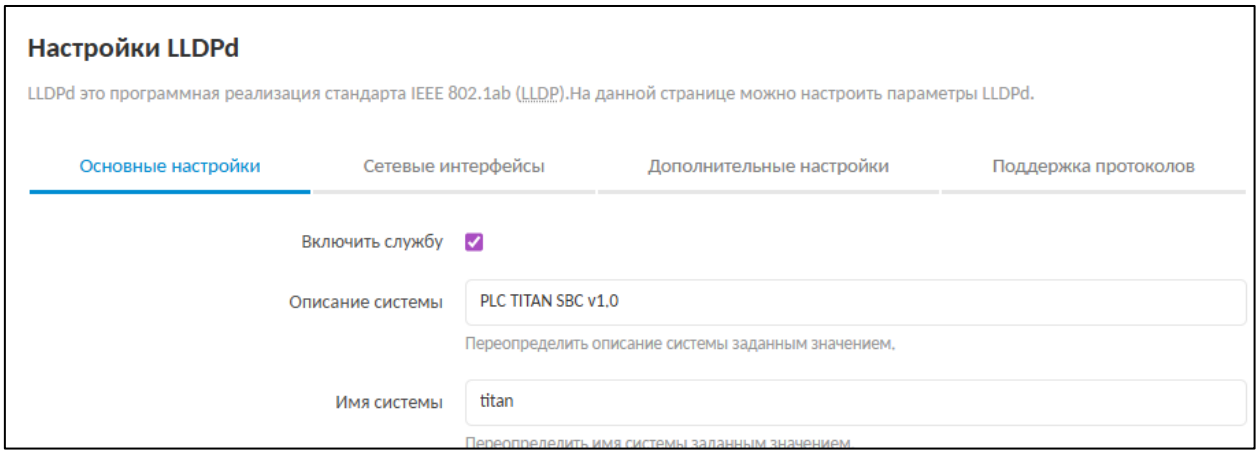


Рисунок 5-9: Страница «Настройки LLDPd»

5.2.2.1 Основные настройки

На вкладке «Основные настройки» (см. рисунок 5-10) доступны следующие параметры:

– «Включить службу» — флаг, включающий или отключающий работу LLDPd;

– «Описание системы» — переопределение системного описания;
– «Имя системы» — переопределение имени системы;
– «Описание платформы» — переопределение описания платформы;
– «Адреса управления данной системы» — переопределение адресов управления;
– «Задержка отправки» — задержка между двумя передачами LLDP PDU;
– «Значение «transmit hold»» — множитель для вычисления TTL;
– «Включить режим «только приём»» — при включении данной опции LLDPd не будет отправлять пакеты, а только прослушивать сеть для обнаружения соседей.

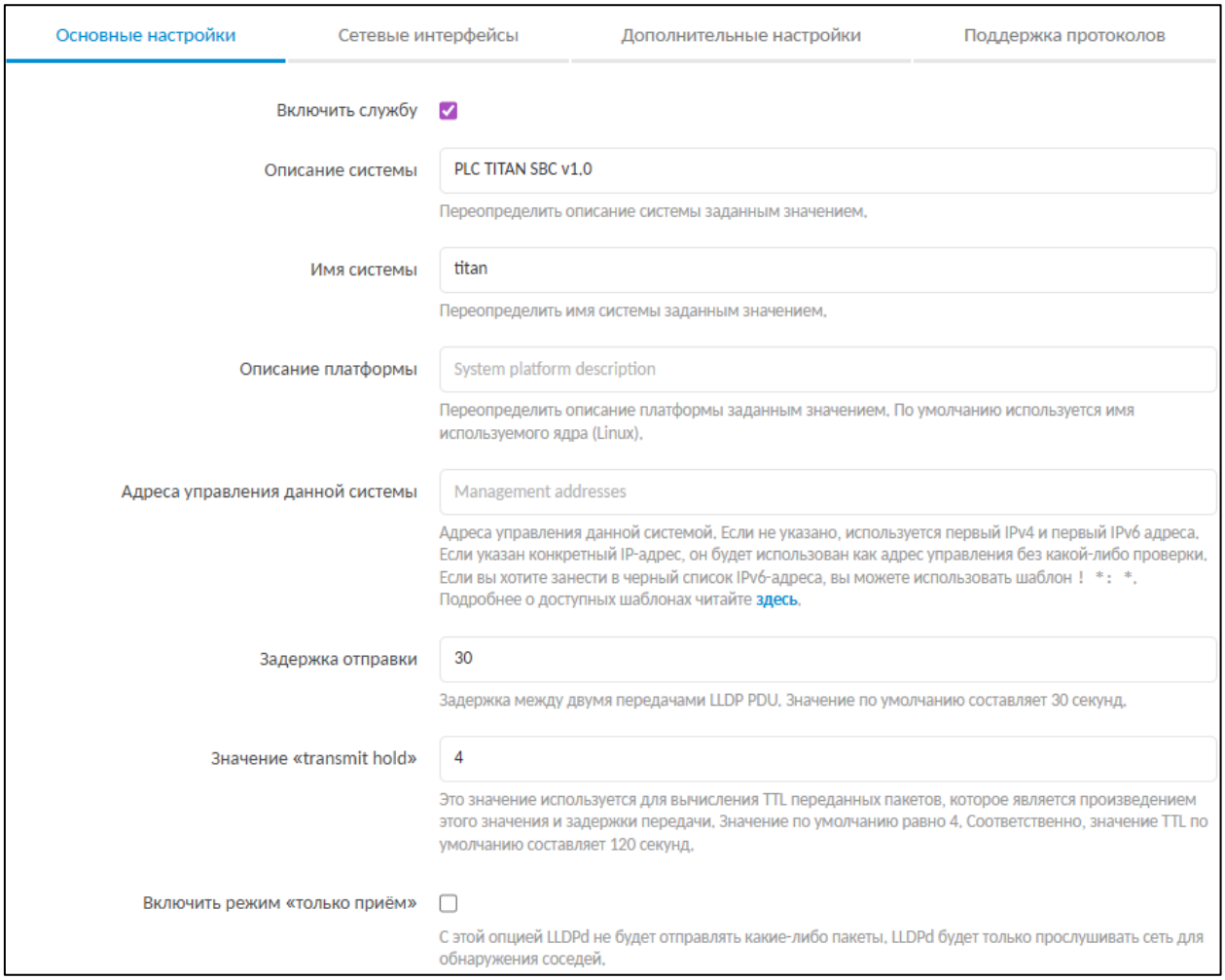


Рисунок 5-10: Вкладка «Основные настройки»

5.2.2.2 Сетевые интерфейсы

На вкладке «Сетевые интерфейсы» (см. рисунок 5-11) производится выбор интерфейсов, на которых будет работать LLDPd.

– «Сетевые интерфейсы» — список интерфейсов, которые должны прослушивать и отправлять LLDPDU;
– «Сетевые интерфейсы, используемые для вычисления ID шасси (chassis ID)» — указание интерфейсов для вычисления идентификатора шасси.

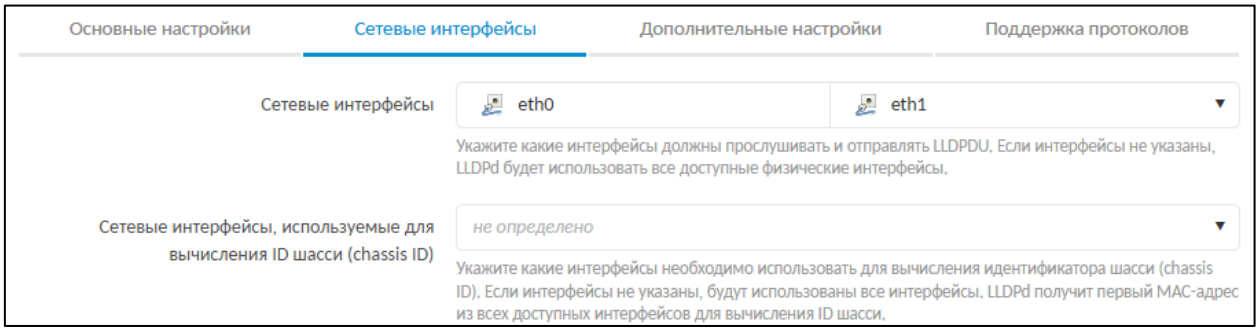


Рисунок 5-11: Вкладка «Сетевые интерфейсы»

5.2.2.3 Дополнительные настройки

На вкладке «Дополнительные настройки» (см. рисунок 5-12) доступны расширенные параметры:

– «Путь к сокету SNMP agentX» — путь к сокету SNMP AgentX;
– «Класс устройства LLDP-MED» — выбор класса устройства для LLDP-MED;
– «Отключить отправку инвентарной информации LLDP-MED TLV» — LLDPd не будет отправлять инвентарную информацию, но будет получать и публиковать её;
– «Поведение при обнаружении нескольких соседей» — таблица фильтрации входящих и исходящих пакетов для различных протоколов;
– «Использовать в качестве ID порта» — принудительное использование имени интерфейса или MAC-адреса в качестве идентификатора порта.
– «MAC-адрес назначения, используемый для отправки LLDPDU» — MAC-адрес назначения для LLDPDU.

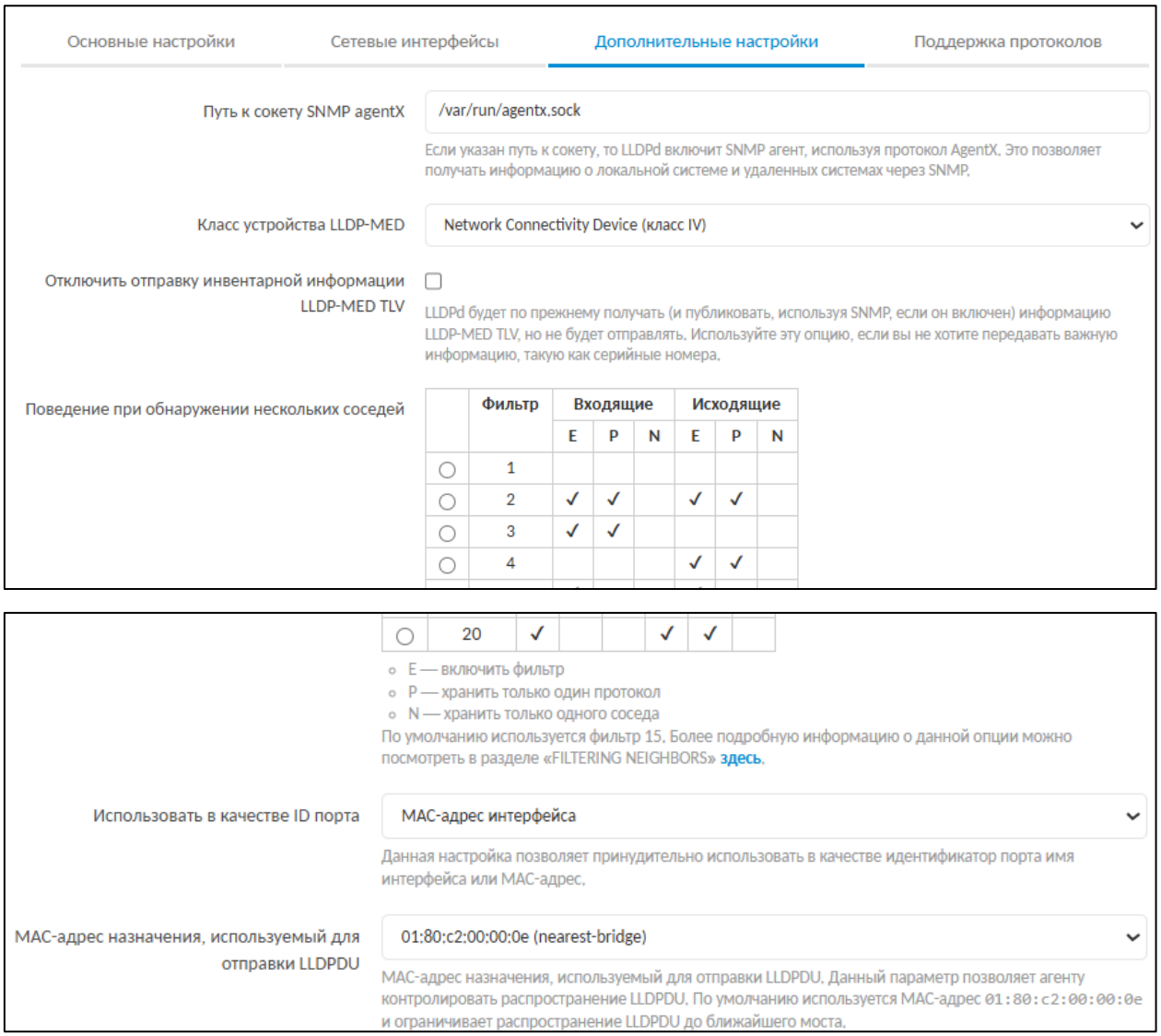


Рисунок 5-12: Вкладка «Дополнительные настройки»

5.2.2.4 Поддержка протоколов

На вкладке «Поддержка протоколов» производится настройка поддержки различных протоколов обнаружения соседей.

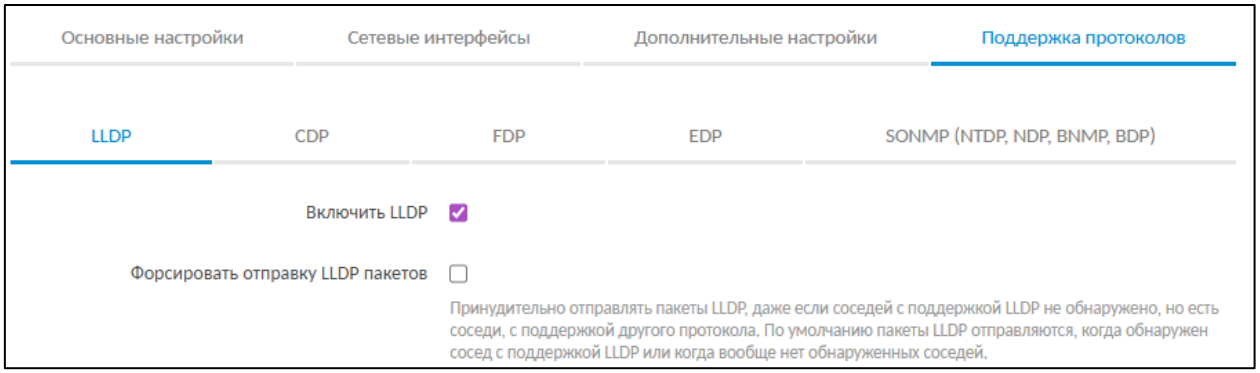


Рисунок 5-13: Вкладка «Поддержка протоколов»

5.2.2.4.1 LLDP

На вкладке настройки протокола LLDP — см. рисунок 5-13.

- «Включить LLDP» — флаг, включающий поддержку протокола LLDP.
- «Форсировать отправку LLDP пакетов» — принудительная отправка LLDP-пакетов.

5.2.2.4.2 CDP

На вкладке настройки протокола CDP (Cisco Discovery Protocol) — см. рисунок 5-14.

- «Включить CDP» — включение поддержки протокола CDP.
- «Версия протокола CDP» — выбор версии.
- «Отправлять CDP пакеты даже если не обнаружено соседей с CDP протоколом» — принудительная отправка CDP-пакетов.

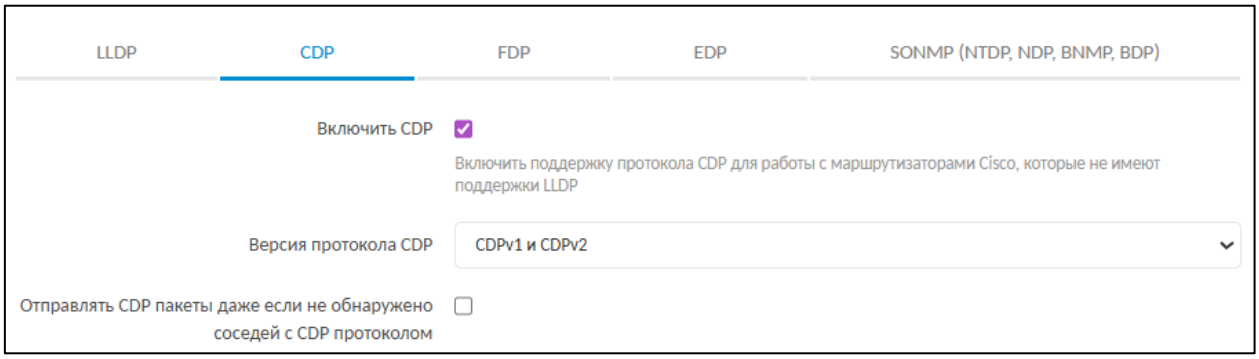


Рисунок 5-14: Настройки протокола CDP

5.2.2.4.3 FDP

На вкладке настройки протокола FDP (Foundry Discovery Protocol) — см. рисунок 5-15.

- «Включить FDP» — включение протокола FDP для работы с маршрутизаторами.
- «Отправлять FDP пакеты даже если не обнаружено соседей с FDP протоколом» — принудительная отправка FDP-пакетов.

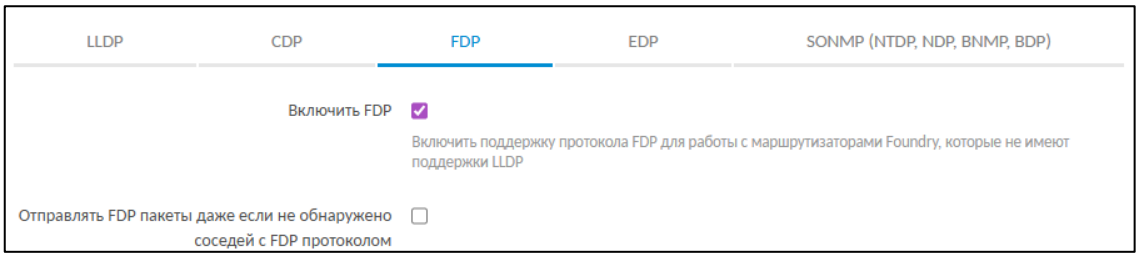


Рисунок 5-15: Настройки протокола FDP

5.2.2.4.4 EDP

На вкладке настройки протокола EDP (Extreme Discovery Protocol) — см. рисунок 5-16.

- «Включить EDP» — включение поддержки протокола EDP для работы с маршрутизаторами.
- «Отправлять EDP пакеты даже если не обнаружено соседей с EDP протоколом» — принудительная отправка EDP-пакетов.

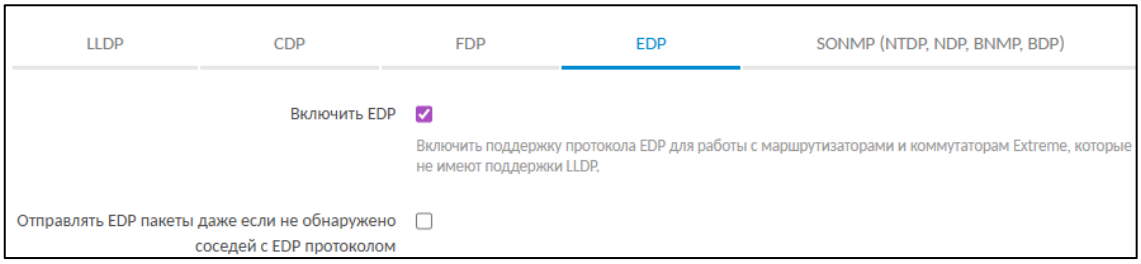


Рисунок 5-16: Настройки протокола EDP

5.2.2.4.5 SONMP

На вкладке настройки протокола SONMP (SynOptics Network Management Protocol, также известного как NDP, NTDP) — см. рисунок 5-17.

«Включить SONMP» — включение протокола SONMP для работы с маршрутизаторами.

«Отправлять SONMP пакеты даже если не обнаружено соседей с SONMP протоколом» — принудительная отправка SONMP-пакетов.

Рисунок 5-17: Настройки протокола 5.2.2.4.5 SONMP

5.3 STP/RSTP

STP (Spanning Tree Protocol) и RSTP (Rapid Spanning Tree Protocol) — это протоколы связующего дерева, предназначенные для предотвращения петель в сетях с избыточными связями. RSTP является улучшенной версией STP, обеспечивающей более быстрое восстановление связности после изменения топологии.

5.3.1 Состояние STP/RSTP

Страница «Состояние STP/RSTP» (см. рисунок 5-18) позволяет просмотреть текущее состояние мостов, управляемых протоколами STP/RSTP, и их портов.

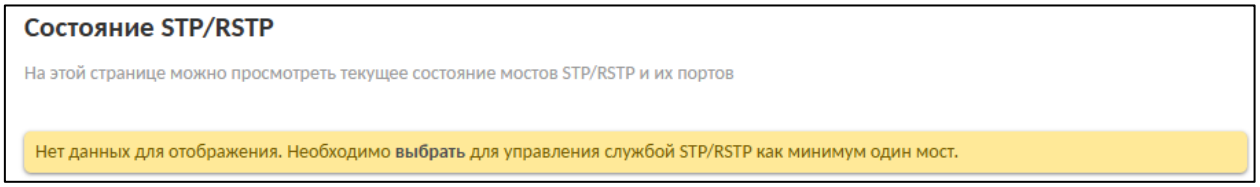


Рисунок 5-18: Страница «Состояние STP/RSTP»

При отсутствии настроенных мостов или если ни один мост не выбран для управления службой STP/RSTP, на странице отображается информационное сообщение.

5.3.2 Настройки STP/RSTP

Страница «Настройки STP/RSTP» (см. рисунок 5-19) позволяет сконфигурировать общие параметры службы STP/RSTP.

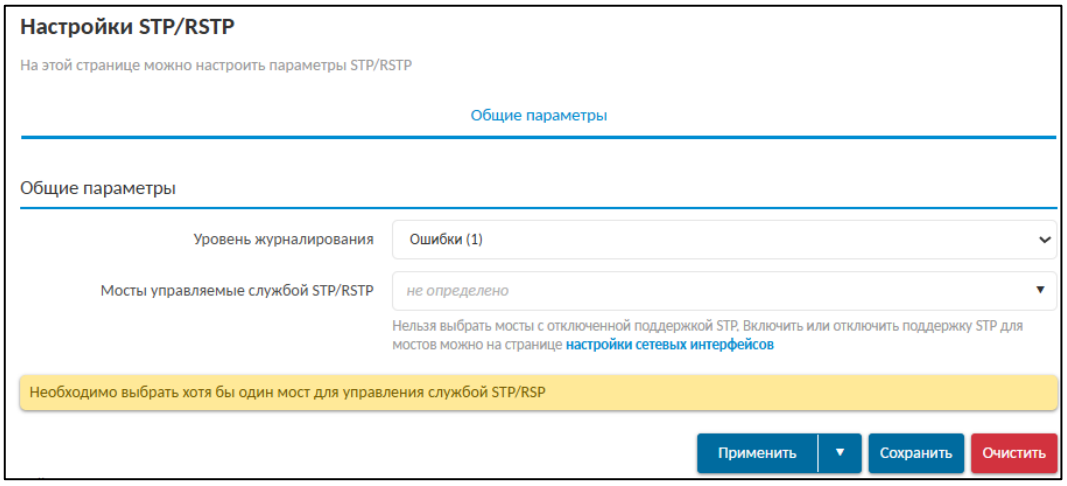


Рисунок 5-19: Страница «Настройки STP/RSTP»

На странице доступны следующие параметры:

– «Уровень журналирования» — выпадающий список для выбора уровня детализации записи событий STP/RSTP в системный журнал.
– «Мосты управляемые службой STP/RSTP» — выпадающий список для выбора мостов (например, «br-lan»), которые будут управляться службой STP/RSTP.

5.4 Настройки SNMP

SNMP (Simple Network Management Protocol) — это стандартный протокол для управления сетевыми устройствами. На странице «Настройки SNMP» раздела «Службы» производится конфигурация SNMP-агента, который предоставляет информацию об устройстве и позволяет управлять им через системы сетевого мониторинга.

Страница разделена на несколько вкладок: «Глобальные», «SNMPv1/SNMPv2c», «SNMPv3», «Трапы», «Система», «Журналирование».

5.4.1 Вкладка «Глобальные»

На вкладке «Глобальные» (см. рисунок 5-20) задаются основные параметры SNMP-агента.

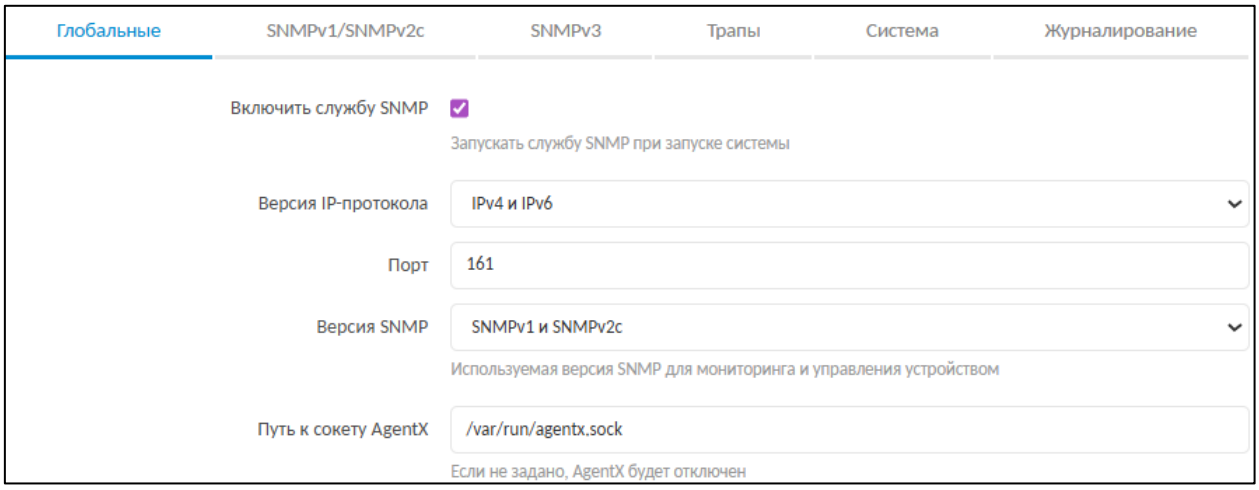


Рисунок 5-20: Настройки SNMP. Вкладка «Глобальные»

На вкладке доступны следующие настройки:

– «Включить службу SNMP» — флаг, включающий или отключающий автоматический запуск SNMP-агента при загрузке системы;

– «Версия IP-протокола» — выбор версии IP-протокола, который будет использовать SNMP-агент;
– «Порт» — UDP-порт, на котором SNMP-агент будет принимать запросы;
– «Версия SNMP» — выбор используемой версии протокола SNMP.
– «Путь к сокету AgentX» — путь к сокету AgentX для взаимодействия с другими агентами.

5.4.2 Вкладка «SNMPv1/SNMPv2c»

На вкладке «SNMPv1/SNMPv2c» (см. рисунок 5-21) настраиваются параметры аутентификации для устаревших версий протокола.

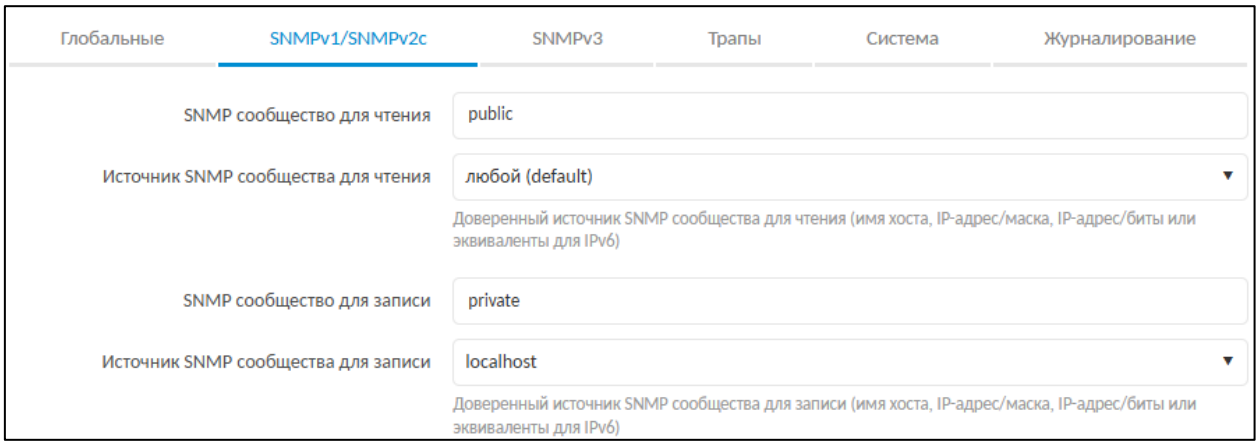


Рисунок 5-21: Настройки SNMP. Вкладка «SNMPv1/SNMPv2c»

– «SNMP сообщество для чтения» — строка сообщества (community string), используемая для чтения данных (GET-запросы).
– «Источник SNMP сообщества для чтения» — ограничение источника запросов для чтения.
– «SNMP сообщество для записи» — строка сообщества, используемая для записи данных (SET-запросы).
– «Источник SNMP сообщества для записи» — ограничение источника запросов для записи.

5.4.3 Вкладка «SNMPv3»

На вкладке «SNMPv3» (см. рисунок 5-22) настраиваются параметры аутентификации и шифрования для защищённой версии протокола.

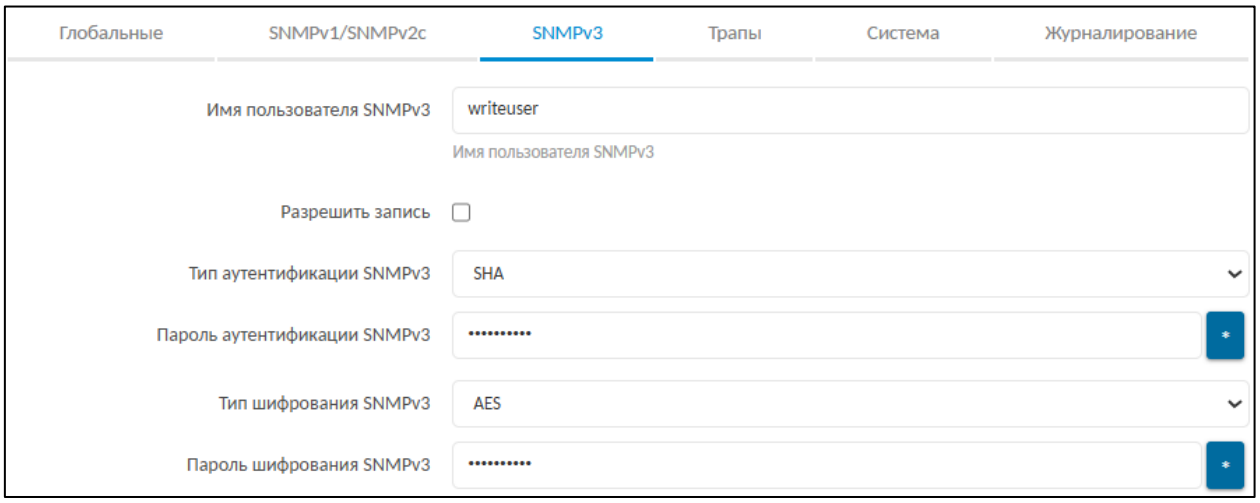


Рисунок 5-22: Настройки SNMP. Вкладка «SNMPv3»

- «Имя пользователя SNMPv3» — имя пользователя для аутентификации;
- «Разрешить запись» — флаг, разрешающий выполнение SET-запросов (запись/изменение параметров) для данного пользователя;
- «Тип аутентификации SNMPv3» — выбор алгоритма аутентификации. Доступные варианты: «SHA», «MD5»;
- «Пароль аутентификации SNMPv3» — пароль для аутентификации (скрыт символами «*»);
- «Тип шифрования SNMPv3» — выбор алгоритма шифрования. Доступные варианты: «AES», «DES»;
- «Пароль шифрования SNMPv3» — пароль для шифрования (скрыт символами «*»).

5.4.4 Вкладка «Трапы»

На вкладке «Трапы» (см. рисунок 5-23) настраиваются параметры отправки SNMP-трапов — асинхронных уведомлений о событиях.

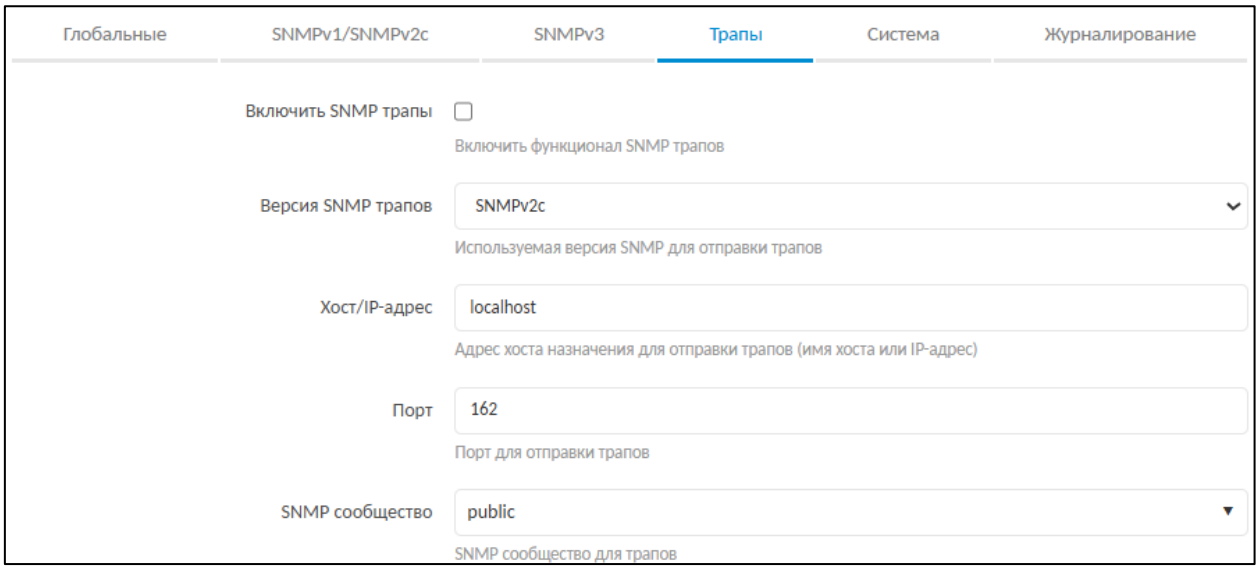


Рисунок 5-23: Настройки SNMP. Вкладка «Трапы»

- «Включить SNMP трапы» — флаг, включающий функционал отправки SNMP-трапов;
- «Версия SNMP трапов» — выбор версии протокола для отправки трапов;
- «Хост/IP-адрес» — адрес хоста назначения для отправки трапов;
- «Порт» — порт для отправки трапов;
- «SNMP сообщество» — строка сообщества для трапов.

5.4.5 Вкладка «Система»

На вкладке «Система» (см. рисунок 5-24) задаются идентификационные сведения об устройстве, которые будут возвращаться SNMP-агентом.

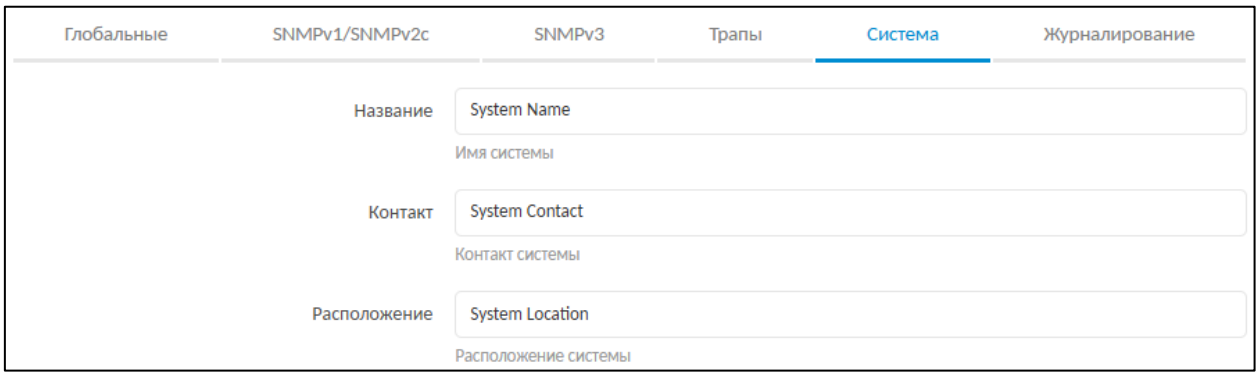


Рисунок 5-24: Настройки SNMP. Вкладка «Система»

- «Название» — имя системы (sysName);

– «Контакт» — контактная информация об администраторе системы (sysContact);
– «Расположение» — физическое расположение устройства (sysLocation).

5.4.6 Вкладка «Журналирование»

На вкладке «Журналирование» (см. рисунок 5-25) настраиваются параметры записи событий SNMP-агента в журналы.

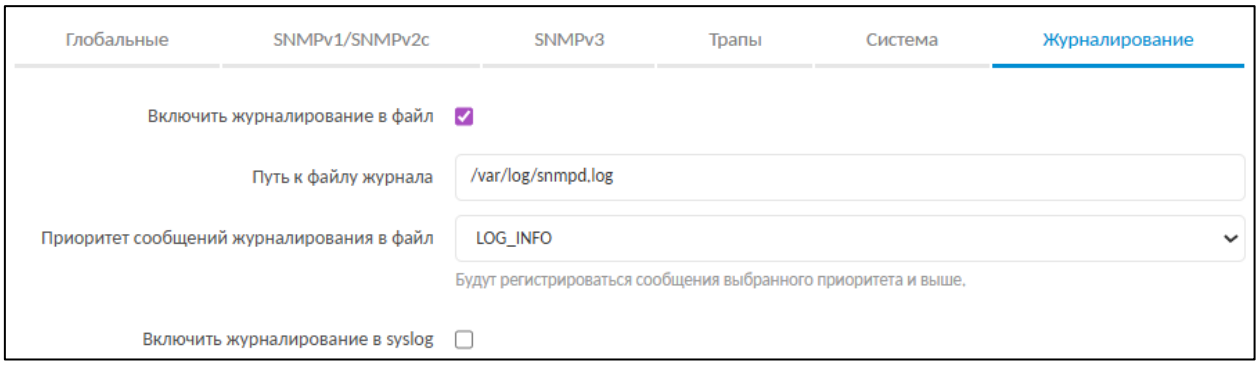


Рисунок 5-25: Настройки SNMP. Вкладка «Журналирование»

– «Включить журналирование в файл» — флаг, включающий запись событий в файл;
– «Путь к файлу журнала» — путь к файлу журнала;
– «Приоритет сообщений журналирования в файл» — минимальный приоритет сообщений, которые будут записываться в файл;
– «Включить журналирование в syslog» — флаг, включающий отправку событий SNMP-агента в системный журнал (syslog).

5.5 Настройки FTP-сервера

FTP-сервер (vsftpd — Very Secure FTP Daemon) позволяет организовать доступ к файлам устройства по протоколам FTP и FTPS. На странице «Настройки FTP-сервера» раздела «Службы» производится конфигурация параметров доступа, пользователей и журналирования.

Страница разделена на несколько вкладок: «Настройки службы», «Настройки подключения», «Основные настройки», «Локальные пользователи», «Виртуальные пользователи», «Анонимный доступ», «Настройки журналирования».

5.5.1 Вкладка «Настройки службы»

На вкладке «Настройки службы» (см. рисунок 5-26) задаются основные параметры запуска FTP-сервера и сетевых интерфейсов.

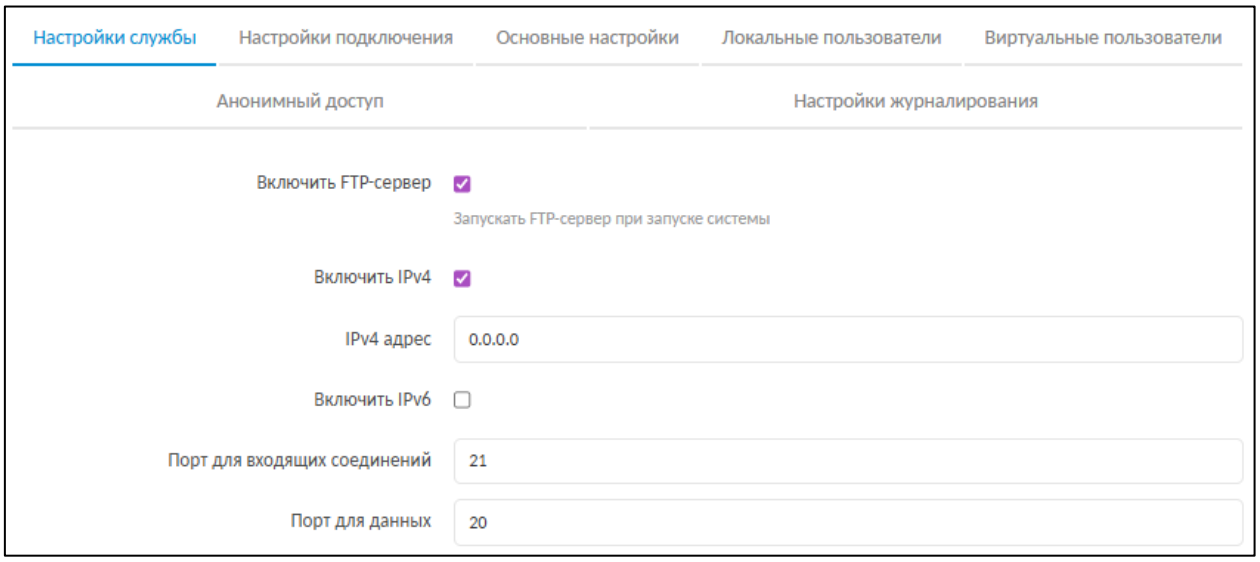


Рисунок 5-26: Настройки FTP-сервера. Вкладка «Настройки службы»

- «Включить FTP-сервер» — флаг, включающий автоматический запуск FTP-сервера при загрузке системы;
- «Включить IPv4» — флаг, включающий поддержку протокола IPv4;
- «IPv4 адрес» — IP-адрес, на котором сервер будет принимать входящие соединения. Значение 0.0.0.0 означает «все доступные IPv4-адреса»;
- «Включить IPv6» — флаг, включающий поддержку протокола IPv6;
- «Порт для входящих соединений» — TCP-порт для управления (команд);
- «Порт для данных» — TCP-порт для передачи данных.

5.5.2 Вкладка «Настройки подключения»

На вкладке «Настройки подключения» (см. рисунок 5-27) настраиваются параметры сетевых соединений и режимов работы FTP.

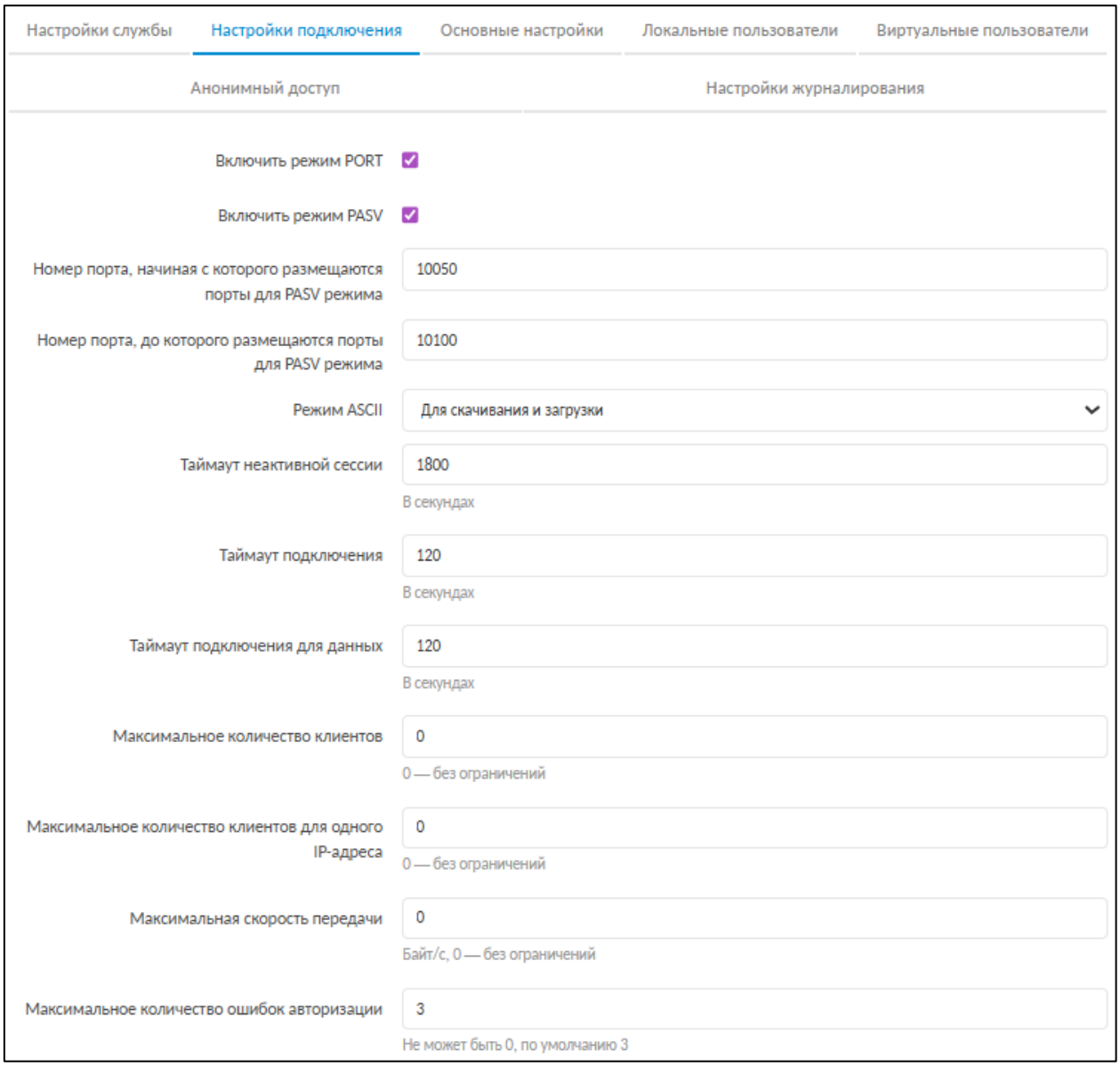


Рисунок 5-27: Настройки FTP-сервера. Вкладка «Настройки подключения»

- «Включить режим PORT» — флаг, включающий активный режим передачи данных (PORT). В активном режиме сервер сам устанавливает соединение с клиентом для передачи данных;
- «Включить режим PASV» — флаг, включающий пассивный режим передачи данных (PASV). В пассивном режиме клиент сам устанавливает соединение с сервером. Рекомендуется для клиентов за NAT;
- «Номер порта, начиная с которого размещаются порты для PASV режима» — начало диапазона портов для пассивного режима;

- «Номер порта, до которого размещаются порты для PASV режима» — конец диапазона портов для пассивного режима;
- «Режим ASCII» — флаг, включающий поддержку текстового режима передачи (ASCII). При включении текстовые файлы передаются с преобразованием перевода строки;
- «Таймаут неактивной сессии» — время ожидания бездействия сессии в секундах;
- «Таймаут подключения» — таймаут установки соединения в секундах;
- «Таймаут подключения для данных» — таймаут для установки соединения передачи данных в секундах;
- «Максимальное количество клиентов» — максимальное количество одновременно подключённых клиентов;
- «Максимальное количество клиентов для одного IP-адреса» — максимальное количество одновременных соединений с одного IP-адреса;
- «Максимальная скорость передачи» — максимальная скорость передачи данных в байтах/с;
- «Максимальное количество ошибок авторизации» — количество допустимых ошибок ввода пароля до разрыва соединения.

5.5.3 Вкладка «Основные настройки»

На вкладке «Основные настройки» (см. рисунок 5-28) настраиваются права доступа и поведение FTP-сервера.

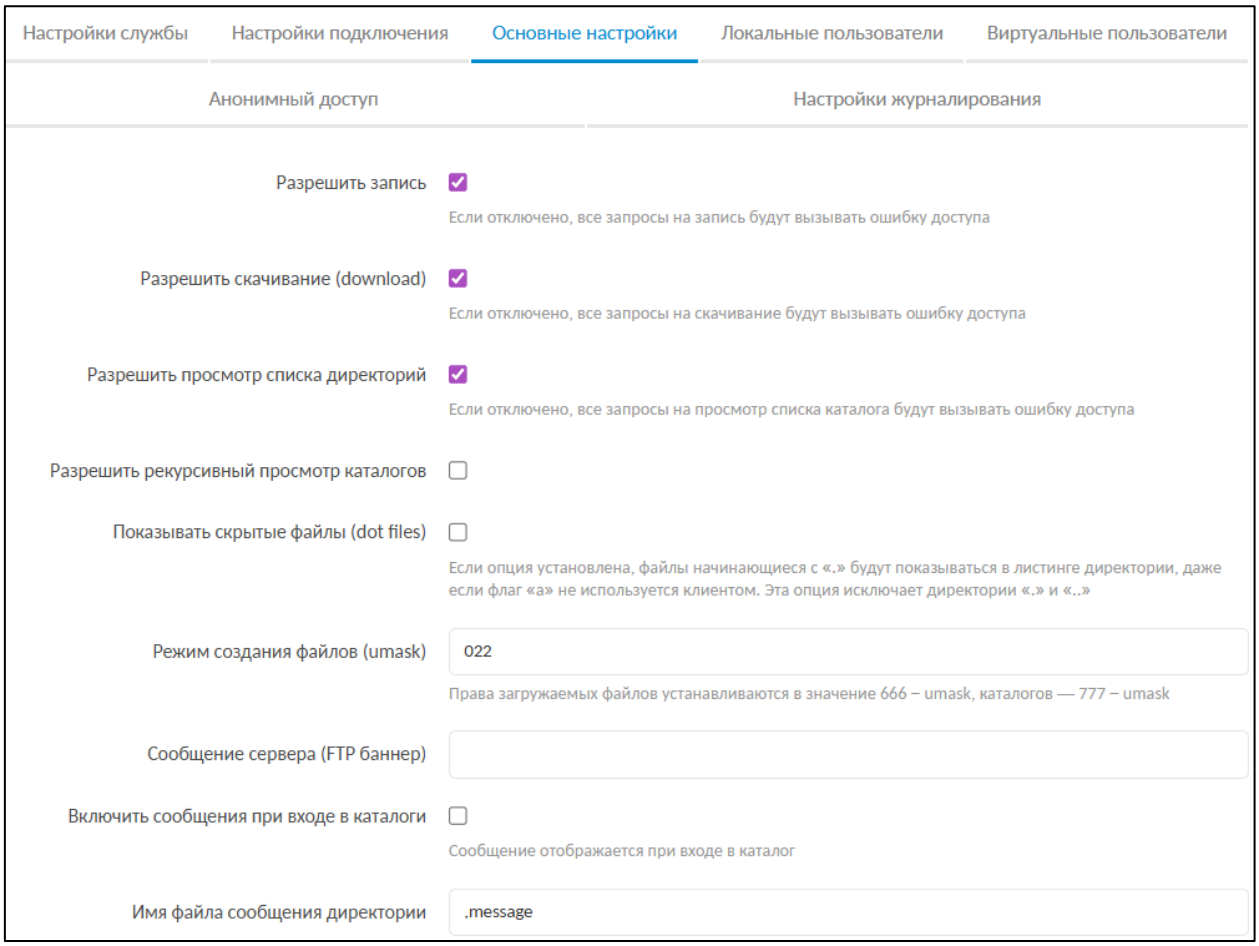


Рисунок 5-28: Настройки FTP-сервера. Вкладка «Основные настройки»

– «Разрешить запись» — флаг, разрешающий запись на сервер;
– «Разрешить скачивание (download)» — флаг, разрешающий скачивание файлов;
– «Разрешить просмотр списка директорий» — флаг, разрешающий просмотр содержимого каталогов;
– «Разрешить рекурсивный просмотр каталогов» — флаг, разрешающий рекурсивный просмотр каталогов;
– «Показывать скрытые файлы (dot files)» — флаг, определяющий, будут ли отображаться скрытые файлы;
– «Режим создания файлов (umask)» — значение umask для создаваемых файлов;
– «Сообщение сервера (FTP баннер)» — текст приветственного сообщения, отображаемого при подключении клиента;

– «Включить сообщения при входе в каталог» — флаг, включающий отображение сообщений при входе в каталог;
– «Имя файла сообщения директории» — имя файла, содержащего сообщение для отображения при входе в каталог.

5.5.4 Вкладка «Локальные пользователи»

На вкладке «Локальные пользователи» (см. рисунок 5-29) настраивается доступ для системных (локальных) пользователей устройства.

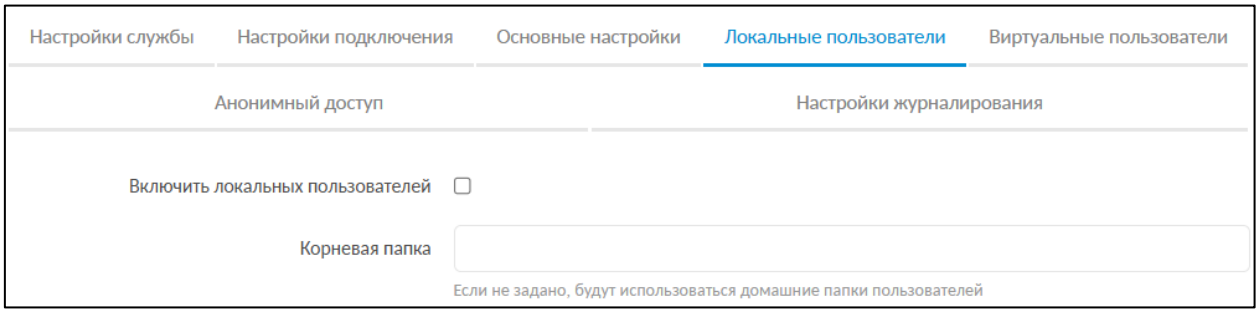


Рисунок 5-29: Настройки FTP-сервера. Вкладка «Локальные пользователи»

– «Включить локальных пользователей» — флаг, разрешающий доступ локальным пользователям системы.
– «Корневая папка» — корневая директория для локальных пользователей.

5.5.5 Вкладка «Виртуальные пользователи»

На вкладке «Виртуальные пользователи» (см. рисунок 5-30) настраиваются виртуальные пользователи FTP-сервера, которые не являются системными пользователями устройства.

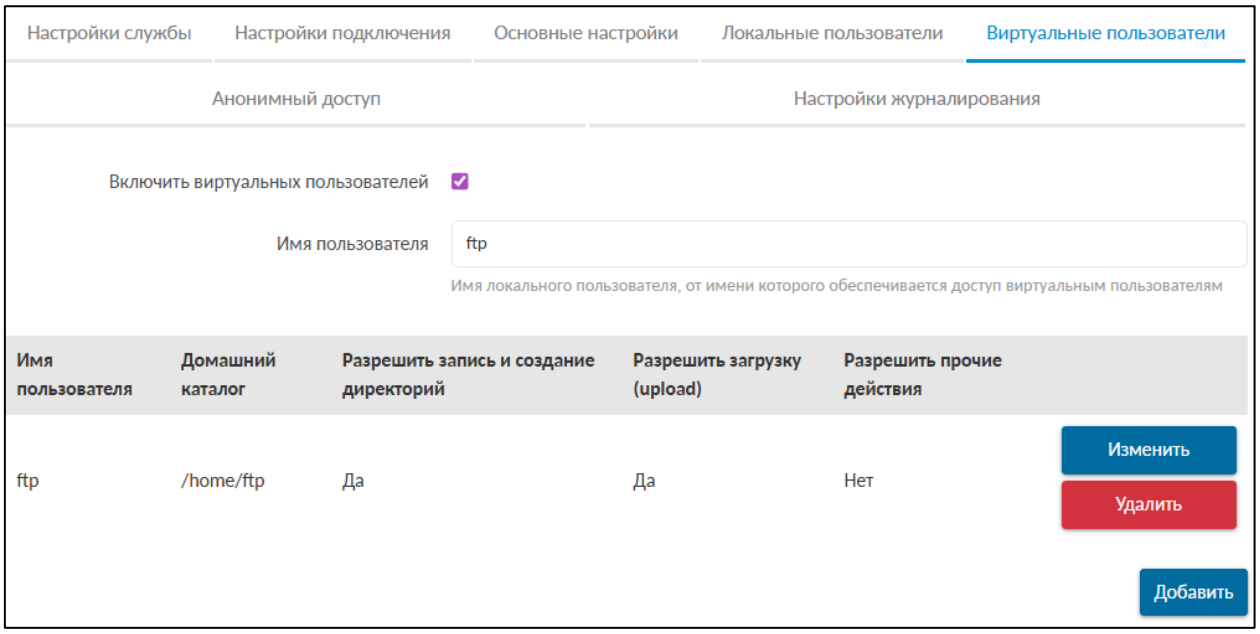


Рисунок 5-30: Настройки FTP-сервера. Вкладка «Виртуальные пользователи»

– «Включить виртуальных пользователей» — флаг, включающий поддержку виртуальных пользователей;
– «Имя пользователя» — имя локального пользователя, от имени которого обеспечивается доступ виртуальным пользователям.

Таблица виртуальных пользователей содержит следующие столбцы:

– «Имя пользователя» — имя виртуального пользователя;
– «Домашний каталог» — корневая директория для данного пользователя;
– «Разрешить запись и создание директорий» — флаг, разрешающий создание файлов и папок;
– «Разрешить загрузку (upload)» — флаг, разрешающий загрузку файлов на сервер;
– «Разрешить прочие действия» — флаг, разрешающий переименование, удаление и другие действия.

5.5.5.1 Редактирование виртуального пользователя

Страница редактирования виртуального пользователя (см. рисунок 5-31) открывается при нажатии кнопки «Изменить».

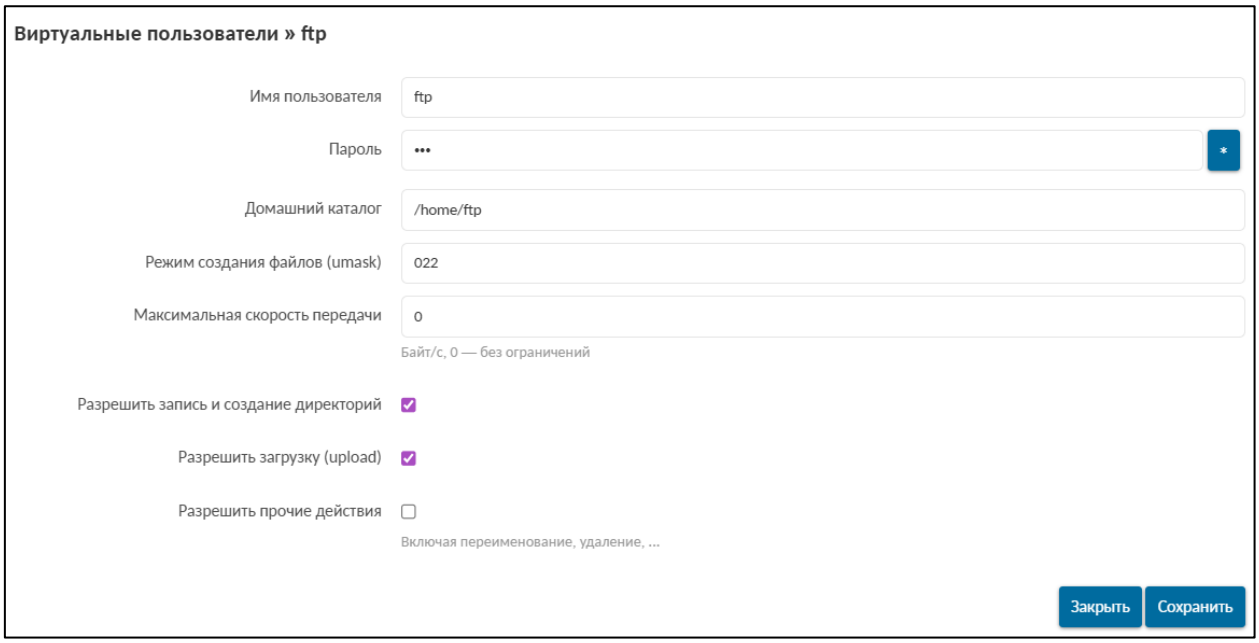


Рисунок 5-31: Редактирование виртуального пользователя

Доступны следующие параметры:

- «Имя пользователя» — имя виртуального пользователя;
- «Пароль» — пароль пользователя;
- «Домашний каталог» — корневая директория пользователя;
- «Режим создания файлов (umask)» — значение umask для создаваемых файлов;
- «Максимальная скорость передачи» — ограничение скорости в байтах/с;
- «Разрешить запись и создание директорий» — флаг, разрешающий создание файлов и папок;
- «Разрешить загрузку (upload)» — флаг, разрешающий загрузку файлов на сервер;
- «Разрешить прочие действия» — флаг, разрешающий переименование, удаление и другие действия;

5.5.5.2 Добавление виртуального пользователя

Страница добавления виртуального пользователя (см. рисунок 5-31, вызывается по кнопке «Добавить») содержит те же параметры, что и страница редактирования. Поля «Имя пользователя» и «Пароль» должны быть заполнены обязательно.

5.5.6 Вкладка «Анонимный доступ»

На вкладке «Анонимный доступ» (см. рисунок 5-32) настраиваются параметры доступа для анонимных пользователей.

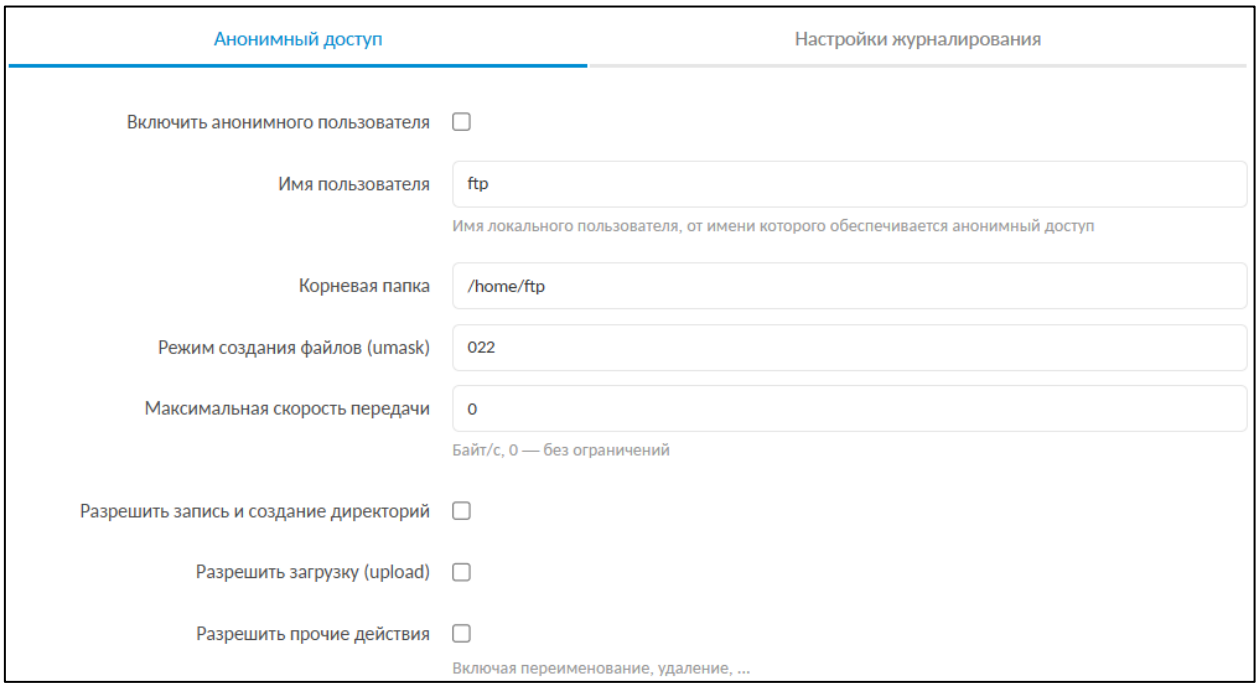


Рисунок 5-32: Настройки FTP-сервера. Вкладка «Анонимный доступ»

- «Включить анонимного пользователя» — флаг, включающий анонимный доступ;
- «Имя пользователя» — имя локального пользователя, от имени которого обеспечивается анонимный доступ;
- «Корневая папка» — корневая директория для анонимных пользователей;
- «Режим создания файлов (umask)» — значение umask для создаваемых файлов;
- «Максимальная скорость передачи» — ограничение скорости в байтах/с;
- «Разрешить запись и создание директорий» — флаг, разрешающий создание файлов и папок;
- «Разрешить загрузку (upload)» — флаг, разрешающий загрузку файлов на сервер;
- «Разрешить прочие действия» — флаг, разрешающий переименование, удаление и другие действия.

5.5.7 Вкладка «Настройки журналирования»

На вкладке «Настройки журналирования» (см. рисунок 5-33) настраиваются параметры записи событий FTP-сервера.

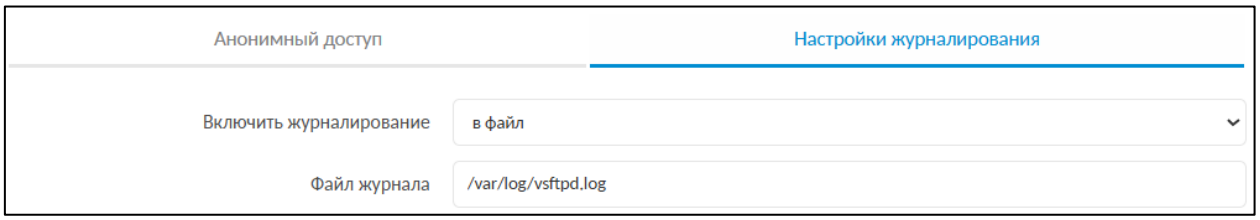


Рисунок 5-33: Настройки FTP-сервера. Вкладка «Настройки журналирования»

– «Включить журналирование в файл» — флаг, включающий запись событий в файл;
– «Файл журнала» — путь к файлу журнала. По умолчанию: /var/log/vsftpd.log.

5.6 Шлюз Modbus TCP в Modbus RTU

Шлюз Modbus TCP в Modbus RTU позволяет устройствам, поддерживающим протокол Modbus TCP, взаимодействовать с устройствами Modbus RTU, подключёнными через последовательные интерфейсы. Шлюз выполняет преобразование протоколов: принимает Modbus TCP-запросы, транслирует их в Modbus RTU и возвращает ответы обратно.

5.6.1 Конфигурация портов

Основная страница «Шлюз Modbus TCP в Modbus RTU» (см. рисунок 5-34) содержит таблицу настроенных последовательных портов.

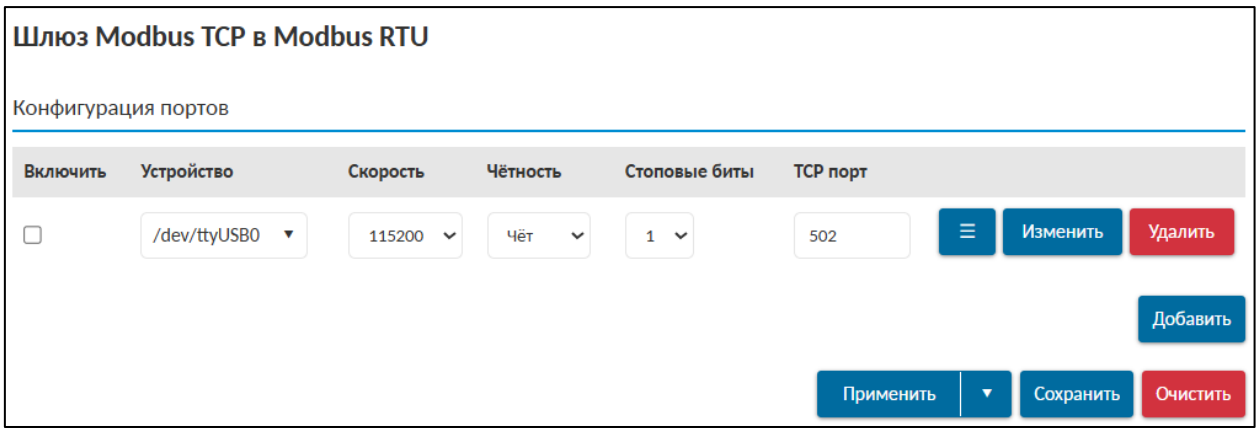


Рисунок 5-34: Шлюз Modbus TCP в Modbus RTU. Конфигурация портов

Таблица имеет следующие столбцы:

- «Включить» — флаг, включающий или отключающий шлюз для данного порта;
- «Устройство» — имя последовательного устройства (например, /dev/ttyUSB0);
- «Скорость» — скорость передачи данных в бодах (например, 115200);
- «Чётность» — режим контроля;
- «Стоповые биты» — количество стоповых битов;
- «TCP порт» — TCP-порт, на котором шлюз принимает Modbus TCP-соединения;

5.6.2 Редактирование шлюза

Страница редактирования шлюза открывается при нажатии кнопки «Изменить» в строке соответствующего порта. Страница разделена на вкладки: «Общие настройки», «Настройки RTU», «Настройки TCP».

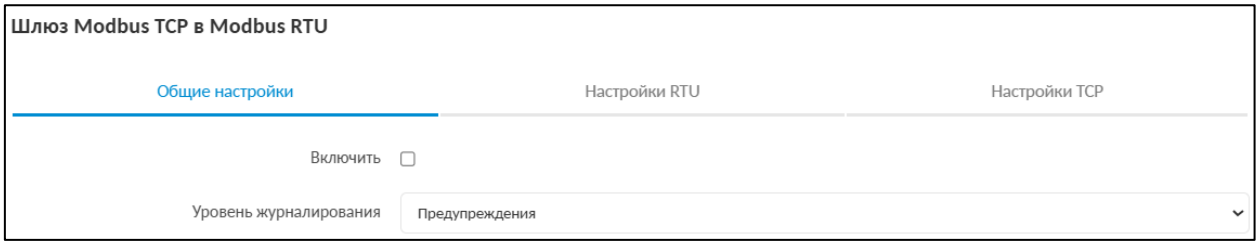


Рисунок 5-35: Редактирование шлюза. Вкладка «Общие настройки»

5.6.2.1 Вкладка «Общие настройки»

На вкладке «Общие настройки» (см. рисунок 5-35) задаются основные параметры шлюза.

- «Включить» — флаг, включающий или отключающий данный шлюз.
- «Уровень журналирования» — выбор уровня детализации записи событий.

5.6.2.2 Вкладка «Настройки RTU»

На вкладке «Настройки RTU» (см. рисунок 5-36) настраиваются параметры последовательного интерфейса для связи с устройствами Modbus RTU.

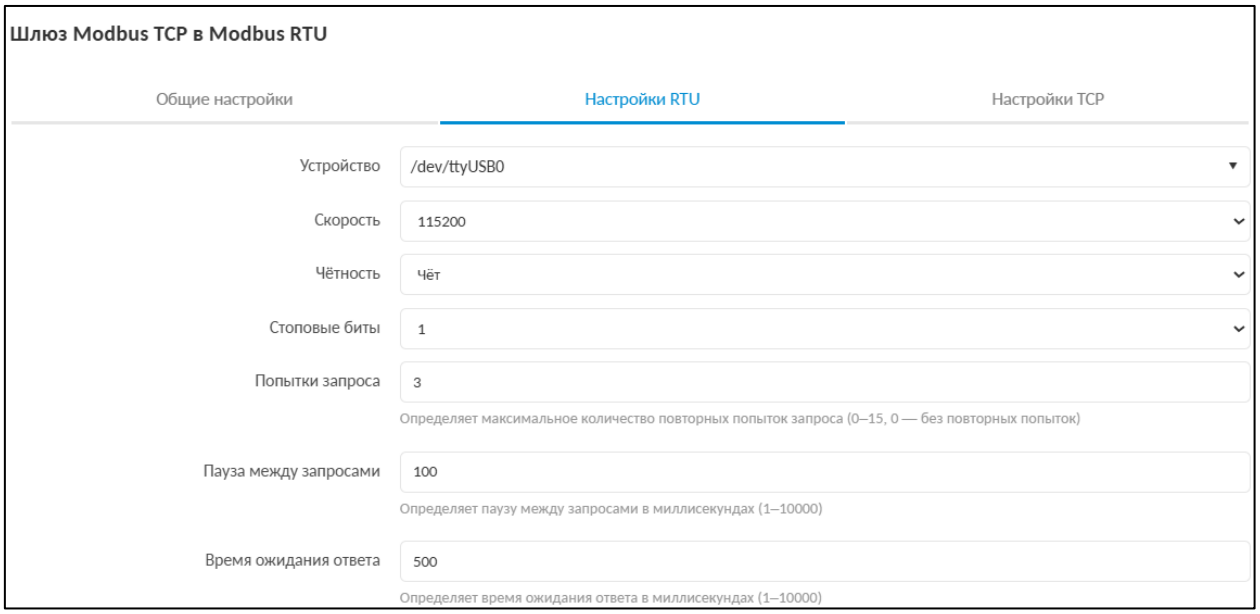


Рисунок 5-36: Редактирование шлюза. Вкладка «Настройки RTU»

- «Устройство» — выпадающий список для выбора последовательного устройства (например, /dev/ttyUSB0, /dev/ttyS0). Значение «— Сделайте выбор —» означает, что устройство не выбрано.
- «Скорость» — скорость передачи данных в бодах.
- «Чётность» — контроль чётности.
- «Стоповые биты» — количество стоповых битов.
- «Попытки запроса» — максимальное количество повторных попыток запроса (диапазон 0–15);
- «Пауза между запросами» — пауза между запросами в миллисекундах (диапазон 1–10000);
- «Время ожидания ответа» — время ожидания ответа от Modbus RTU-устройства в миллисекундах (диапазон 1–10000).

5.6.2.3 Вкладка «Настройки TCP»

На вкладке «Настройки TCP» (см. рисунок 5-37) настраиваются параметры TCP-сервера шлюза.

Рисунок 5-37: Редактирование шлюза. Вкладка «Настройки TCP»

- «TCP адрес» — IP-адрес, на котором шлюз будет принимать TCP-соединения;
- «TCP порт» — TCP-порт для приёма Modbus TCP-соединений;
- «Максимальное количество TCP подключений» — максимальное количество одновременных TCP-соединений (диапазон 1–128);
- «Таймаут» — таймаут подключения в секундах (диапазон 0–1000).

5.6.3 Добавление шлюза

Страница добавления нового шлюза содержит те же вкладки и параметры, что и страница редактирования. Настройки выполняются аналогично разделу 5.6.2 «Редактирование шлюза». При добавлении нового шлюза необходимо заполнить параметры на всех трёх вкладках, после чего сохранить изменения.

5.7 uHTTPd

uHTTPd — это веб-сервер, предназначенный для встраиваемых систем.

Страница разделена на несколько вкладок: «Основные настройки», «Второстепенные настройки», «Дополнительные настройки», «Параметры самоподписанного сертификата».

5.7.1 Вкладка «Основные настройки»

На вкладке «Основные настройки» (см. рисунок 5-38) задаются основные параметры веб-сервера: порты прослушивания, настройки HTTPS и SSL-сертификатов.

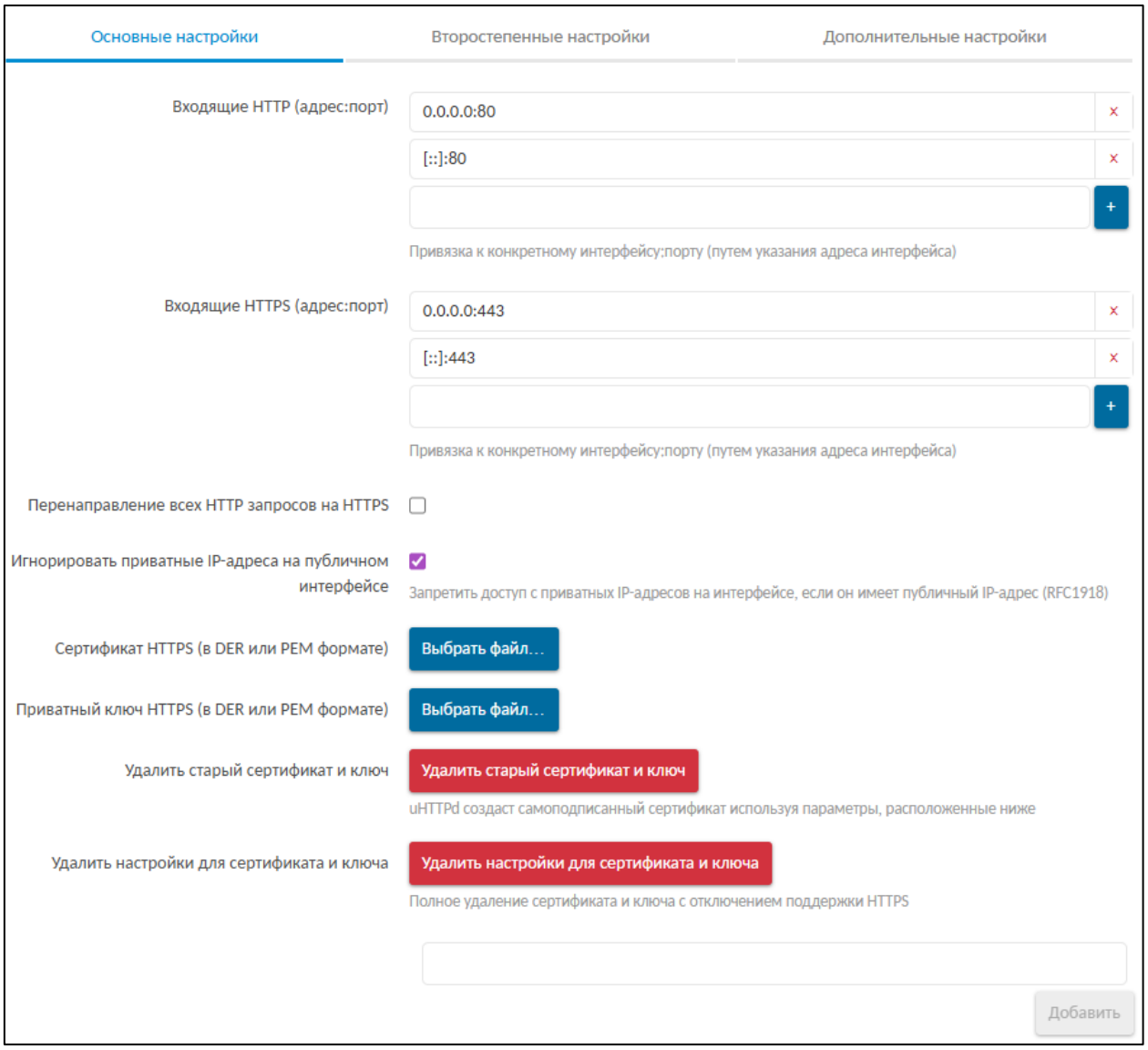


Рисунок 5-38: uHTTPd. Вкладка «Основные настройки»

- «Входящие HTTP (адрес: порт)» — адреса и порты для входящих HTTP-соединений.
- «Входящие HTTPS (адрес: порт)» — адреса и порты для входящих HTTPS-соединений.
- «Перенаправление всех HTTP запросов на HTTPS» — при включении данной опции все HTTP-запросы будут автоматически перенаправляться на HTTPS.

– «Игнорировать приватные IP-адреса на публичном интерфейсе» — при включении сервер игнорирует запросы с приватных IP-адресов.
– «Сертификат HTTPS (в DER или PEM формате)» — выбор файла SSL-сертификата для HTTPS.
– «Приватный ключ HTTPS (в DER или PEM формате)» — выбор файла приватного ключа для HTTPS.
– «Удалить старый сертификат и ключ» — кнопка, при нажатии которой старый сертификат и ключ удаляются.
– «Удалить настройки для сертификата и ключа» — кнопка для полного удаления сертификата и ключа с отключением поддержки HTTPS.

5.7.2 Вкладка «Второстепенные настройки»

На вкладке «Второстепенные настройки» (см. рисунок 5-39) настраиваются параметры обслуживания веб-сервера, не связанные напрямую с безопасностью и интерфейсами.

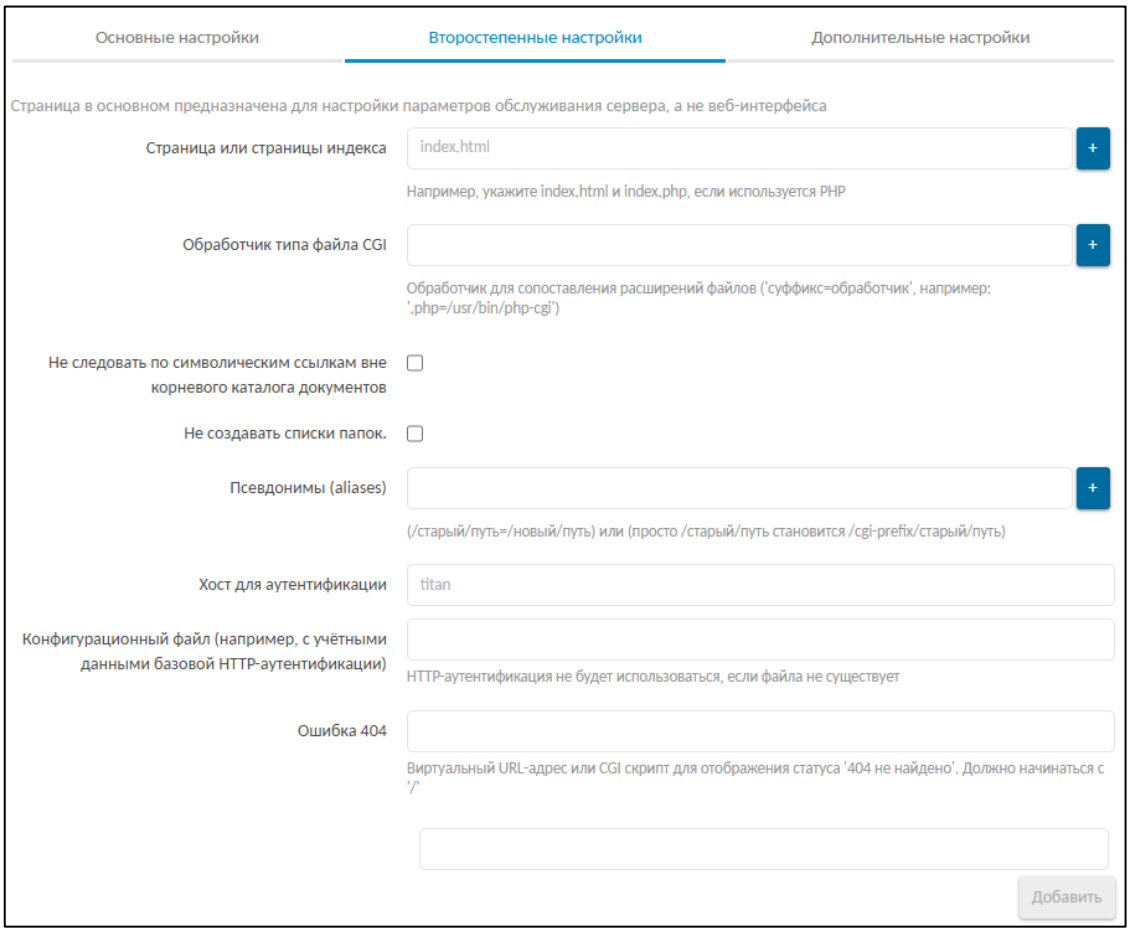


Рисунок 5-39: uHTTPd. Вкладка «Второстепенные настройки»

- «Страница или страницы индекса» — перечень индексных файлов, разделённых запятыми.
- «Обработчик типа файла CGI» — сопоставление расширений файлов с обработчиками.
- «Не следовать по символическим ссылкам вне корневого каталога документов» — запрещает переход по символьным ссылкам, ведущим за пределы корневой папки.
- «Не создавать списки папок» — запрещает автоматическое создание списков содержимого директорий.
- «Псевдонимы (aliases)» — позволяет задать псевдонимы путей в формате /старый/путь=/новый/путь.
- «Хост для аутентификации» — имя хоста для HTTP-аутентификации.
- «Конфигурационный файл (например, с учётными данными базовой HTTP-аутентификации)» — путь к файлу с учётными записями.
- «Ошибка 404» — виртуальный URL-адрес или CGI-скрипт для отображения статуса «404 Not Found».

5.7.3 Вкладка «Дополнительные настройки»

Вкладка «Дополнительные настройки» (см. рисунки 5-40а и 5-40б) содержит параметры, которые редко используются или влияют на обслуживание веб-интерфейса.

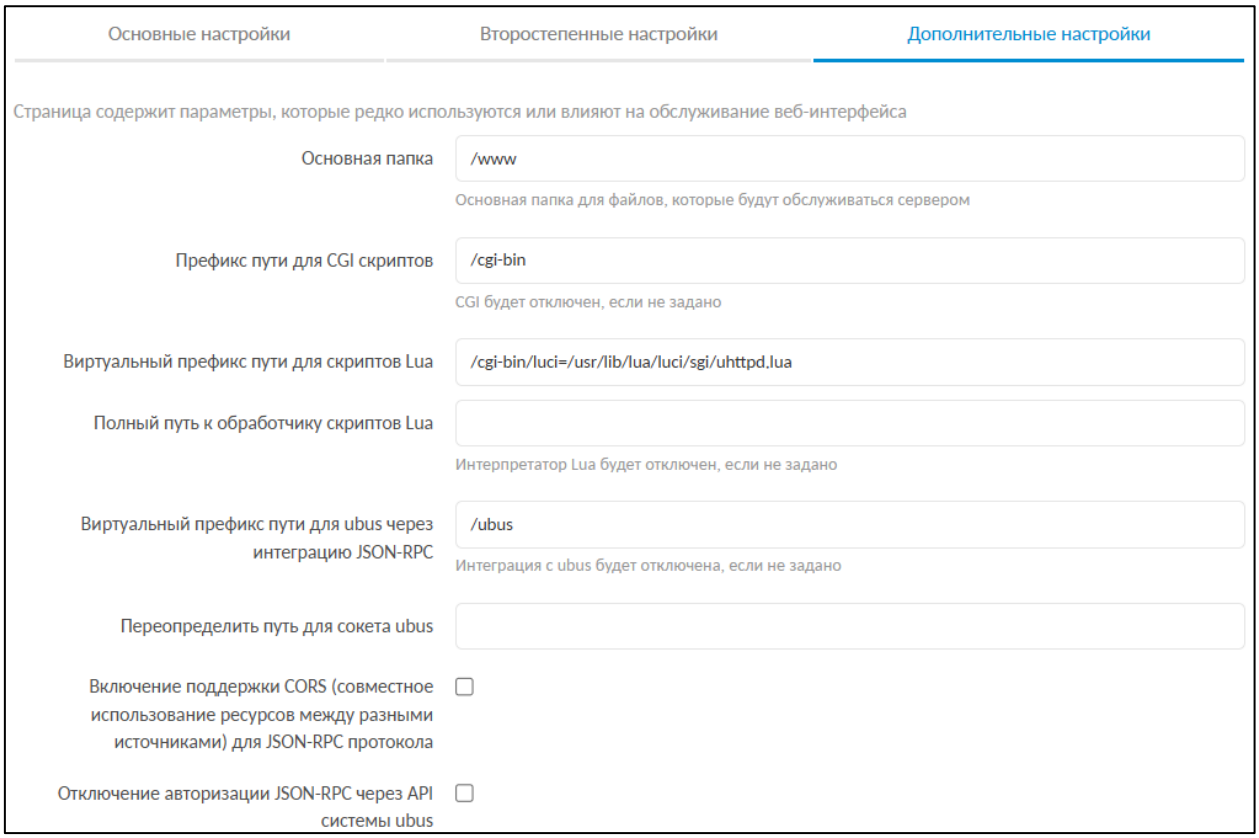


Рисунок 5-40a: uHTTPd. Вкладка «Дополнительные настройки». Основные параметры

- «Основная папка» — корневая директория для файлов, которые будут обслуживаться сервером.
- «Префикс пути для CGI скриптов» — путь для CGI-скриптов. CGI будет отключён, если не задано.
- «Виртуальный префикс пути для скриптов Lua» — настройка для обработки Lua-скриптов. Интерпретатор Lua будет отключён, если не задан.
- «Полный путь к обработчику скриптов Lua» — полный путь к обработчику скриптов Lua (аналогично предыдущему параметру).
- «Виртуальный префикс пути для ubus через интеграцию JSON-RPC» — префикс для доступа к ubus через JSON-RPC.
- «Переопределить путь для сокета ubus» — позволяет указать альтернативный путь к сокету ubus.
- «Включение поддержки CORS» — включает совместное использование ресурсов между разными источниками (Cross-Origin Resource Sharing) для JSON-RPC протокола.

– «Отключение авторизации JSON-RPC через API системы ubus» — отключает проверку авторизации для JSON-RPC-запросов к ubus.

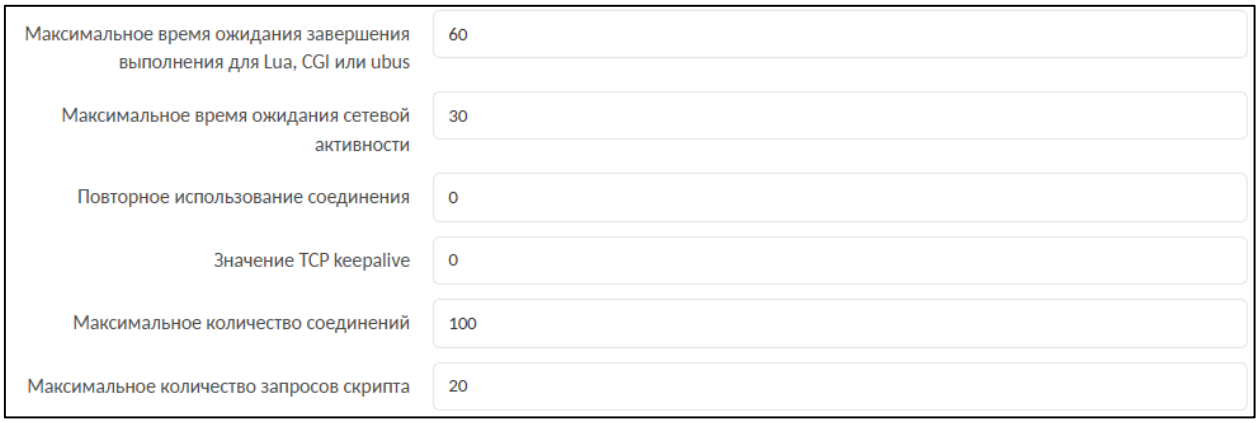


Рисунок 5-40б: uHTTPd. Вкладка «Дополнительные настройки». Таймауты и ограничения

– «Максимальное время ожидания завершения выполнения для Lua, CGI или ubus» — таймаут выполнения скриптов в секундах.
– «Максимальное время ожидания сетевой активности» — таймаут сетевой активности в секундах.
– «Повторное использование соединения» — настройка keepalive для соединений.
– «Значение TCP keepalive» — параметр TCP keepalive.
– «Максимальное количество соединений» — максимальное количество одновременных соединений.
– «Максимальное количество запросов скрипта» — максимальное количество обрабатываемых запросов скрипта.

5.7.4 «Параметры самоподписанного сертификата»

На вкладке «Параметры самоподписанного сертификата» (см. рисунок 5-41) задаются параметры для генерации самоподписанного SSL-сертификата, который используется при включении HTTPS и отсутствии загруженного сертификата.

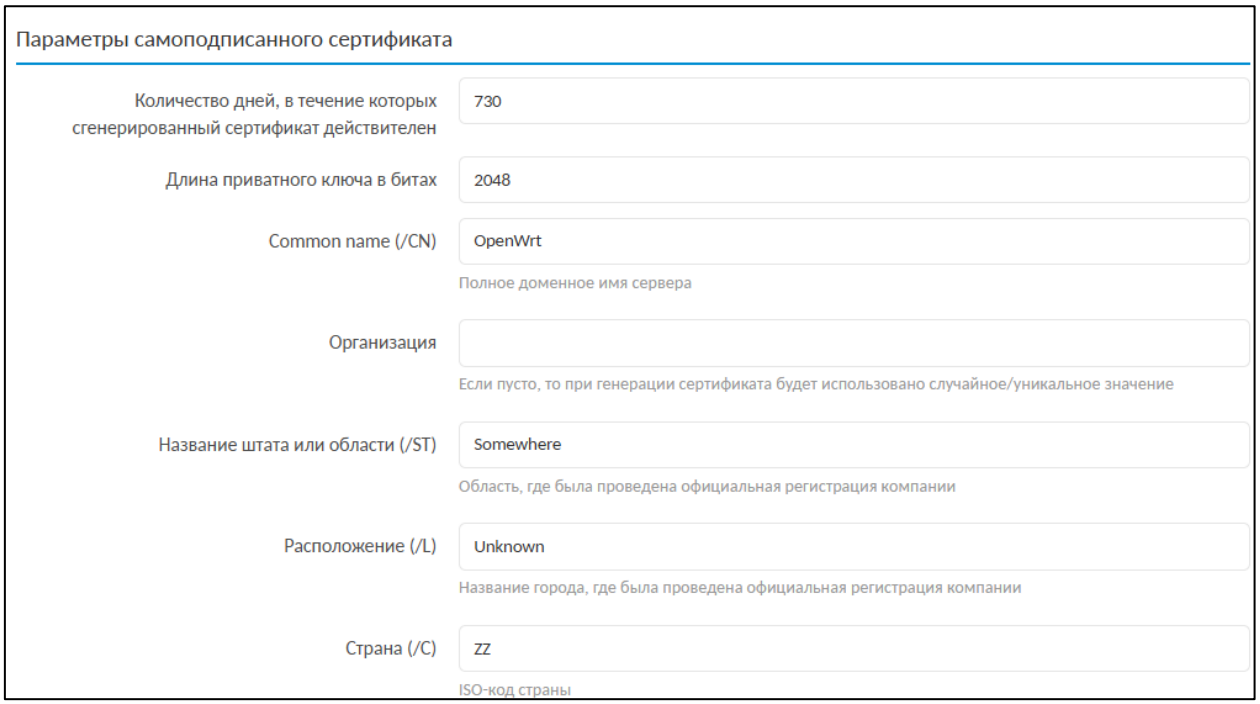


Рисунок 5-41: uHTTPd. Вкладка «Параметры самоподписанного сертификата»

– «Количество дней, в течение которых сгенерированный сертификат действителен» — срок действия сертификата в днях.
– «Длина приватного ключа в битах» — длина ключа RSA.
– «Common name (/CN)» — полное доменное имя сервера.
– «Организация» — название организации.
– «Название штата или области (/ST)» — штат или область.
– «Расположение (/L)» — название города.
– «Страна (/C)» — двухбуквенный ISO-код страны.

6 Сеть

6.1 Интерфейсы

Для управления сетевыми интерфейсами системы предназначена страница «Интерфейсы» раздела «Сеть». Внешний вид страницы «Интерфейсы» показан на рисунке 6-1.

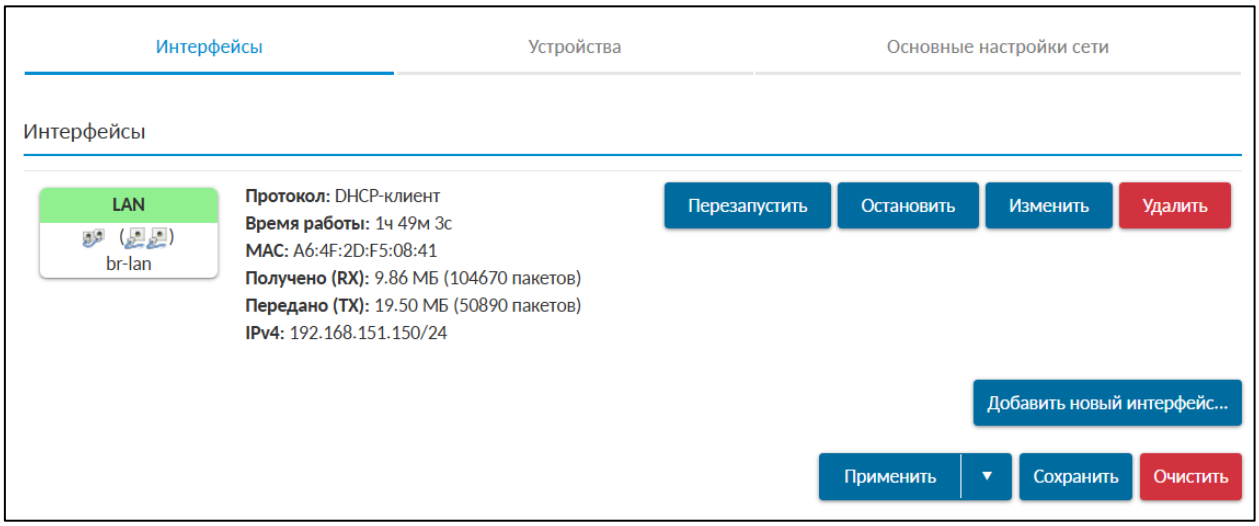


Рисунок 6-1: Страница «Интерфейсы»

На странице расположен список «Интерфейсы», в которой перечислены имеющиеся сетевые интерфейсы в системе. Для каждого интерфейса приведён значок, который содержит следующую информацию:

- название интерфейса;
- тип интерфейса (ethernet, мост, тонинг или беспроводной) и состояние подключения,
- если интерфейс является мостом, то количество портов моста определяется количеством иконок интерфейсов, указанных в скобках;
- название системного сетевого интерфейса, соответствующего данному интерфейсу.

Слева от значка для каждого интерфейса выводится краткая информация и статистика в режиме реального времени:

- «Протокол» — протокол интерфейса.
- «Время работы» — время работы данного интерфейса.

- «MAC» — MAC-адрес интерфейса (если это применимо для протокола интерфейса).
- «Получено (RX)» — количество принятых байт (пакетов) с момента запуска.
- «Передано (TX)» — количество передаваемых байт (пакетов) с момента запуска.
- «IPv4» — текущий IPv4 адрес, назначенный интерфейсу (если назначен).
- «IPv6» — текущий IPv6 адрес, назначенный интерфейсу (если назначен).
- «IPv4-PD» — текущий IPv4 префикс (если назначен).
- «Ошибка» — ошибка интерфейса (если обнаружена).

В последнем столбце таблицы расположены кнопки управления интерфейсом:

- «Перезапустить» — выполняет переподключение соответствующего интерфейса (отключение с последующим подключением).
- «Остановить» — выполняет принудительное отключение соответствующего интерфейса.
- «Изменить» — открывает страницу редактирования параметров интерфейса.
- «Удалить» — удаляет соответствующую интерфейс.

Дополнительно на странице «Интерфейсы» в разделе «Основные настройки сети» доступна настройка ULA префикса IPv6 (см. рисунок 7-1).

6.1.1 Редактирование интерфейсов

Внешний вид страницы редактирования сетевого интерфейса показан на рисунке 6-2.

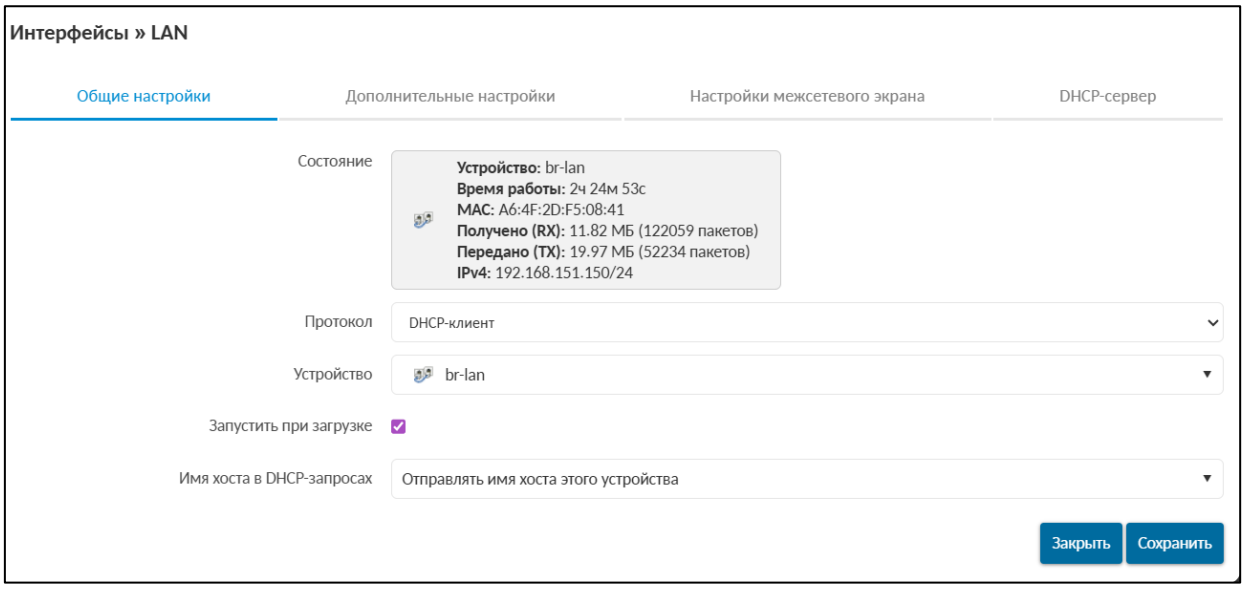


Рисунок 6-2: Страница редактирования сетевого интерфейса

Страница редактирования сетевого интерфейса разделена на вкладки:

– «Общие настройки»;
– «Дополнительные настройки»;
– «Настройки канала»;
– «Настройки межсетевого экрана».

6.1.1.1 Общие настройки

На вкладке «Общие настройки» (см. рисунок 7-4) представлены настройки интерфейса.

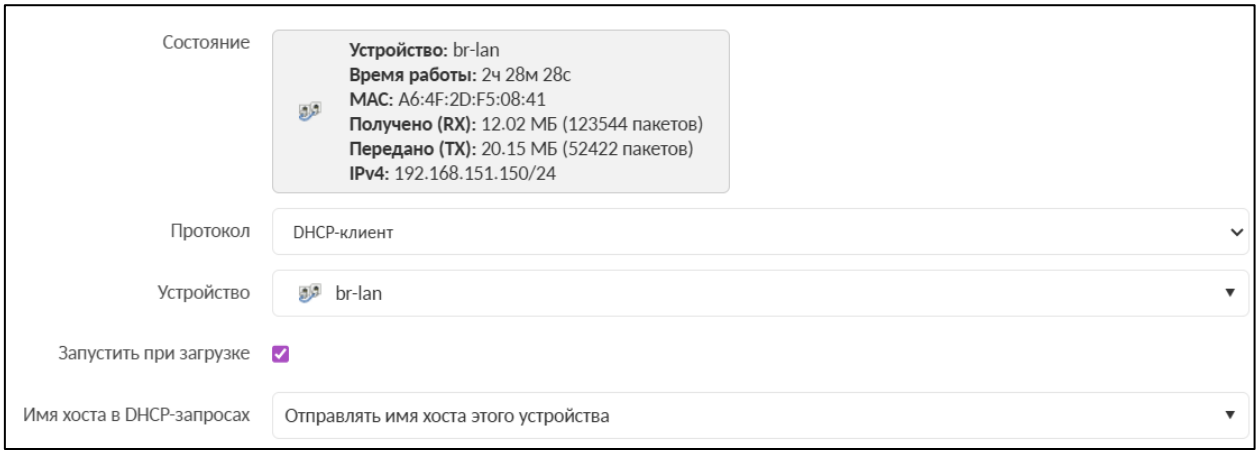


Рисунок 6-3: Общие настройки сетевого интерфейса

Выбор протокола производится при помощи выпадающего списка «Протокол» на вкладке «Общие настройки» (см. рисунок 6-3). Выпадающий список выбора протокола показан на рисунке 6-4.

Рисунок 6-4: Выпадающий список выбора протокола интерфейса

После выбора нового протокола, на странице основных настроек будет отображена кнопка «Изменить протокол», как показано на рисунке 6-5.

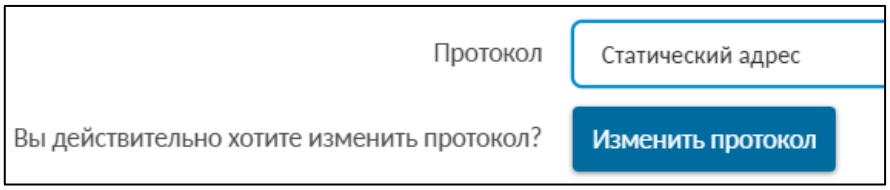


Рисунок 6-5: Кнопка смены протокола сетевого интерфейса

При нажатии кнопки «Изменить протокол» протокол сетевого интерфейса будет изменён на выбранный. При этом набор основных и дополнительных настроек будет заменён в соответствии с выбранным протоколом.

Среди общих для всех протоколов, можно выделить следующие настройки:

– «Запустить при загрузке» — включает или отключает автоматический запуск интерфейса при загрузке системы;
– «Имя хоста этого устройства» — включает или отключает отправку имени данного устройства в DHCP-запросах.

На рисунке 6-6, для примера, приведён внешний вид вкладки настроек для протокола «DHCP-клиент».

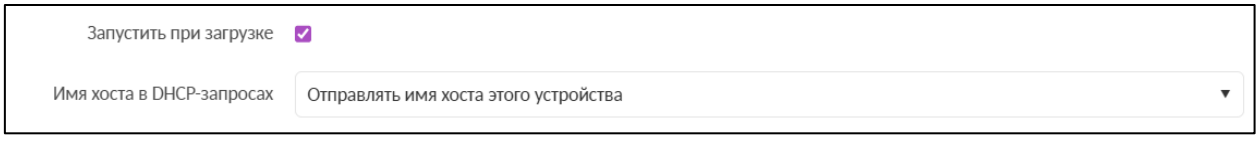


Рисунок 6-6 — Вид общих настроек

6.1.1.2 Дополнительные настройки

На вкладке «Дополнительные настройки» (представленной на рисунке 6-7) доступны следующие параметры:

Поведение интерфейса:

– «Принудительное подключение (Force link)» — устанавливает параметры интерфейса независимо от реального состояния физического подключения. Если опция включена, события подключения/отключения кабеля для данного интерфейса не будут вызывать hotplug-обработчики.

Рисунок 6-7: Настройки интерфейса

Настройки DHCP-клиента:

– «Использовать широковещательный флаг» — включает использование широковещательного флага (broadcast flag) в DHCP-запросах.

– «ID клиента при DHCP-запросе» — позволяет указать идентификатор клиента, который будет использоваться в DHCP-запросах.

– «Класс производителя (Vendor class), который отправлять при DHCP-запросе» — позволяет указать класс производителя (vendor class), передаваемый в DHCP-запросах.

– «Использовать шлюз по умолчанию» — определяет, будет ли данный интерфейс использоваться в качестве маршрута по умолчанию.

– «Использовать объявляемые узлом DNS сервера» — определяет, будут ли использоваться DNS-серверы, полученные от DHCP-сервера.

– «Использовать метрику шлюза» — позволяет указать метрику шлюза для данного интерфейса. DNS-серверы в локальном файле resolv.conf сортируются по весу, указанному здесь.

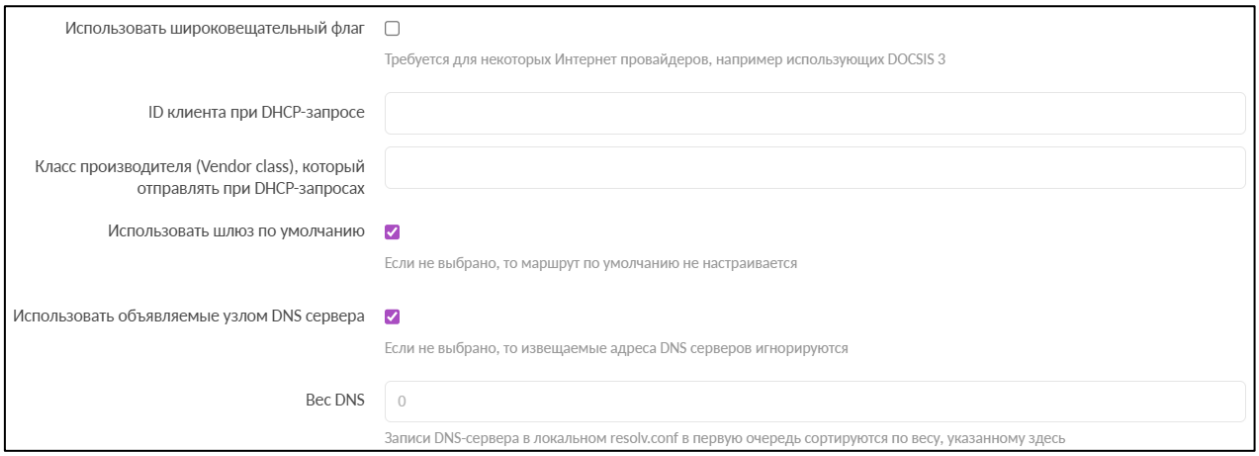


Рисунок 6-8: Настройки DHCP-клиента

Таблицы маршрутизации

- «Переопределить таблицу маршрутизации IPv4» — позволяет указать альтернативную таблицу маршрутизации для IPv4.
- «Переопределить таблицу маршрутизации IPv6» — позволяет указать альтернативную таблицу маршрутизации для IPv6.

Рисунок 6-9: Настройки маршрутизации

Настройки IPv6

- «Делегировать IPv6 префиксы» — включает нисходящее делегирование префиксов IPv6, доступных на этом интерфейсе.
- «IPv6 назначение длины» — задаёт длину префикса IPv6, выделяемую интерфейсу.
- «Фильтр IPv6 префикса» — позволяет ограничить диапазон префиксов IPv6 для выделения нисходящих подсетей.
- «IPv6 суффикс» — определяет суффикс для формирования IPv6-адреса интерфейса.
- «IPv6 привилегии» — определяет приоритет интерфейса при делегировании префиксов нескольким нисходящим потокам.

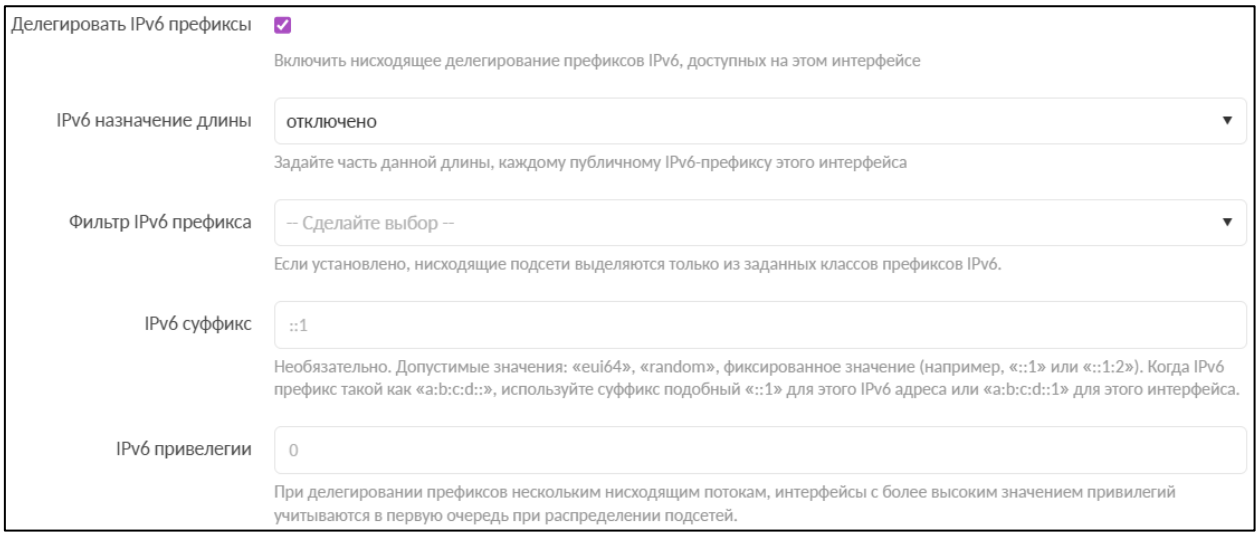


Рисунок 6-10: Настройки IPv6

6.1.1.3 Настройки межсетевого экрана

Во вкладке «Настройки межсетевого экрана» производится выбор или создание новой зоны, прикреплённой к редактируемому сетевому интерфейсу. Внешний вид вкладки «Настройки межсетевого экрана» показан на рисунке 6-11.

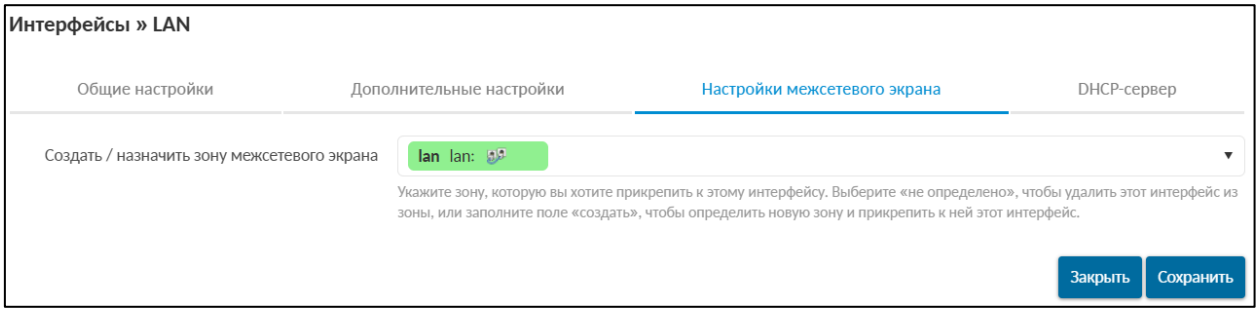


Рисунок 6-11: Настройки межсетевого экрана сетевого интерфейса

На вкладке размещён только один элемент управления — выпадающий список «Создать / назначить зону сетевого экрана» (см. рисунок 6-12).

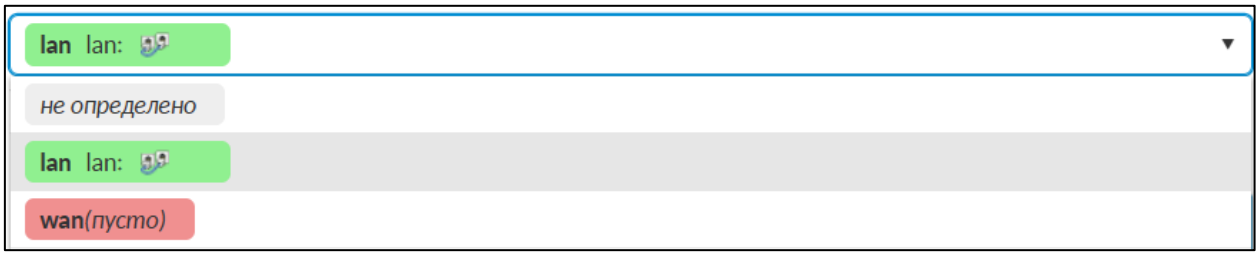


Рисунок 6-12: Выпадающий список выбора зоны межсетевого экрана

При помощи данного выпадающего списка можно выбрать существующую зону межсетевого экрана или создать новую, введя её имя в

поле «создать». При выборе «не определённо», редактируемый сетевой интерфейс будет удалён из зоны, к которой он был прикреплён ранее.

6.1.1.4 Настройки DHCP-сервера

При выборе протокола «Статический адрес» для сетевого интерфейса появляется возможность запуска DHCP-сервера на данном интерфейсе. Настройки DHCP-сервера представлены в подразделе «DHCP-сервер» страницы редактирования сетевого интерфейса.

Вкладка «DHCP-сервер» разделена на несколько подразделов: «Общие настройки», «Дополнительные настройки» и «Настройки IPv6».

6.1.1.4.1 Общие настройки

В подразделе «Общие настройки» (см. рисунок 6-13) представлены следующие параметры:

- «Игнорировать интерфейс» — отключает DHCP-сервер для данного интерфейса.
- «Запустить» — начальный адрес пула адресов, выдаваемых DHCP-сервером в аренду.
- «Предел» — максимальное количество адресов, которое может быть выдано DHCP-сервером в аренду.
- «Срок аренды адреса» — время истечения срока аренды выдаваемых адресов. Минимальное значение — 2 минуты (2m). Может быть указано в формате: 12h (12 часов), 3d (3 дня) и т.п.

Рисунок 6-13: Общие настройки DHCP-сервера

6.1.1.4.2 Дополнительные настройки

В подразделе «Дополнительные настройки» (см. рисунок 6-14) представлены следующие параметры:

- «Динамический DHCP» — включает или отключает режим динамического выделения адресов клиентам.
- «Принудительно (Force)» — запускать DHCP-сервер в данной сети, даже если в ней уже обнаружен другой работающий DHCP-сервер.
- «IPv4-маска сети» — позволяет переопределить маску подсети, отправляемую клиентам.
- «DHCP настройки» — позволяет определить дополнительные опции DHCP, передаваемые клиентам. Например, опция 6,192.168.2.1,192.168.2.2 извещает DHCP-клиентов об адресах DNS-серверов 192.168.2.1 и 192.168.2.2.

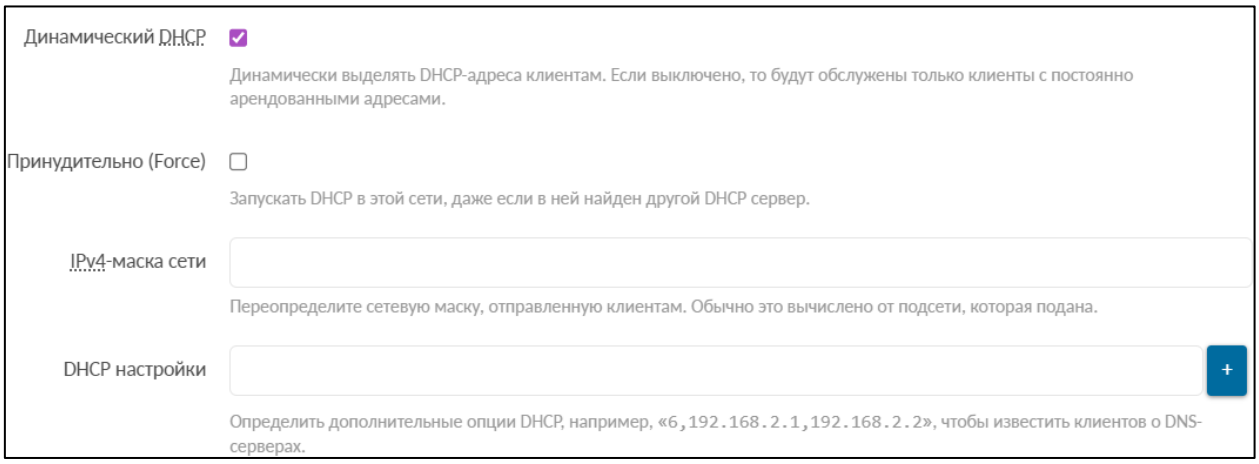


Рисунок 6-14: Дополнительные настройки DHCP-сервера

6.1.1.4.3 Настройки IPv6

В подразделе «Настройки IPv6» (см. рисунок 6-15) представлены параметры DHCP-сервера для протокола IPv6:

- «Служба RA» — конфигурирует режим работы службы Router Advertisement (RA) для автоматической конфигурации и маршрутизации на данном интерфейсе. Доступные варианты:
  - «Отключено» — служба RA выключена;
  - «Режим сервера» — служба RA работает в режиме сервера;

- «Режим передачи» — служба RA работает в режиме ретрансляции;
- «Гибридный режим» — гибридный режим работы.

– «DHCPv6 сервис» — конфигурирует режим работы службы DHCPv6 на этом интерфейсе. Доступные варианты:

- «Отключено»;
- «Режим сервера»;
- «Режим передачи»;
- «гибридный режим»

– «NDP-Proxy» — конфигурирует режим работы службы NDP-прокси на этом интерфейсе. Доступные варианты:

- «Отключено»;
- «режим передачи»;
- «гибридный режим».

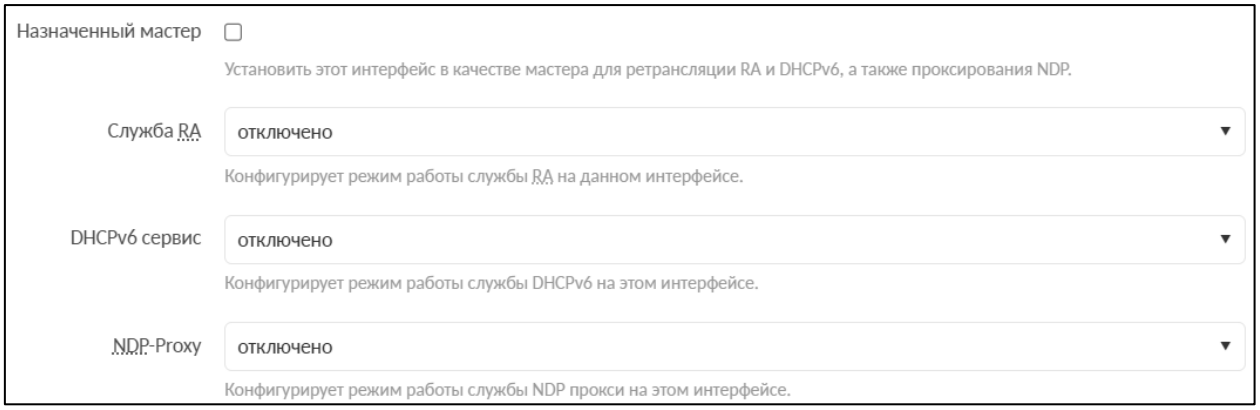


Рисунок 6-15: Настройки IPv6 DHCP-сервера

6.1.2 Создание нового интерфейса

Для создания нового интерфейса предназначена кнопка «Добавить новый интерфейс» (см. рисунок 6-1), расположенная внизу таблицы интерфейсов.

При нажатии кнопки «Добавить новый интерфейс» будет открыта страница создания нового сетевого интерфейса, как показано на рисунке 6-16, на которой следует указать символьное имя и протокол интерфейса.

Рисунок 6-16: Создание нового сетевого интерфейса

После ввода основных параметров интерфейса, для его создания следует нажать кнопку «Создать интерфейс». Если основные параметры создаваемого интерфейса были введены без ошибок, произойдет переход на страницу редактирования нового интерфейса, которая подробна описана в разделе 6.1.1 данного руководства.

6.1.3 Удаление интерфейсов

Для удаления интерфейса предназначена кнопка «Удалить» (см. рисунок 6-1), расположенная в строке соответствующего интерфейса.

При нажатии кнопки «Удалить» интерфейс будет помечен для удаления.

Рисунок 6-17: Помеченный для удаления интерфейс

В случае подтверждения удаления (нажатие кнопки «ОК»), сетевой интерфейс будет удалён.

6.1.4 Устройства

На вкладке «Устройства» раздела «Сеть» можно определить пользовательский список хостов и соответствующее им параметры. Внешний вид страницы «Устройства» показан на рисунке 6-18.

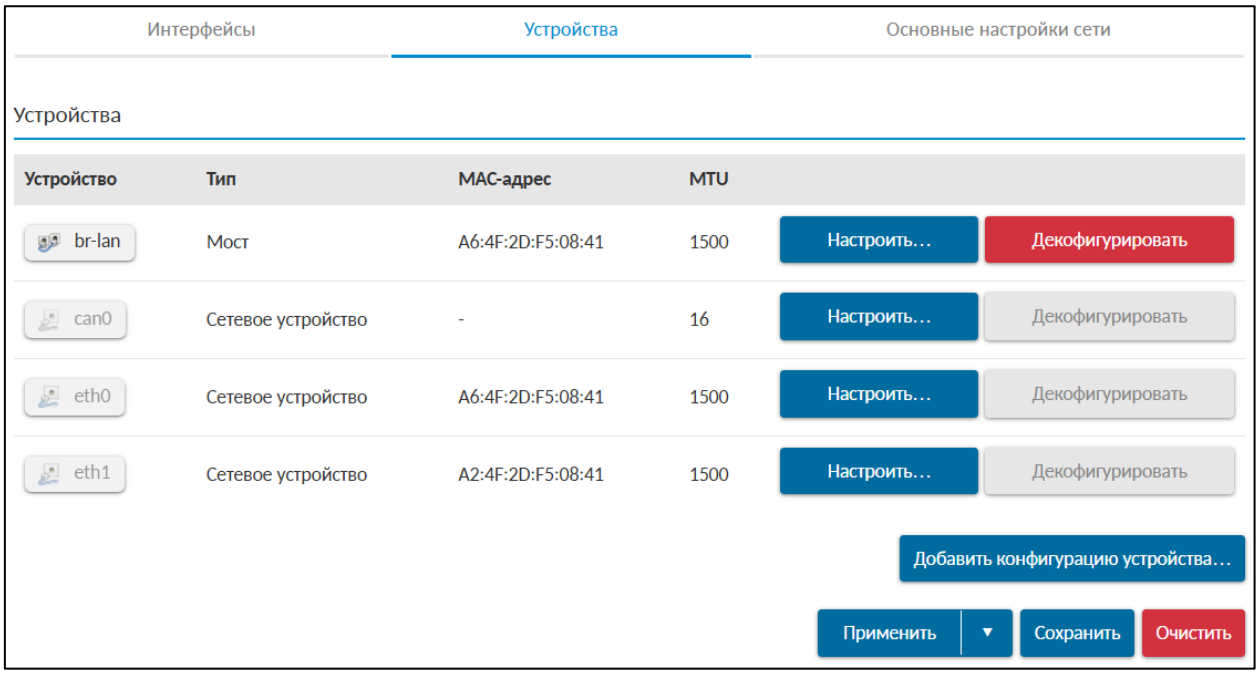


Рисунок 6-18: Страница «Имена хостов»

Добавление нового устройства осуществляется нажатием кнопки «Добавить конфигурацию устройства» с последующим указанием имени хоста и соответствующих параметров в таблице (см. рисунок 6-19).

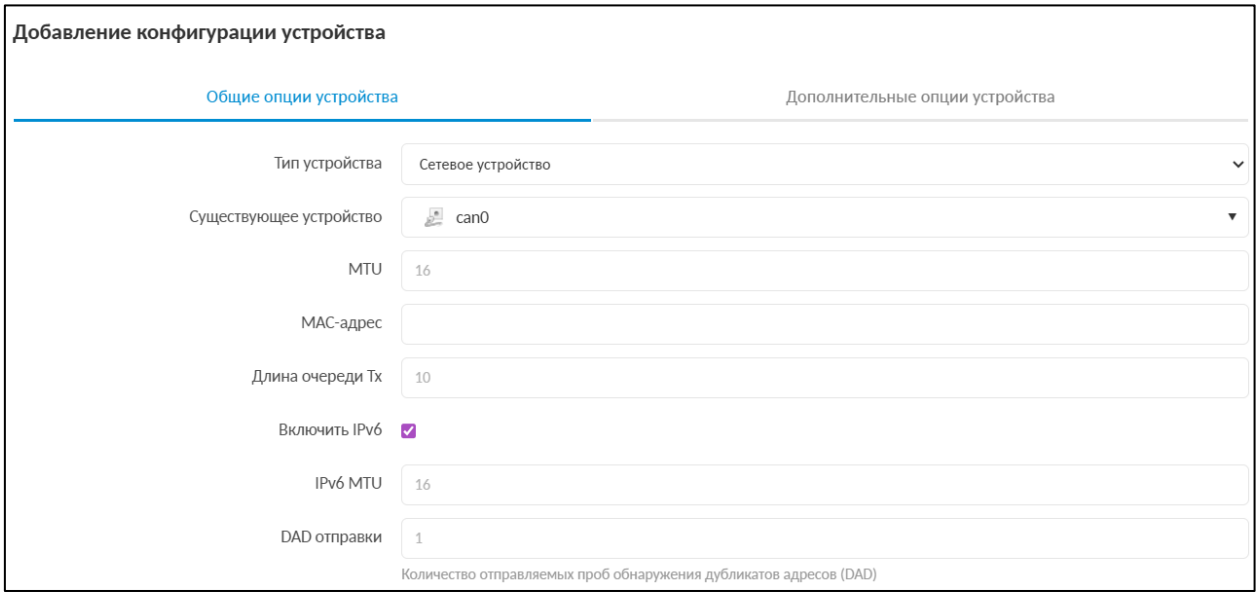


Рисунок 6-19: Страница «Устройства». Добавление новой записи. Общие опции

При необходимости можно настроить дополнительные опции добавляемого устройства.

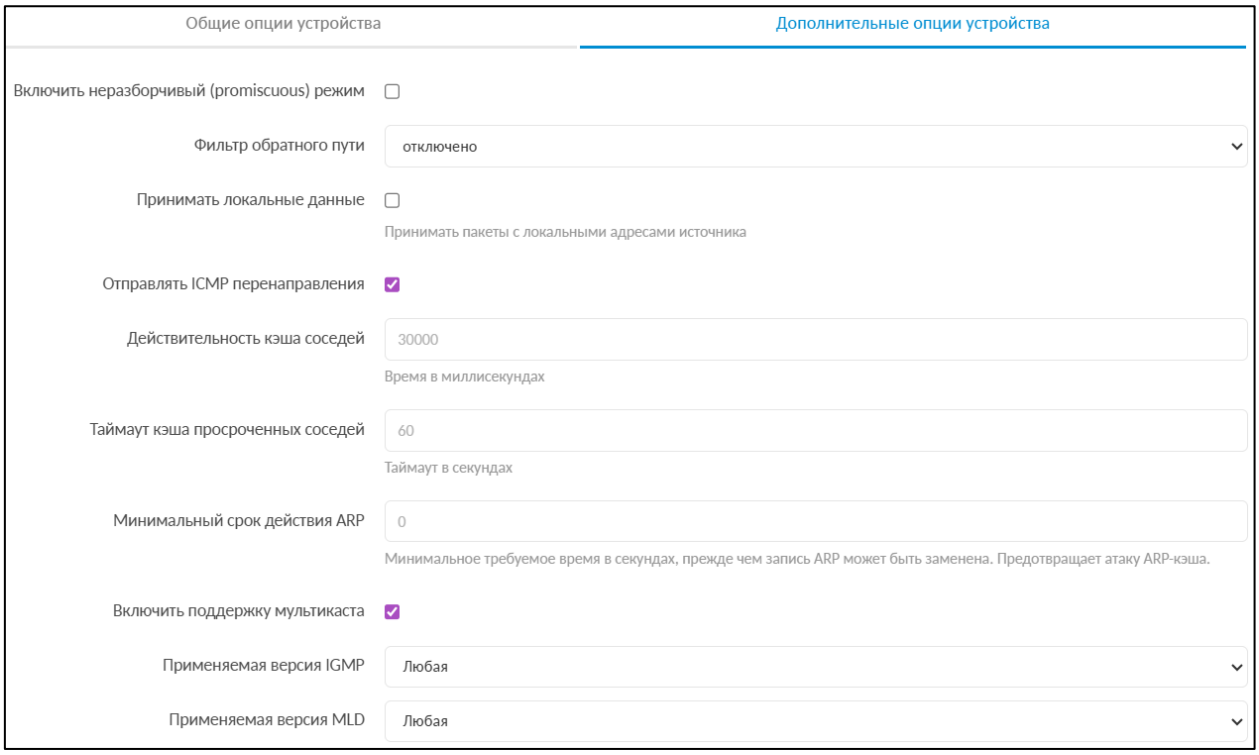


Рисунок 6-20: Страница «Устройства». Добавление новой записи. Дополнительные опции

Удалить существующую запись имени хоста можно при помощи кнопки «Деконфигурировать», расположенной в соответствующей строке.

6.1.5 Основные настройки сети

В разделе «Основные настройки сети» страницы «Интерфейсы» отображаются дополнительные глобальные параметры сетевой конфигурации устройства. Внешний вид раздела показан на рисунке 6-21.

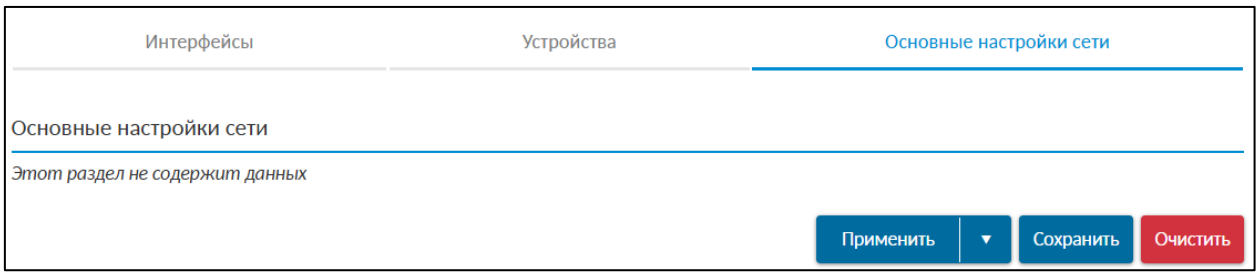


Рисунок 6-21: Основные настройки сети

При отсутствии доступных для редактирования параметров в данном разделе отображается сообщение: «Этот раздел не содержит данных».

Ниже расположены кнопки управления:

– «Применить» — применяет внесённые изменения без сохранения в постоянную конфигурацию (изменения действуют до перезагрузки устройства);
– «Сохранить» — сохраняет текущие настройки в постоянную конфигурацию;
– «Очистить» — сбрасывает все несохранённые изменения в полях ввода.

6.2 Маршрутизация

На странице «Маршрутизация» раздела «Сеть» производится настройка статических маршрутов и правил маршрутизации для протоколов IPv4 и IPv6. Данные настройки позволяют определить, через какой интерфейс и шлюз можно достичь определённого хоста или сети.

Страница разделена на несколько вкладок (или подразделов):

– «Статические маршруты IPv4»;
– «Статические маршруты IPv6»;
– «Правила IPv4»;
– «Правила IPv6».

6.2.1 Статические маршруты (IPv4 / IPv6)

В подразделе «Статические маршруты» отображается таблица уже созданных статических маршрутов. Таблица имеет следующие столбцы:

– «Интерфейс» — сетевой интерфейс, через который будет отправляться трафик для данного маршрута;
– «Назначение» — IP-адрес или сеть назначения (в формате CIDR для IPv6);
– «Шлюз» — IP-адрес шлюза, через который должен передаваться трафик к указанному назначению;
– «Метрика» — метрика маршрута (чем меньше значение, тем выше приоритет);

– «Таблица» — идентификатор таблицы маршрутизации, в которую добавляется маршрут;
– «Отключить» — позволяет временно отключить маршрут без его удаления.

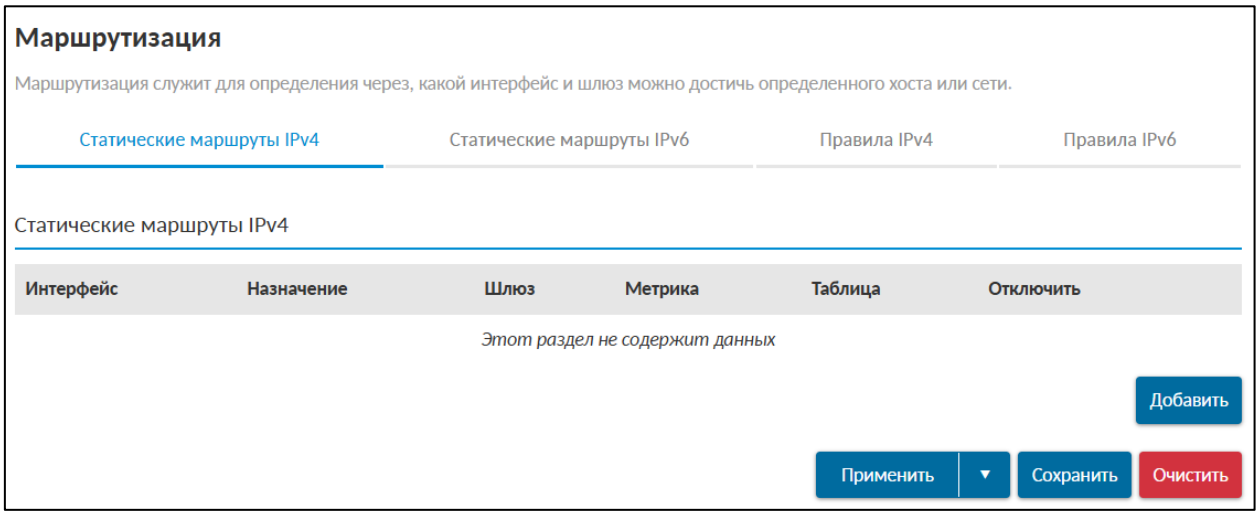


Рисунок 6-22: Страница «Статические маршруты»

При отсутствии настроенных маршрутов в таблице отображается сообщение: «Этот раздел не содержит данных».

Добавление нового статического маршрута осуществляется нажатием кнопки «Добавить» с последующим указанием параметров маршрута в добавленной строке таблицы (см. рисунок 6-23).

Рисунок 6-23: Страница «Статические маршруты». Добавление нового маршрута

Удалить существующий маршрут можно при помощи кнопки «Удалить», расположенной в строке соответствующего маршрута.

6.2.2 Правила маршрутизации (IPv4 / IPv6)

В подразделе «Правила» отображается таблица уже созданных правил маршрутизации. Правила позволяют управлять выбором таблицы маршрутизации в зависимости от параметров пакета. Таблица имеет следующие столбцы:

- «Приоритет» — числовое значение, определяющее порядок применения правил (чем меньше число, тем выше приоритет);
- «Входящий интерфейс» — сетевой интерфейс, с которого поступил пакет (опционально);
- «Отправитель» — IP-адрес или подсеть источника трафика;
- «Исходящий интерфейс» — сетевой интерфейс, через который должен отправляться пакет (опционально);
- «Получатель» — IP-адрес или подсеть назначения трафика;
- «Таблица» — идентификатор таблицы маршрутизации, которая будет использоваться для пакетов, соответствующих данному правилу;
- «Отключить» — позволяет временно отключить правило без его удаления.

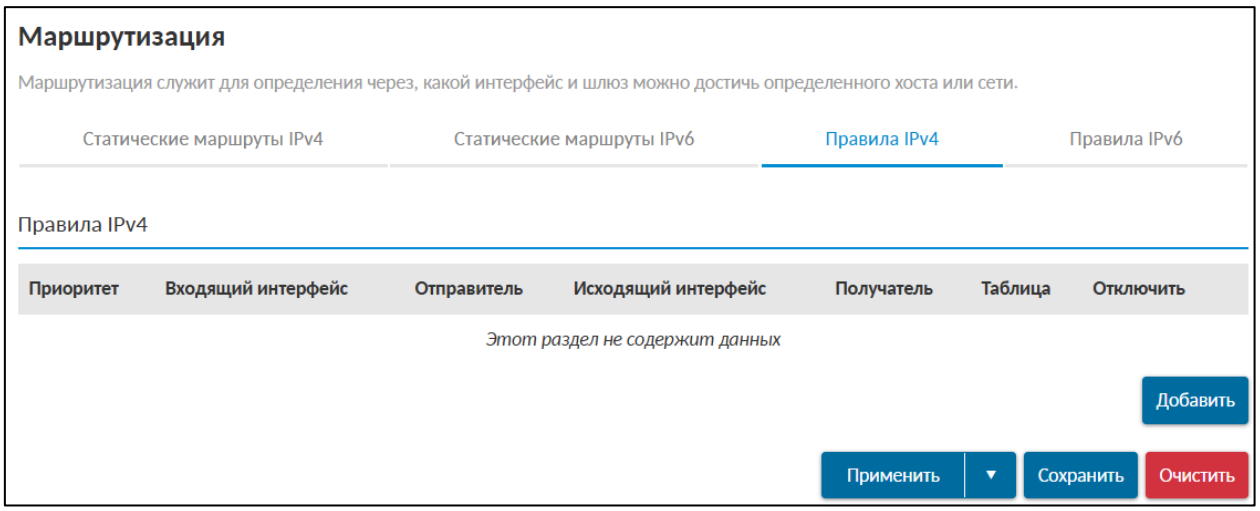


Рисунок 6-24: Страница «Правила»

При отсутствии настроенных правил в таблице отображается сообщение: «Этот раздел не содержит данных».

Для добавления нового правила маршрутизации предназначена кнопка «Добавить». При её нажатии открывается страница редактирования параметров правила.

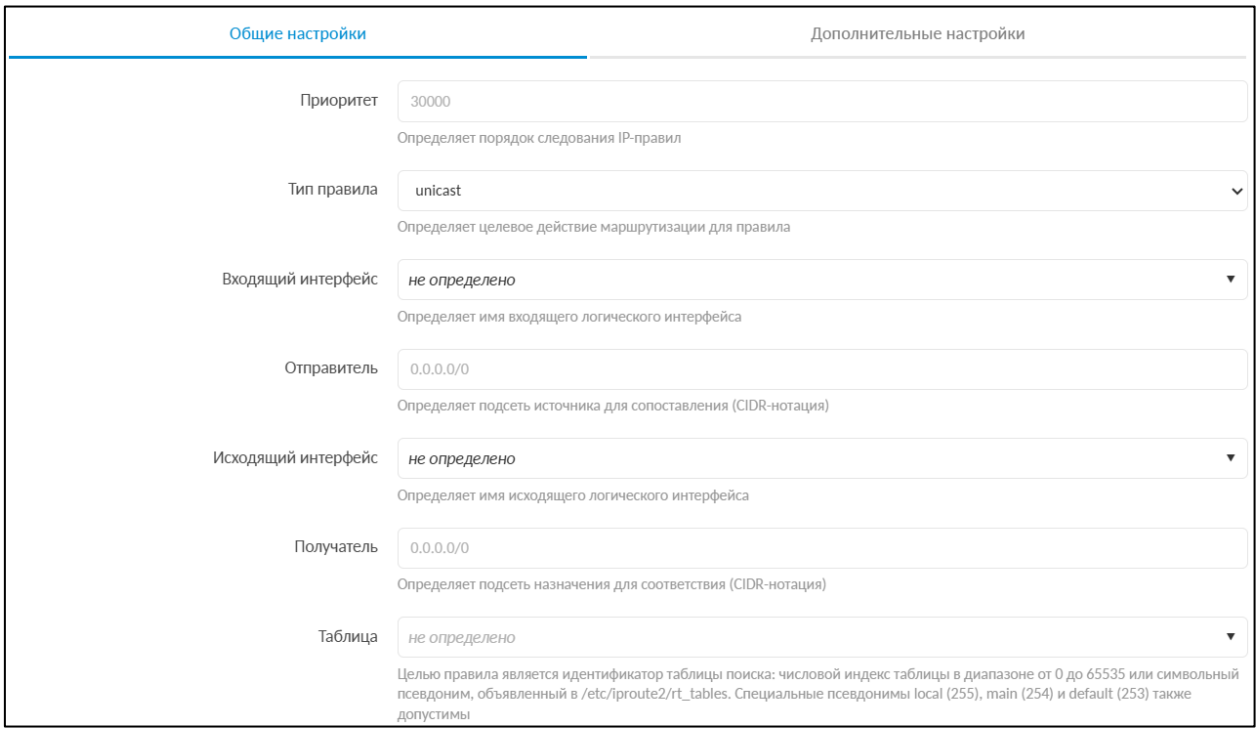


Рисунок 6-25: Добавление нового правила

6.3 DHCP и DNS

На странице «DHCP и DNS» раздела «Сеть» представлены настройки сетевой службы dnsmasq, которая представляет собой легковесный DNS и DHCP-сервер. Внешний вид страницы «DHCP и DNS» показан на рисунке 6-26.

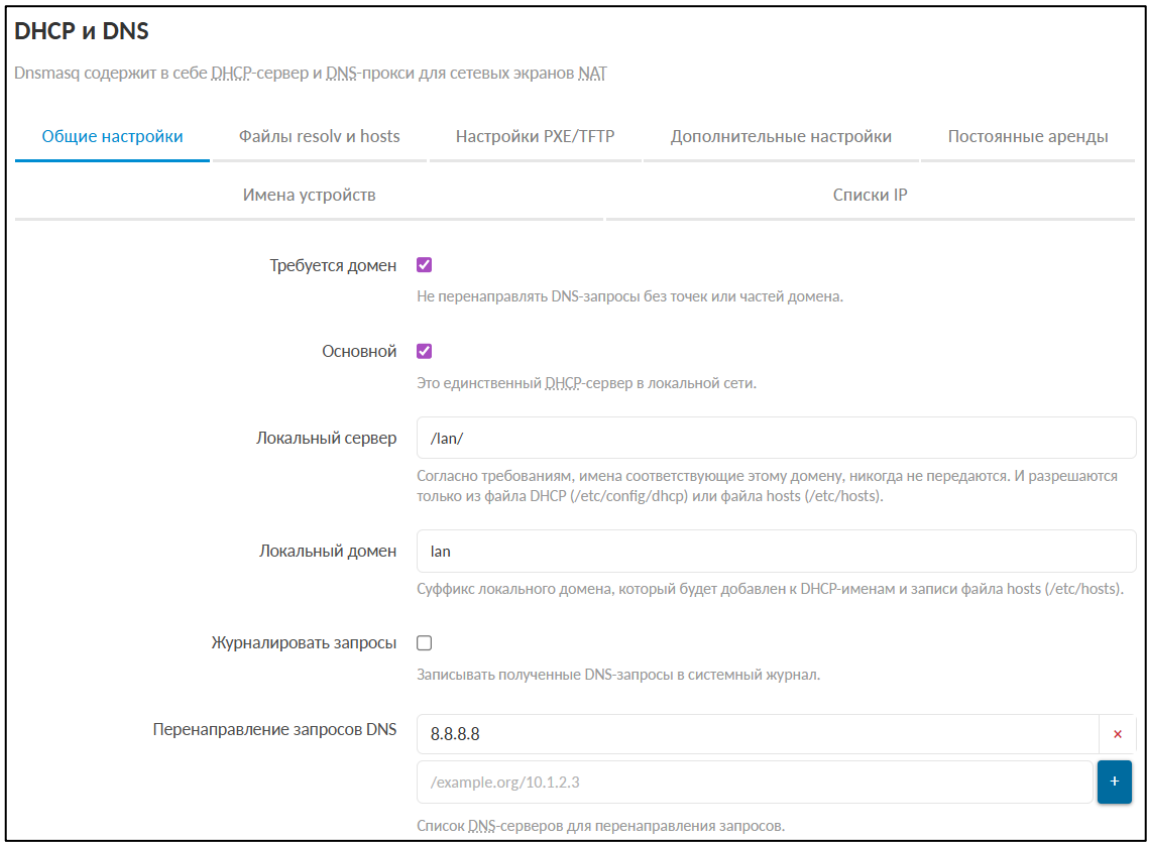


Рисунок 6-26: Страница «DHCP и DNS»

Настройки службы dnsmasq на странице «DHCP и DNS» разделены на несколько вкладок:

- «Общие настройки»;
- «Файлы resolv и hosts»;
- «Настройки PXE/TFTP»;
- «Дополнительные настройки»
- «Постоянные аренды»
- «Имена устройств»
- «Списки IP»

6.3.1 Общие настройки

Общие настройки службы dnsmasq расположены во вкладке «Общие настройки» страницы «DHCP и DNS».

На вкладке доступны следующие группы настроек:

Имена устройств:

– «Требуется домен» — не перенаправлять DNS-запросы без точек или частей домена.
– «Основной» — определяет, является ли данный DHCP-сервер единственным в локальной сети.
– «Локальный сервер» — задаёт домен, имена которого никогда не передаются на вышестоящие DNS-серверы. Такие имена разрешаются только из файла DHCP («/etc/config/dhcp») или файла hosts («/etc/hosts»). Значение по умолчанию — «/lan/».
– «Локальный домен» — суффикс локального домена, который будет добавлен к DHCP-именам и записям файла hosts («/etc/hosts»). Значение по умолчанию — «lan».

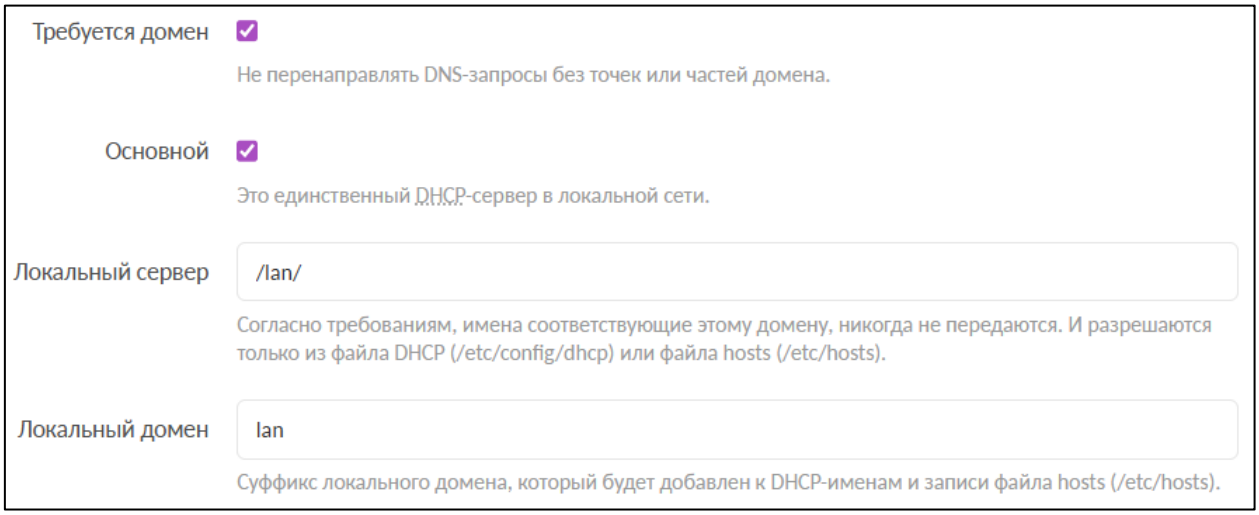


Рисунок 6-27: Страница «DHCP и DNS». Общие настройки. Имена устройств.

Журналирование

– «Журналировать запросы» — записывать полученные DNS-запросы в системный журнал. При включении опции все входящие DNS-запросы будут регистрироваться.

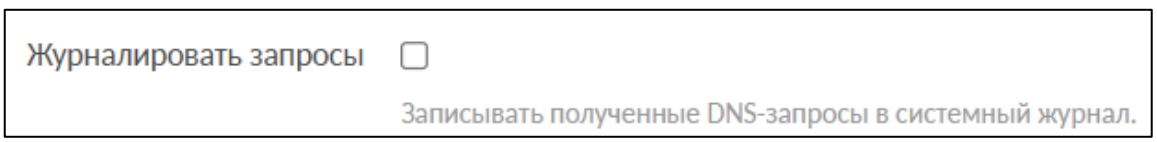


Рисунок 6-28: Страница «DHCP и DNS». Общие настройки. Журналирование.

Перенаправление запросов DNS

- «Перенаправление запросов DNS» — список DNS-серверов для перенаправления запросов. Позволяет указать, на какие DNS-серверы следует направлять запросы. Может содержать записи вида:
- «8.8.8.8» — IP-адрес DNS-сервера;
- «/example.org/10.1.2.3» — перенаправление запросов для указанного домена на определённый DNS-сервер.
- «Адреса» — список доменов для принудительного преобразования в IP-адрес. Позволяет задать статические соответствия между доменами и IP-адресами. Пример: «/router.local/192.168.0.1».
- «Наборы IP адресов» — список наборов IP-адресов для заполнения указанными IP-адресами доменов. Пример: «/example.org/ipset.ipset6».
- «Защита от DNS Rebinding» — отбрасывать ответы вышестоящего сервера, содержащие адреса RFC1918 (приватные адреса). При включении опции блокируются ответы DNS, которые могут быть использованы для атаки DNS Rebinding.
- «Разрешить localhost» — разрешить ответы внешней сети в диапазоне 127.0.0.0/8 и ::1. Может потребоваться, например, для RBL-сервисов.
- «Белый список доменов» — список доменов, для которых разрешены ответы RFC1918 (приватные адреса). При включённой защите от DNS Rebinding для указанных доменов ответы с приватными адресами не будут отбрасываться. Пример: «ihost.netflix.com».

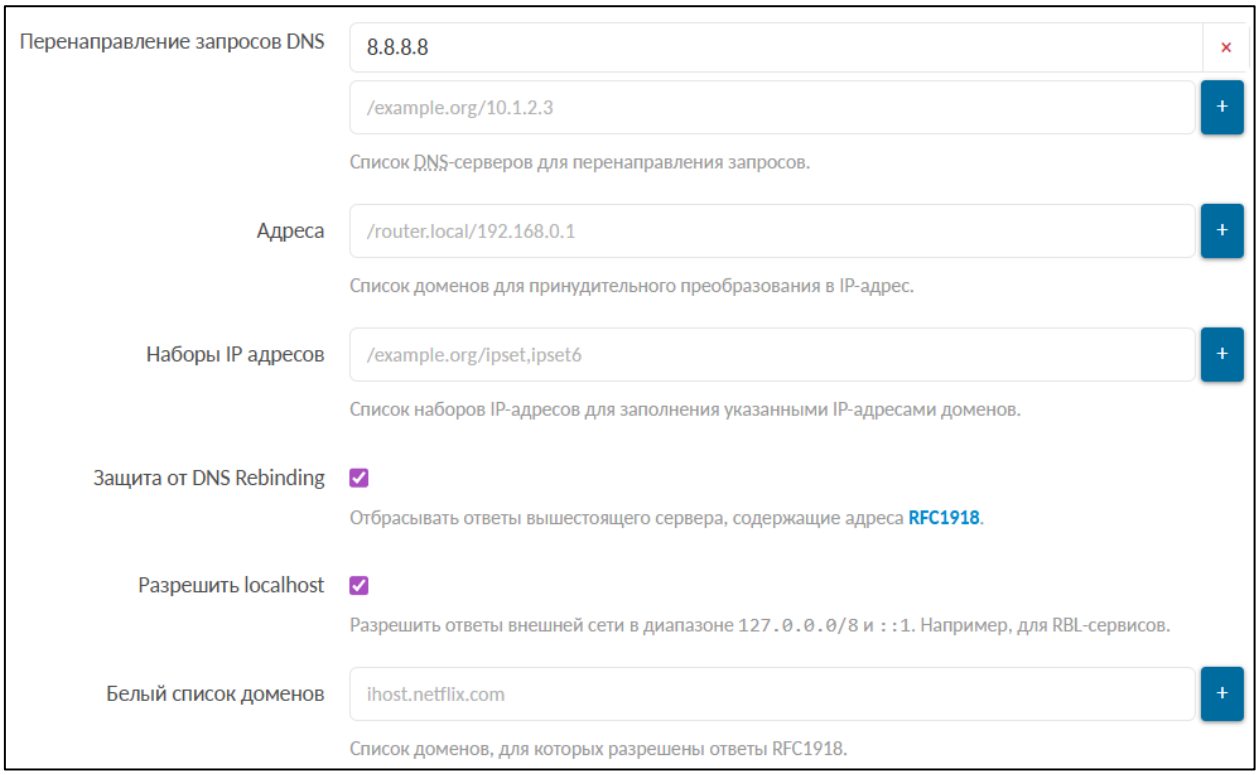


Рисунок 6-29: Страница «DHCP и DNS». Общие настройки. Перенаправление запросов DNS.

Дополнительные настройки DNS

- «Только локальный DNS» — ограничивает службу DNS только для подсетей интерфейса, использующего DNS.
- «Не использовать wildcard» — привязывать динамически к интерфейсам, а не по шаблону адреса.
- «Интерфейс для входящих соединений» — указывает интерфейсы, которые будет прослушивать служба DNS.
- «Исключить интерфейсы» — запрещает прослушивание указанных интерфейсов.

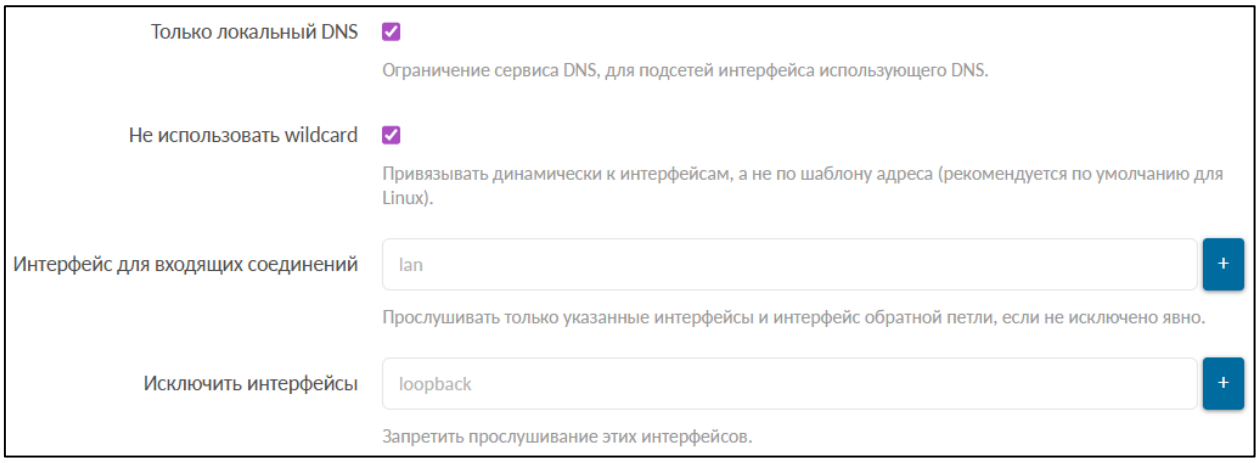


Рисунок 6-30: Страница «DHCP и DNS». Общие настройки. Дополнительные настройки DNS.

6.3.2 Настройки файлов «resolv.conf» и «hosts»

Во вкладке «Файлы resolv и hosts» страницы «DHCP и DNS» расположены настройки, касающиеся файлов «resolv.conf» и «hosts», а также дополнительных конфигурационных файлов DHCP-сервера. Внешний вид вкладки показан на рисунке 6-31.

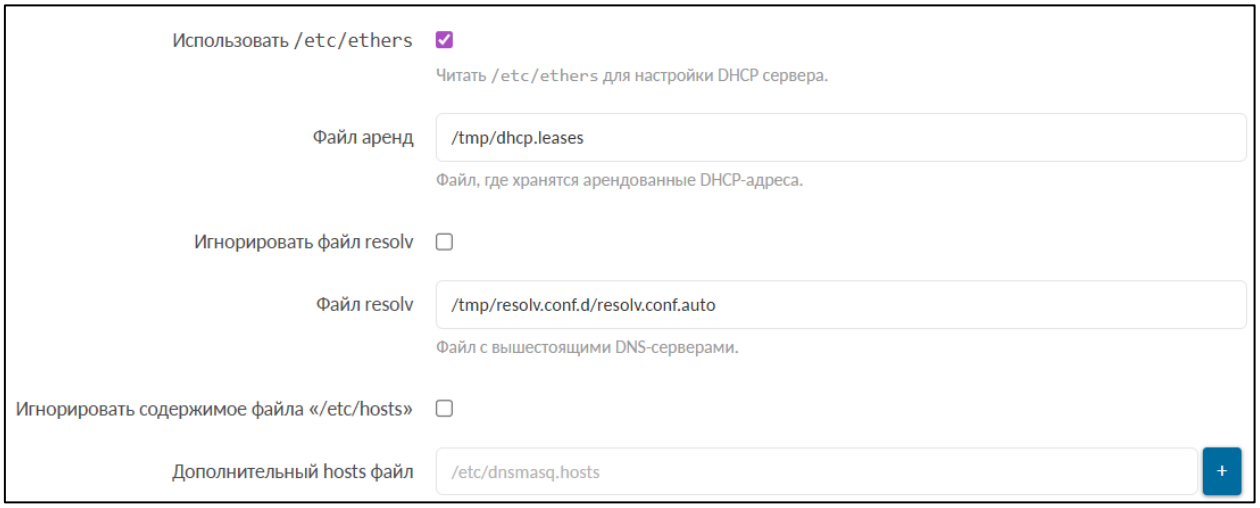


Рисунок 6-31: Страница «DHCP и DNS». Файлы resolv и hosts

На вкладке доступны следующие настройки:

– «Использовать /etc/ethers» — указание использовать конфигурационный файл «/etc/ethers» для настройки DHCP-сервера.
– «Файл аренд» — путь к файлу, где хранится информация об арендованных DHCP-адресах.

– «Игнорировать файл resolv» — указание службе dnsmasq игнорировать данные файла «resolv.conf».
– «Файл resolv» — путь к файлу «resolv.conf», содержащему список вышестоящих DNS-серверов.
– «Игнорировать содержимое файла «/etc/hosts»» — указание службе dnsmasq игнорировать данные файла «/etc/hosts».
– «Дополнительный hosts файл» — позволяет указать один или несколько дополнительных файлов «hosts».

6.3.3 Настройки PXE/TFTP

Во вкладке «Настройки PXE/TFTP» страницы «DHCP и DNS» расположены параметры для настройки встроенного TFTP-сервера и PXE-опций загрузки. Внешний вид вкладки показан на рисунке 6-32.

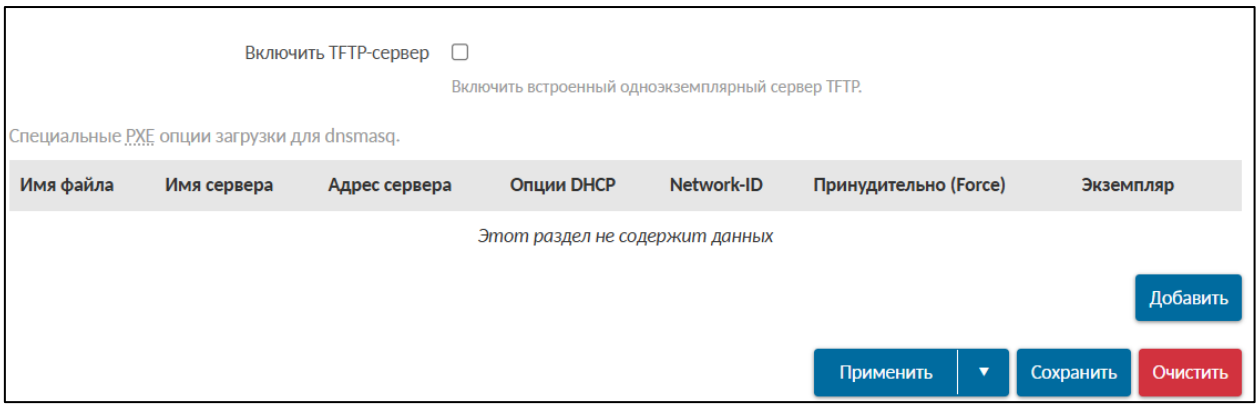


Рисунок 6-32: Страница «DHCP и DNS». Настройки PXE/TFTP

Для активации TFTP-сервера на странице предусмотрена галочка «Включить TFTP-сервер».

В подразделе «Специальные PXE опции загрузки для dnsmasq» отображается таблица уже созданных PXE-опций. Таблица имеет следующие столбцы:

– «Имя файла» — имя файла, который будет загружен клиентом (например, загрузочный образ);
– «Имя сервера» — имя TFTP-сервера, от которого клиенту следует загружать файл (опционально);

– «Адрес сервера» — IP-адрес TFTP-сервера (может отличаться от адреса самого устройства);
– «Опции DHCP» — дополнительные DHCP-опции, передаваемые клиенту вместе с PXE-параметрами;
– «Network-ID» — идентификатор сети, для которой применяются данные PXE-опции;
– «Принудительно (Force)» — принудительное применение опций независимо от запроса клиента;
– «Экземпляр» — идентификатор экземпляра PXE-сервера (позволяет различать несколько наборов опций).

При отсутствии настроенных PXE-опций в таблице отображается сообщение: «Этом раздел не содержит данных».

Для добавления новой PXE-опции предназначена кнопка «Добавить». При её нажатии открывается страница редактирования параметров PXE-опции.

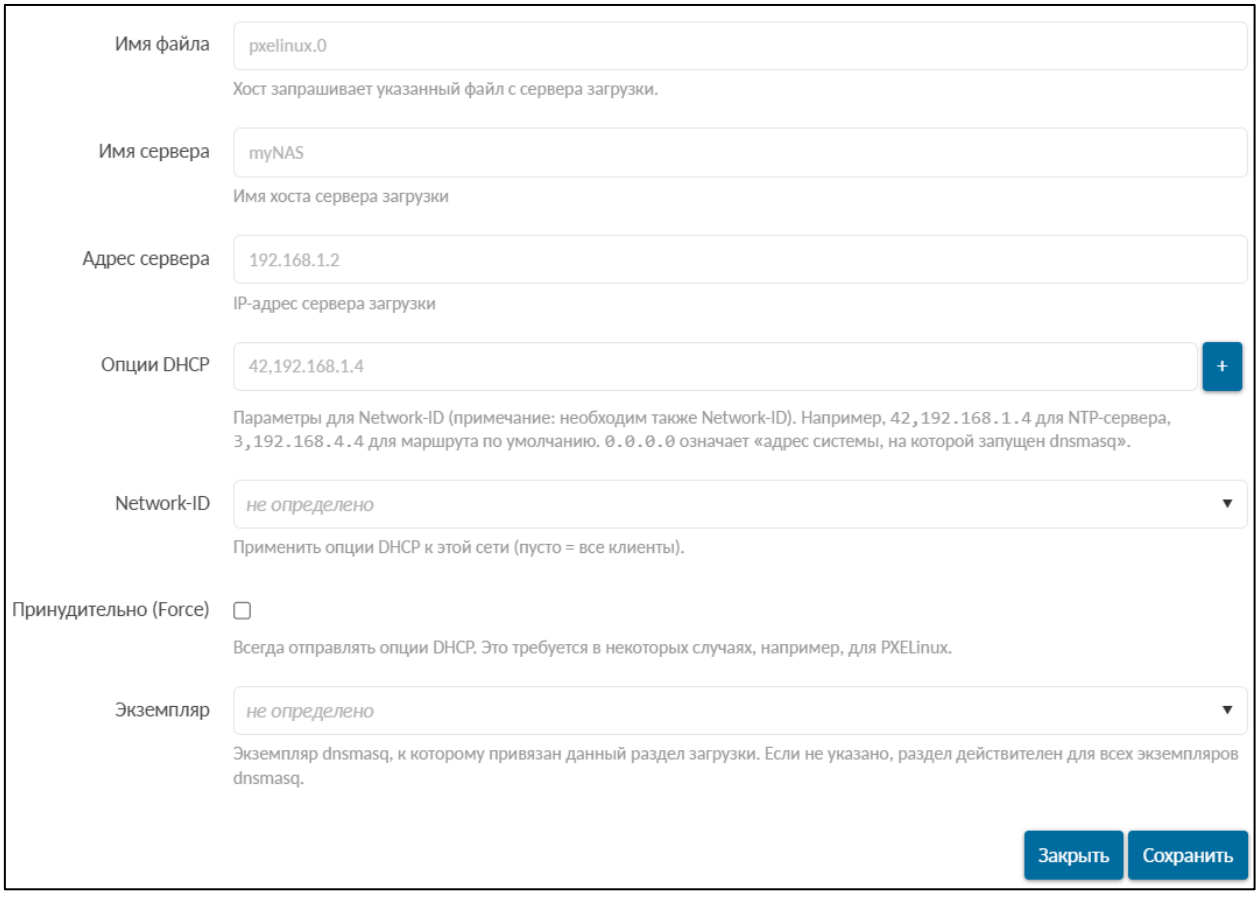


Рисунок 6-33: Параметры новой PXE-опции

6.3.4 Дополнительные настройки

Дополнительные настройки службы dnsmasq расположены во вкладке «Дополнительные настройки» страницы «DHCP и DNS».

Во вкладке доступны следующие настройки:

Логирование и поведение DHCP/DNS

- «Подавить логирование» — подавляет логирование стандартной работы протоколов DNS и DHCP.
- «Выделять IP-адреса последовательно» — выдавать DHCP-клиентам IP-адреса последовательно, начиная с меньшего доступного адреса.
- «Фильтровать частные» — не перенаправлять обратные DNS-запросы для локальных сетей (диапазоны RFC1918).
- «Фильтровать бесполезные» — не перенаправлять запросы, которые не могут быть обработаны публичными DNS-серверами (например, запросы для локальных доменов).
- «Локализовывать запросы» — локализовать имя хоста в зависимости от запрашиваемой подсети, если доступно несколько IP-адресов.
- «Расширять имена узлов» — добавлять локальный суффикс домена для имён из файла hosts («/etc/hosts»).

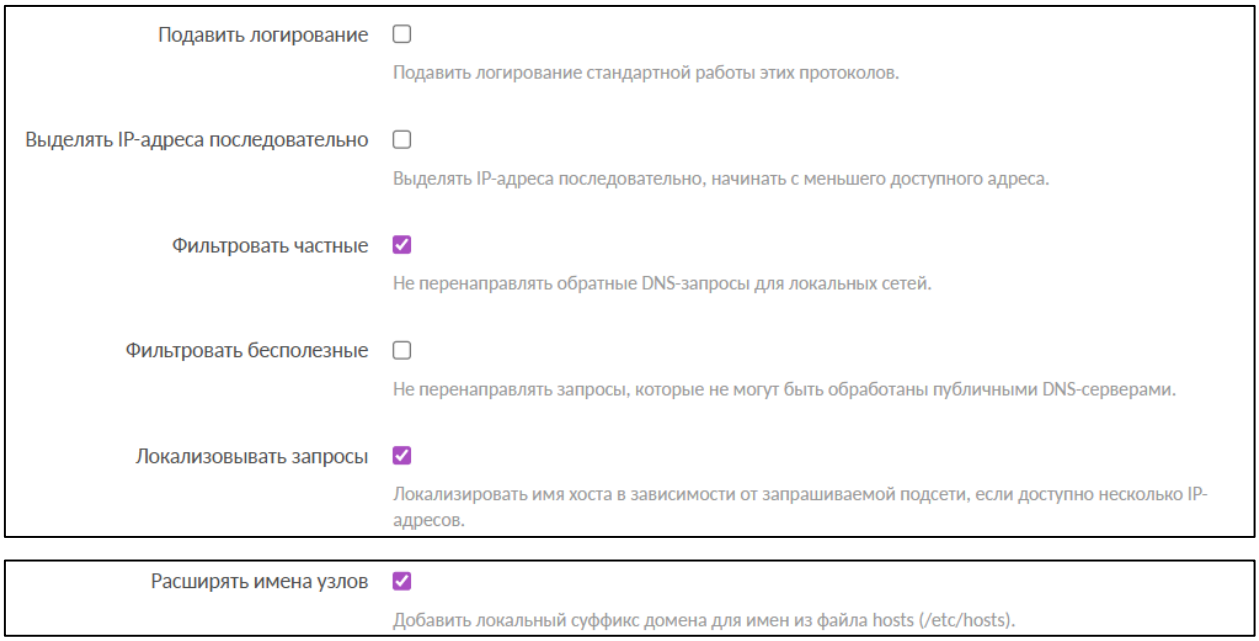


Рисунок 6-34: «DHCP и DNS». Дополнительные настройки. Логирование и поведение DHCP/DNS

Настройки DNSSEC

– «DNSSEC» — включает проверку DNSSEC. Требуется поддержка внешней сетью DNSSEC.

– «DNSSEC проверка без знака» — проверять, действительно ли ответы от неподписанных доменов приходят от неподписанных доменов.

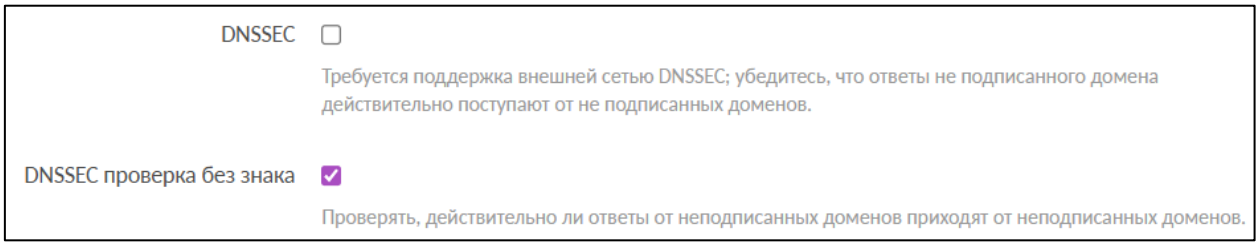


Рисунок 6-35: «DHCP и DNS». Дополнительные настройки. Настройки DNSSEC

Кэширование

– «Отключить кэш отрицательных ответов» — не кэшировать отрицательные ответы (например, для несуществующих доменов).

– «Размер кэша DNS запроса» — количество кэшированных DNS-записей. Максимальное значение — 10000. При указании значения «0» кэширование DNS-запросов будет отключено.

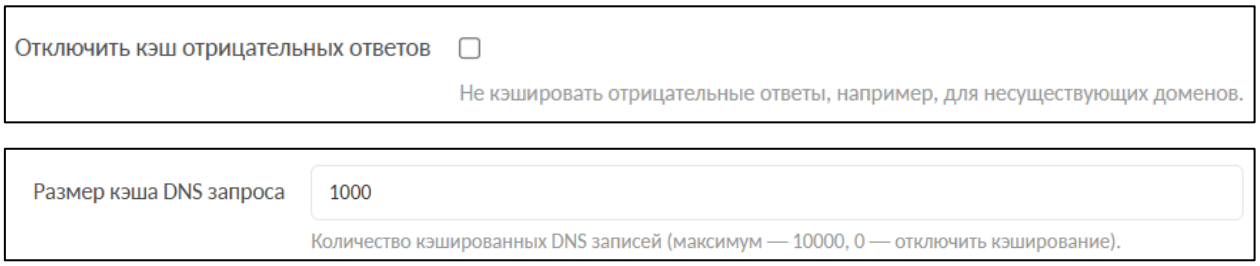


Рисунок 6-36: «DHCP и DNS». Дополнительные настройки. Кеширование

Файлы конфигурации

– «Дополнительный файл серверов» — путь к файлу со списком вышестоящих DNS-серверов, опционально специфичных для домена.

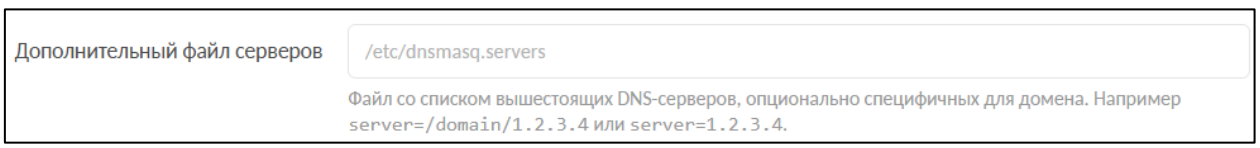


Рисунок 6-37: «DHCP и DNS». Дополнительные настройки. Файлы конфигурации

Порядок опроса DNS-серверов

– «Строгий порядок» — DNS-серверы будут опрашиваться строго в порядке, определённом в файле resolv.conf.
– «Все серверы» — опрашивать все имеющиеся внешние DNS-серверы.

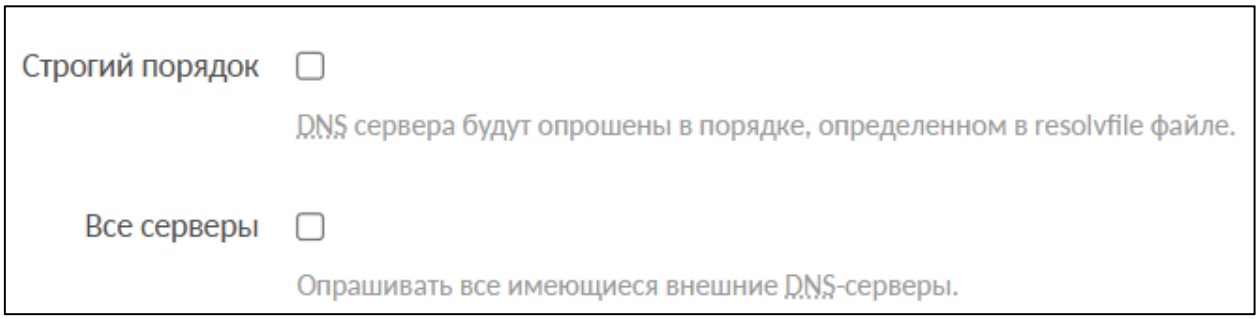


Рисунок 6-38: «DHCP и DNS». Дополнительные настройки. Порядок опроса DNS-серверов

Обработка NX-доменов

«Переопределение поддельного NX-домена» — список IP-адресов, поставляющих поддельные результаты домена NX (несуществующий домен).

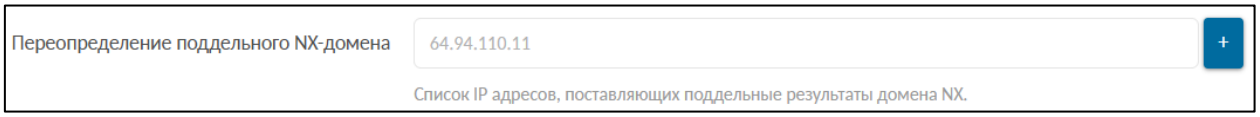


Рисунок 6-39: «DHCP и DNS». Дополнительные настройки. Обработка NX-доменов

Порты

«DNS порт сервера» — номер порта для входящих DNS-запросов.

«DNS порт запроса» — фиксированный порт для исходящих DNS-запросов.

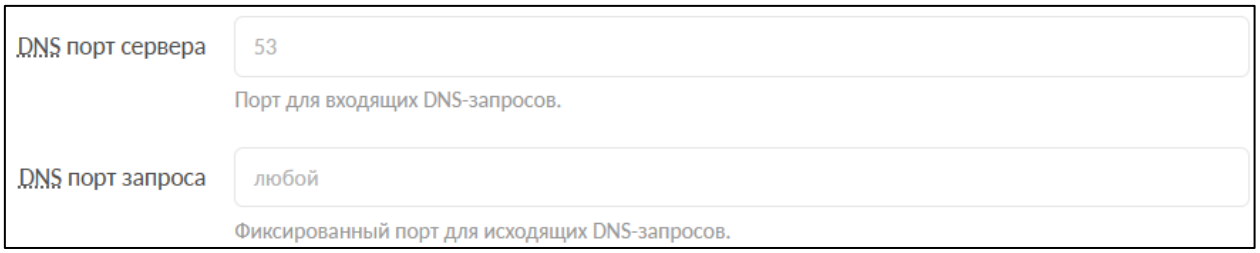


Рисунок 6-40 «DHCP и DNS». Дополнительные настройки. Порты

Ограничения

«Макс. кол-во аренд DHCP аренды» — максимальное количество активных арендованных DHCP-адресов.

«Макс. EDNS0 размер пакета» — максимально допустимый размер UDP-пакетов EDNS0.

«Макс. кол-во одновременных запросов» — максимальное количество одновременно обрабатываемых DNS-запросов.

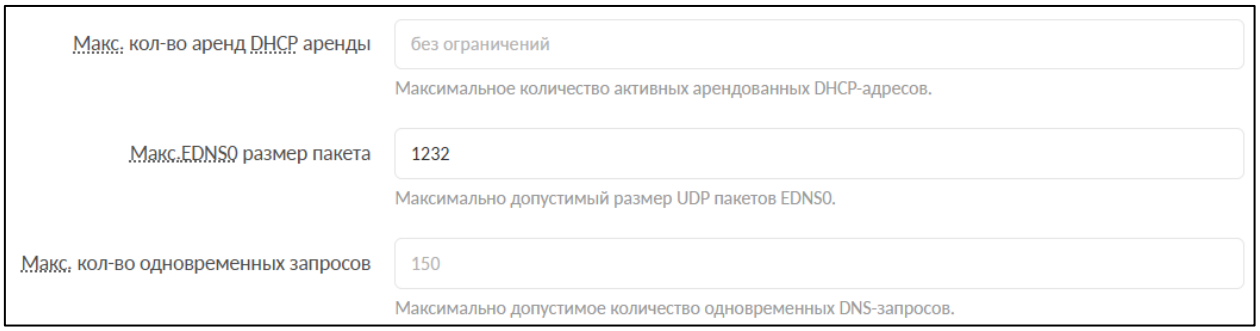


Рисунок 6-41 «DHCP и DNS». Дополнительные настройки. Ограничения

6.3.5 Постоянные аренды

Постоянная аренда используется для присвоения фиксированных IP-адресов и имён DHCP-клиентам. Постоянная аренда также необходима для статических интерфейсов, в которых обслуживаются только клиенты с присвоенными адресами.

Управление постоянными арендами размещено в подразделе «Постоянные аренды» страницы «DHCP и DNS». Внешний вид подразделе «Постоянные аренды» показан на рисунке 6-42.

Рисунок 6-42: Настройка постоянных аренд DHCP-сервера

Добавление новой постоянной аренды осуществляется нажатием кнопки «Добавить» с последующим указанием параметров постоянной аренды в добавленной строке таблицы (см. рисунок 6-43).

Рисунок 6-43: Добавление записи постоянной аренды DHCP-сервера

Удалить существующую постоянную аренду можно при помощи кнопки «Удалить», расположенной в строке соответствующей записи.

6.3.6 Имена устройств

В подразделе «Имена устройств» страницы «DHCP и DNS» производится настройка статических привязок доменных имён к IP-адресам. Внешний вид подраздела показан на рисунке 6-44.

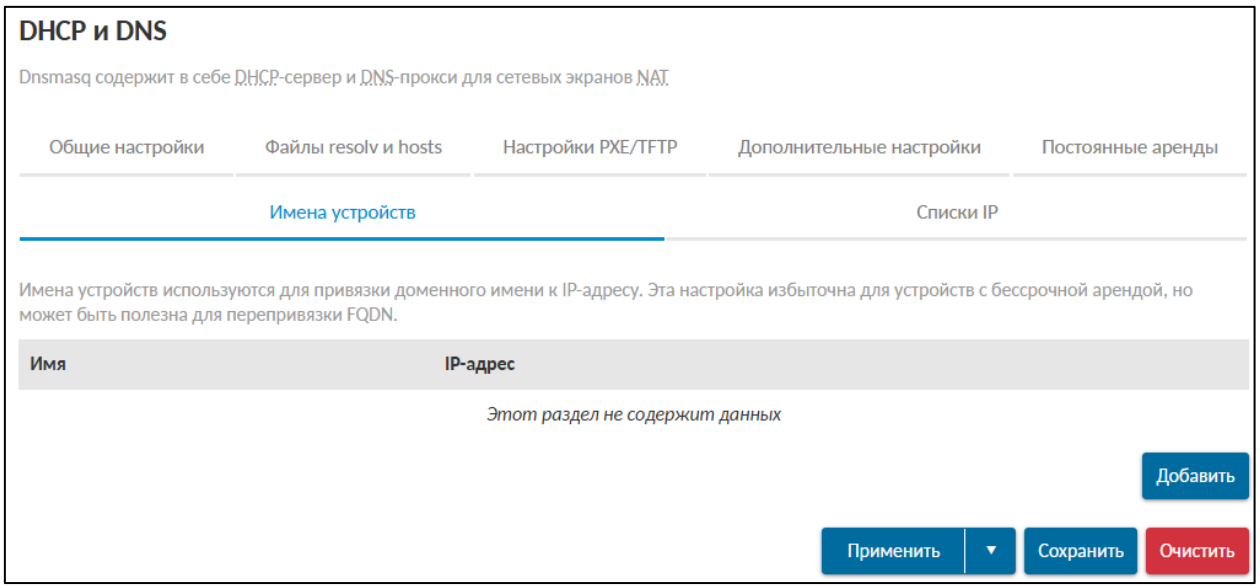


Рисунок 6-44: DHCP и DNS. Имена устройств

В подразделе отображается таблица уже созданных привязок имён к IP-адресам. Таблица имеет следующие столбцы:

– «Имя» — доменное имя (FQDN или короткое имя), которое будет привязано к указанному IP-адресу;
– «IP-адрес» — IP-адрес (IPv4 или IPv6), соответствующий указанному имени.

Для добавления новой привязки предназначена кнопка «Добавить». При её нажатии в таблице появляется новая строка для ввода имени и IP-адреса.

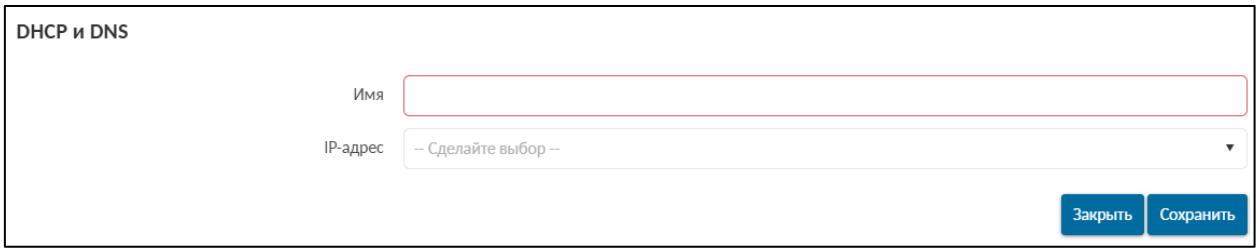


Рисунок 6-45: DHCP и DNS. Имена устройств. Добавление нового устройства

6.3.7 Списки IP

В подразделе «Списки IP» страницы «DHCP и DNS» производится настройка статических привязок доменных имён к наборам IP-адресов. Внешний вид подраздела показан на рисунке 6-46.

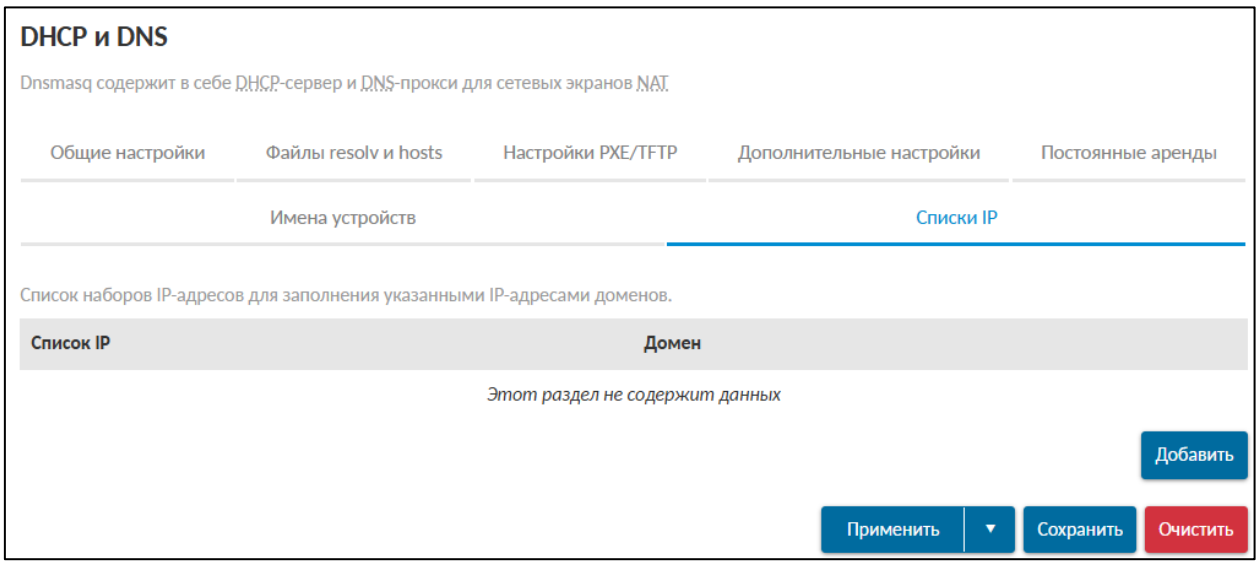


Рисунок 6-46: DHCP и DNS. Списки IP

В подразделе отображается таблица уже созданных привязок доменов к наборам IP-адресов. Таблица имеет следующие столбцы:

– «Список IP» — имя набора IP-адресов (ipset), который будет заполнен IP-адресами указанных доменов;
– «Домен» — доменное имя, IP-адреса которого будут добавлены в указанный набор.

При отсутствии настроенных привязок в таблице отображается сообщение: «Этот раздел не содержит данных».

Для добавления новой привязки предназначена кнопка «Добавить». При её нажатии в таблице появляется новая строка для ввода имени набора IP-адресов и домена.

Рисунок 6-47: DHCP и DNS. Добавление нового списка IP

6.4 Диагностика

На странице «Диагностика» раздела «Сеть» реализован интерфейс к некоторым диагностическим сетевым утилитам:

– «Пинг-запрос
– «Трассировка»
– «DNS-запрос»
– Внешний IP-адрес
– ARP сканирование

6.4.1 Пинг-запрос

Выполнение диагностики пинг-запроса для IPv4-адреса соответствует выполнению команды:

```
ping -c 5 -W 1 <адрес>
```

или для IPv6-адреса:

```
ping6 -c 5 <адрес>
```

Результат выполнения пинг-запроса отображается в текстовом виде под формой ввода. Ниже приведён пример вывода успешного пинг-запроса для адреса ya.ru:

```
PING ya.ru (87.250.250.242): 56 data bytes
64 bytes from 87.250.250.242: seq=0 ttl=48 time=16.959 ms
64 bytes from 87.250.250.242: seq=1 ttl=48 time=17.029 ms
64 bytes from 87.250.250.242: seq=2 ttl=48 time=17.197 ms
64 bytes from 87.250.250.242: seq=3 ttl=48 time=17.338 ms
64 bytes from 87.250.250.242: seq=4 ttl=48 time=16.608 ms
--- ya.ru ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 16.608/17.026/17.338 ms
```

6.4.2 Трассировка

Выполнение трассировки для IPv4-адреса соответствует выполнению команды:

```
traceroute -q 1 -w 1 -n <адрес>
```

или для IPv6-адреса:

```
traceroute6 -q 1 -w 2 -n <адрес>
```

Результат выполнения пинг-запроса отображается в текстовом виде под формой ввода. Ниже приведён пример вывода успешной трассировки для адреса ya.ru:

```
traceroute to ya.ru (87.250.250.242), 30 hops max, 38 byte packets
1 192.168.0.1 0.598 ms
2 10.82.190.5 2.009 ms
3 212.232.64.221 2.274 ms
4 212.232.64.209 0.857 ms
5 212.232.64.85 0.980 ms
6 212.232.67.218 1.172 ms
7 188.65.69.56 0.823 ms
```

8 188.65.69.65 1.152 ms
9 46.19.184.17 1.225 ms
10 46.19.184.5 1.090 ms
11 194.226.100.90 1.319 ms
12 *
13 87.250.250.242 17.069 ms

6.4.3 DNS-запрос

Выполнение DNS-запроса адреса соответствует выполнению команды:

nslookup <адрес>

Результат выполнения пинг-запроса отображается в текстовом виде под формой ввода. Ниже приведён пример вывода успешного DNS-запроса для адреса ya.ru:

Server: 127.0.0.1
Address: 127.0.0.1#53
Name: ya.ru
Address 1: 87.250.250.242
Address 2: 2a02:6b8::2:242

6.4.4 Внешний IP-адрес

«Определить внешний IP-адрес» — кнопка, при нажатии на которую выполняется запрос к внешнему серверу для определения публичного IP-адреса. После выполнения запроса адрес отображается в соответствующем поле.

6.4.5 ARP-сканирование

Подраздел «ARP сканирование» позволяет выполнить сканирование локальной сети для обнаружения устройств по протоколу ARP.

6.5 Межсетевой экран

Настройки межсетевого экрана (брандмауэра) расположены на странице «Межсетевой экран» раздела «Сеть» и разделены на вкладки:

- «Общие настройки» — основные настройки межсетевого экрана и настройка зон
- «Перенаправление портов» — настройка правил перенаправления портов
- «Правила для трафика» — настройка правил межсетевого экрана для входящего, исходящего и перенаправляемого трафика
- «Правила NAT» — настройка правил трансляции сетевых адресов (NAT)
- «Пользовательские правила» — настройка пользовательских правил межсетевого экрана

6.5.1 Общие настройки

Внешний вид страницы «Межсетевой экран» с открытой вкладкой «Общие настройки» показан на рисунке 6-48.

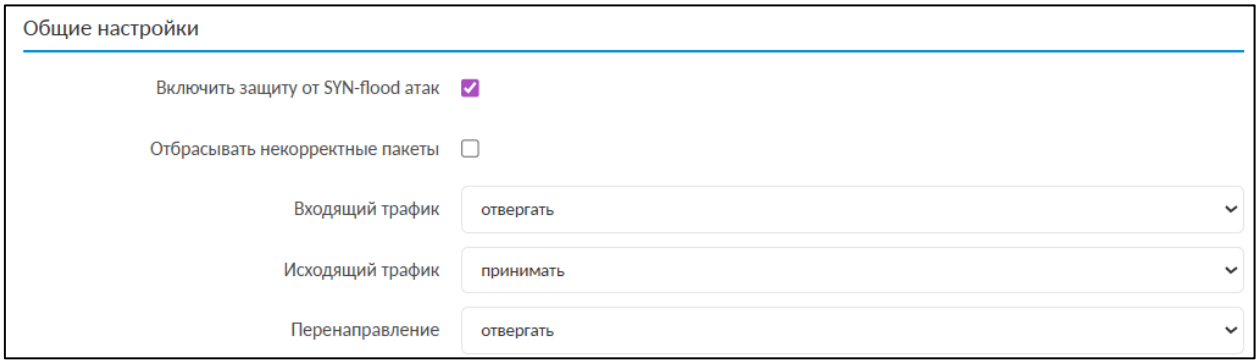


Рисунок 6-48: Общие настройки межсетевого экрана

На данной вкладке содержатся следующие настройки межсетевого экрана:

- «Включить защиту от SYN-flood атак» — управление функцией защиты от SYN-flood атак.
- «Отбрасывать некорректные пакеты» — управление функцией отбрасывания некорректных входящих пакетов.

– «Входящий трафик» — устанавливает политику «по умолчанию» для всего входящего трафика (принимать, отвергать или не обрабатывать).
– «Исходящий трафик» — устанавливает политику «по умолчанию» для всего исходящего трафика (принимать, отвергать или не обрабатывать).
– «Перенаправление» — устанавливает политику «по умолчанию» для всего перенаправляемого трафика (принимать, отвергать или не обрабатывать).

6.5.2 Настройка зон

В подразделе «Зоны» (вкладка «Общие параметры» страницы «Межсетевой экран») перечислены существующие зоны в виде таблицы с их основными параметрами в столбцах (см. рисунок 6-49).

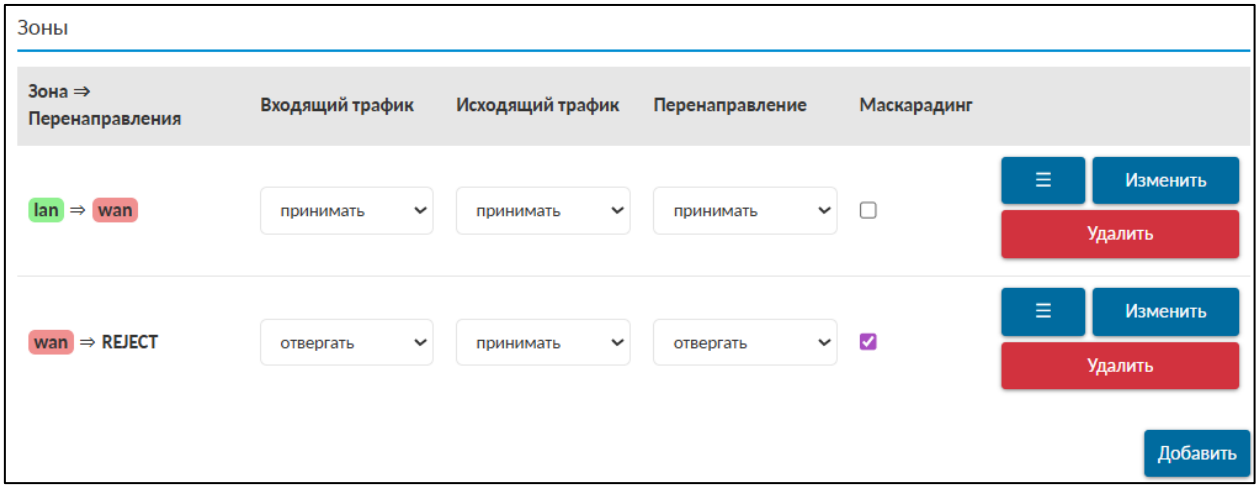


Рисунок 6-49: Настройка зон межсетевого экрана. Таблица зон

К основным параметрам зоны относятся следующие настройки (столбцы таблицы):

– «Входящий трафик» — устанавливает политику «по умолчанию» для всего исходящего трафика зоны (принимать, отклонять или не обрабатывать).
– «Исходящий трафик» — устанавливает политику «по умолчанию» для всего исходящего трафика зоны (принимать, отклонять или не обрабатывать).

– «Перенаправление» — устанавливает политику «по умолчанию» для всего перенаправляемого трафика зоны (принимать, отклонять или не обрабатывать).
– «Маскарадинг» — включает или отключает трансляцию IP-адресов для указанной зоны.

Дополнительно, в таблице приведены следующие параметры зон:

– «Зона => Перенаправления» — зона источник и зоны назначения, в которые разрешено перенаправление трафика (см. раздел 7.5.2.1).

6.5.2.1 Редактирование зон

Страница редактирования параметров зоны межсетевого экрана открывается при нажатии кнопки «Изменить» в строке соответствующей зоны. Страница разделена на несколько вкладок: «Общие настройки», «Дополнительные настройки», «Отслеживание соединений (conntrack)» и «Дополнительные аргументы iptables». Внешний вид страницы показан на рисунках 7-32 — 7-35.

6.5.2.1.1 Вкладка «Общие настройки»

На вкладке «Общие настройки» (см. рисунок 6-50) представлены основные параметры зоны:

– «Название» — уникальное символьное имя зоны (например, «lan»);
– «Входящий трафик» — устанавливает политику «по умолчанию» для всего входящего трафика зоны (принимать, отклонять или не обрабатывать);
– «Исходящий трафик» — устанавливает политику «по умолчанию» для всего исходящего трафика зоны (принимать, отклонять или не обрабатывать);
– «Перенаправление» — устанавливает политику «по умолчанию» для всего перенаправляемого трафика зоны (принимать, отклонять или не обрабатывать);

– «Маскарадинг» — включает или отключает трансляцию IP-адресов (NAT) для указанной зоны;
– «Ограничение MSS» — включает или отключает ограничение MSS (Maximum Segment Size) при передаче для данной зоны;
– «Охватываемые сети» — выбор сетевых интерфейсов, входящих в указанную зону.

В подразделе «Перенаправление между зонами» настраиваются политики перенаправления трафика между редактируемой зоной и другими зонами:

– Разрешить перенаправление в 'зоны назначения'» — разрешает перенаправление трафика из редактируемой зоны в зоны-назначения;
– «Разрешить перенаправление из 'зон источников'» — разрешает перенаправление трафика из выбранных зон-источников в редактируемую зону.

Перенаправление является однонаправленным. Например, перенаправление из зоны «lan» в зону «wan» не допускает перенаправление трафика из «wan» в «lan».

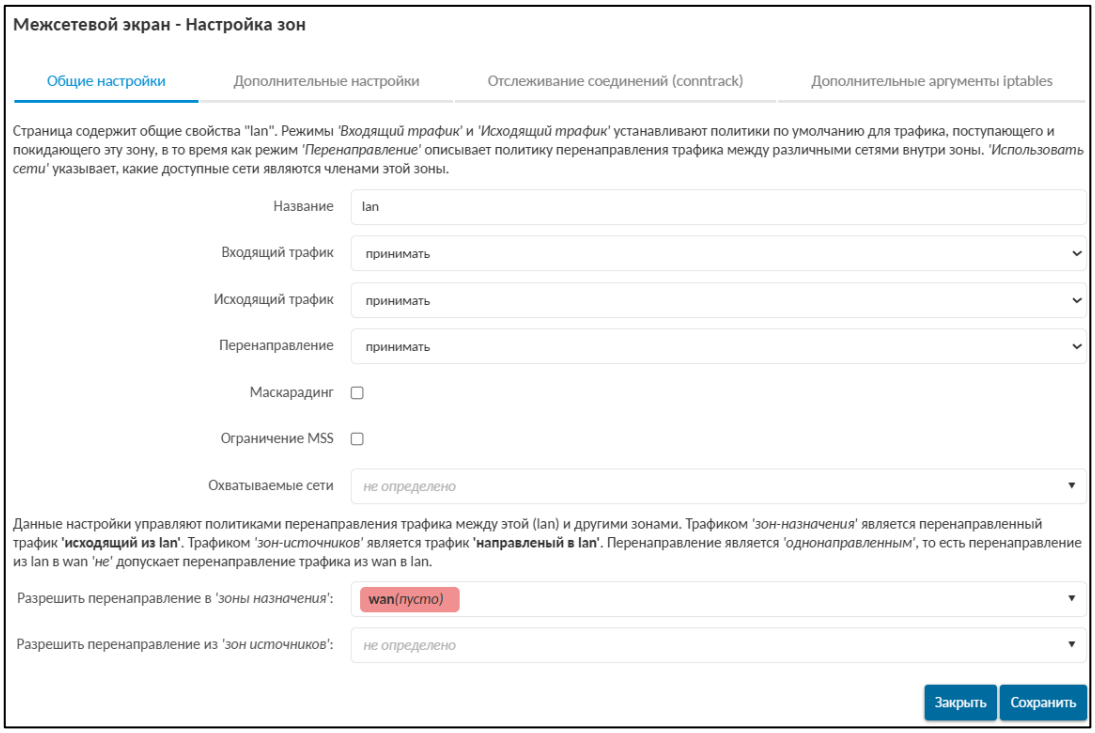


Рисунок 6-50: Настройка зон. Общие настройки

6.5.2.1.2 Вкладка «Дополнительные настройки»

На вкладке «Дополнительные настройки» (см. рисунок 6-51) доступны следующие параметры:

- «Охватываемые устройства» — позволяет классифицировать трафик зоны по сетевым устройствам, управляемым не через netifd.
- «Охватываемые подсети» — позволяет классифицировать трафик зоны по источнику или подсети назначения вместо сети или устройств.
- «Использовать протокол» — выбор версии используемого IP-протокола в указанной зоне.
- «Использовать маскарадинг только для указанных подсетей-отправителей» — позволяет ограничить использование трансляции адресов (маскарадинга) только для указанных подсетей-отправителей.
- «Использовать маскарадинг только для указанных подсетей-получателей» — позволяет ограничить использование трансляции адресов (маскарадинга) только для указанных подсетей-получателей.
- «Включить журналирование в этой зоне» — включает или отключает запись срабатывания правил межсетевого экрана для данной зоны в системный журнал.

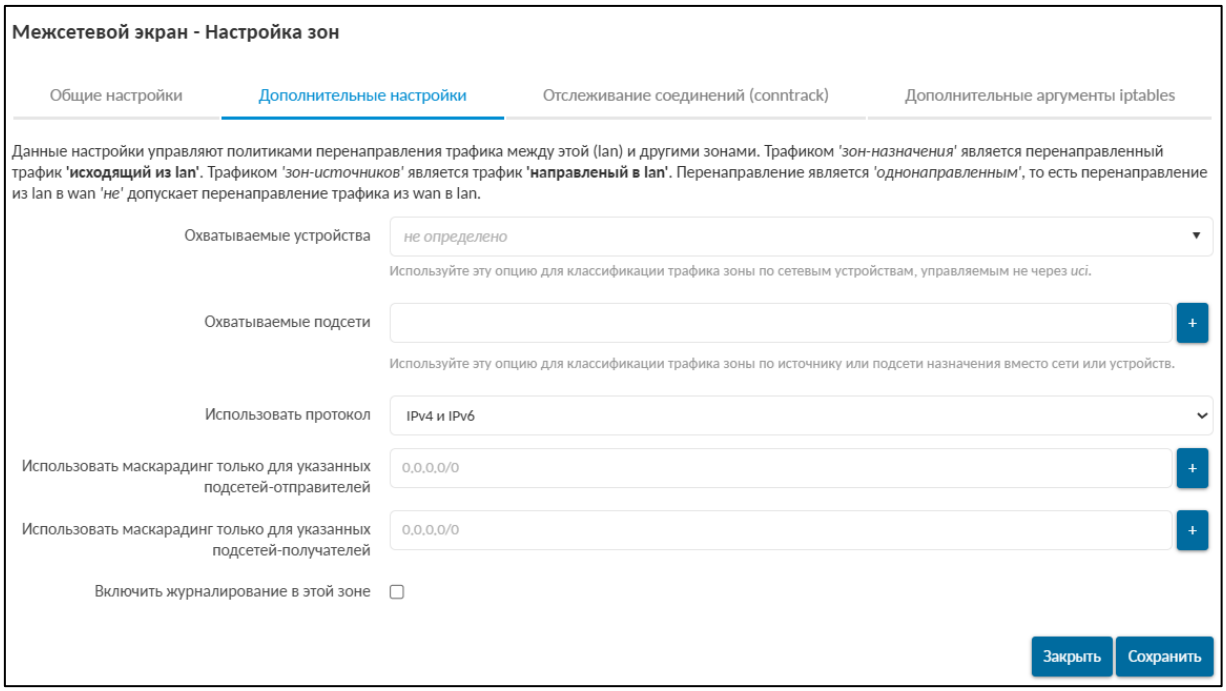


Рисунок 6-51: Настройка зон. Дополнительные настройки

6.5.2.1.3 Вкладка «Отслеживание соединений (conntrack)»

На вкладке «Отслеживание соединений (conntrack)» (см. рисунок 6-52) доступны следующие параметры:

– «Разрешить «недействительный» трафик» — при включении данной опции не устанавливаются дополнительные правила для отклонения перенаправляемого трафика с состоянием «invalid» (недействительный).
– «Автоматическое назначение помощников» — автоматическое назначение помощников отслеживания соединений (conntrack helpers) на основе протокола и порта трафика.

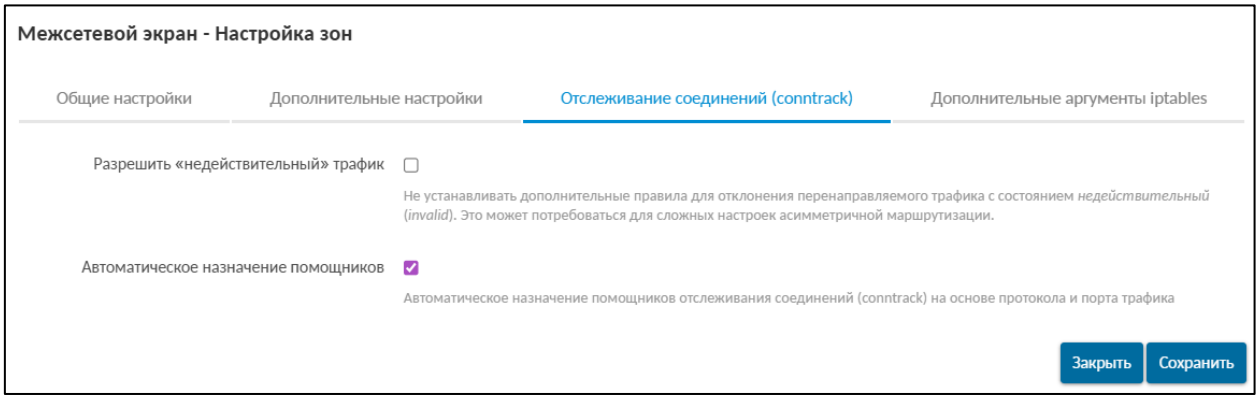


Рисунок 6-52: Настройка зон. «Отслеживание соединений (conntrack)»

6.5.2.1.4 Вкладка «Дополнительные аргументы iptables»

На вкладке «Дополнительные аргументы iptables» (см. рисунок 6-53) можно указать дополнительные аргументы для команд iptables. Данные опции следует использовать с особой осторожностью, так как неверные значения могут привести к нарушению работы правил межсетевого экрана, полностью открывая доступ ко всем службам системы.

– «Дополнительные аргументы для источника» — дополнительные аргументы iptables для классификации трафика зоны источника.
– «Дополнительные аргументы для назначения» — дополнительные аргументы iptables для классификации трафика зоны назначения.

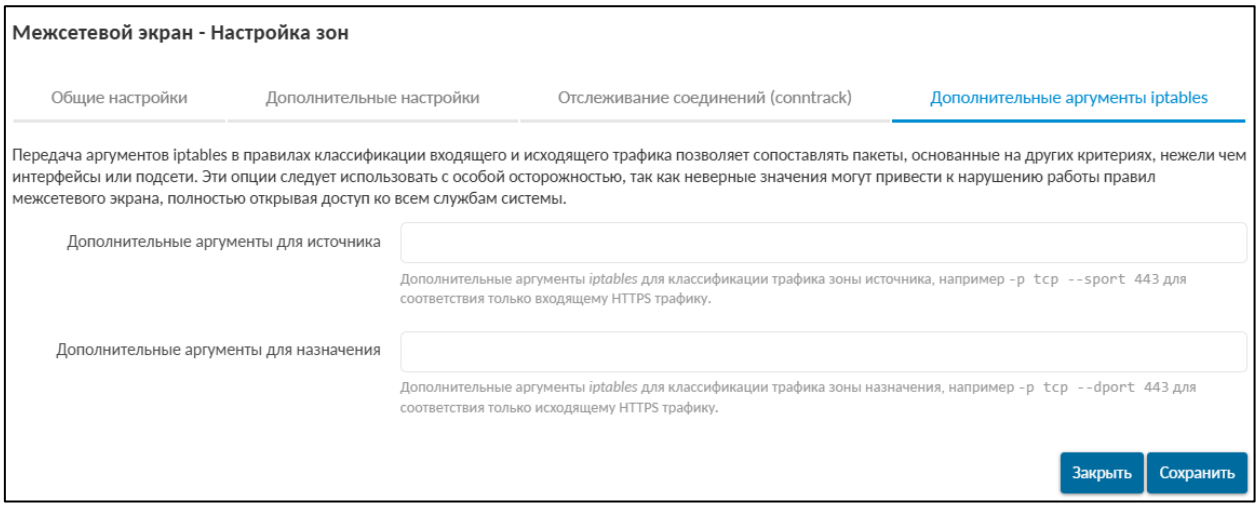


Рисунок 6-53: Настройка зон. «Дополнительные аргументы iptables»

6.5.2.2 Добавление зон

Для добавления новой зоны предназначена кнопка «Добавить», расположенная снизу таблицы зон. При этом открывается такая же страница редактирования параметров зоны, как и при изменении существующей зоны (см. раздел 5.5.2.1).

6.5.2.3 Удаление зон

Удаление существующей зоны выполняется при помощи кнопки «Удалить», расположенной в строке соответствующей зоны.

6.5.3 Перенаправление портов

Перенаправление портов — это сопоставление определённого порта на внешнем интерфейсе устройства с определённым портом нужного устройства в локальной сети. Перенаправление портов позволяет, например, удалённым компьютерам из сети интернет соединяться с устройством или службой внутри частной локальной сети.

Внешний вид вкладки «Перенаправление портов» страницы «Межсетевой экран» показан на рисунке 6-54.

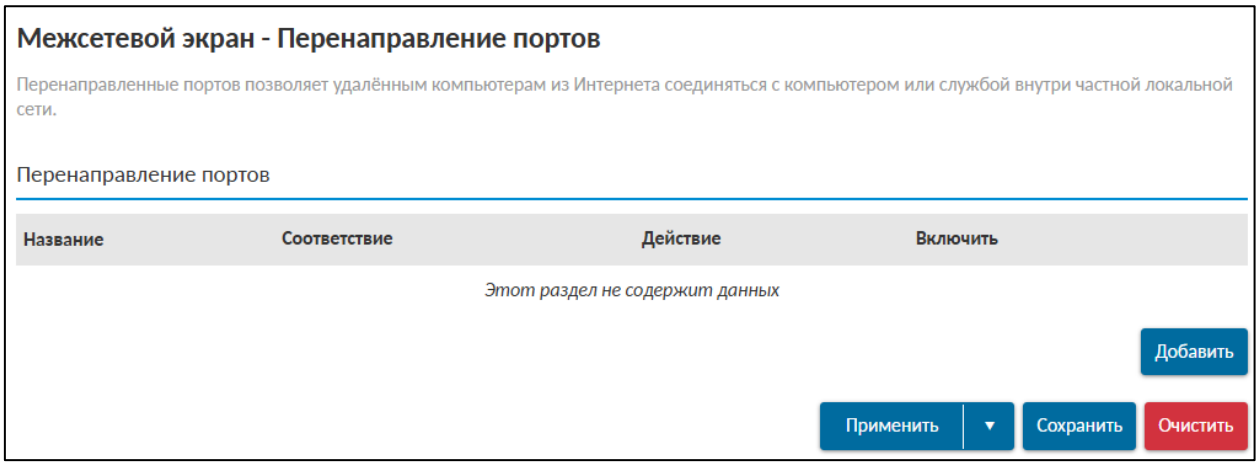


Рисунок 6-54: Вкладка «Перенаправление портов» страницы «Межсетевой экран»

В самом начале страницы приведена таблица «Перенаправление портов» с перечислением уже созданных правил перенаправления портов. Таблица имеет следующие столбцы:

- «Имя» — уникальное имя правила перенаправления.
- «Соответствие» — в данном столбце приведены условия для входящего трафика, при совпадении которых данное правило будет применяться.
- «Действие» — в данном столбце приведён адрес и порт устройства, куда будет перенаправляться трафик при применении данного правила.
- «Включить» — позволяет включить или отключить данное правило. Если правило выключено, то оно не будет применяться к входящему трафику.

6.5.3.1 Добавление правил перенаправления портов

Страница добавления правила перенаправления портов открывается при нажатии кнопки «Добавить». Страница разделена на вкладки «Общие настройки» и «Дополнительные настройки».

Вкладка «Общие настройки» содержит основные параметры правила перенаправления портов:

- «Название» — уникальное символьное имя правила.
- «Протокол» — выбор протокола для перенаправления.
- «Зона источника» — выбор зоны, из которой принимается входящий трафик для перенаправления.

– «Внешний порт» — порт или диапазон портов на внешнем интерфейсе, на который поступают входящие подключения.
– «Зона назначения» — выбор зоны, в которую будет перенаправляться трафик.
– «Внутренний IP-адрес» — IP-адрес устройства в локальной сети, на которое будет перенаправляться трафик.
– «Внутренний порт» — порт или диапазон портов на внутреннем устройстве, на который будет перенаправляться трафик.

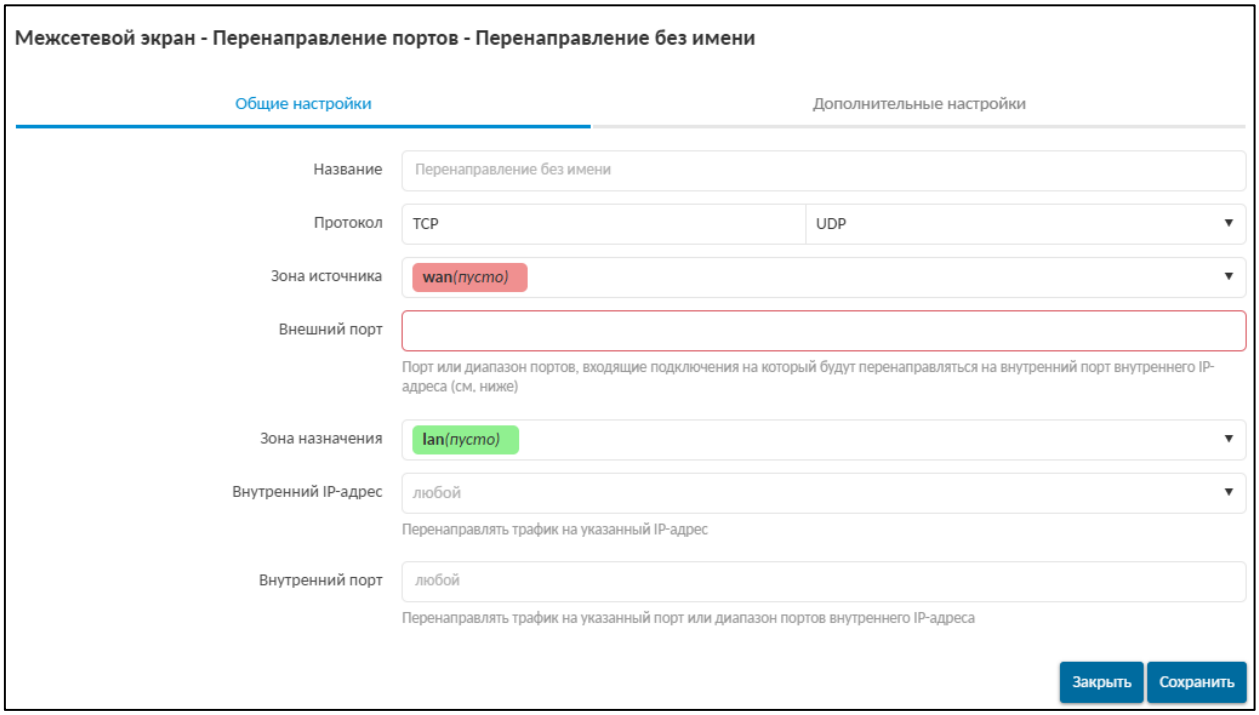


Рисунок 6-55: Перенаправление портов. Общие настройки

Вкладка «Дополнительные настройки» содержит следующие расширенные параметры:

– «MAC-адрес источника» — позволяет указать один или несколько MAC-адресов источника трафика.
– «IP-адрес источника» — позволяет указать IP-адрес или диапазон адресов источника трафика.
– «Порт источника» — позволяет указать порт или диапазон портов источника трафика.

- «Внешний IP-адрес» — позволяет ограничить применение правила для входящих подключений на указанный IP-адрес устройства.
- «Включить NAT Loopback» — включает технологию NAT Loopback, позволяющую считать пакет, пришедший из внутренней сети на внешний IP-адрес устройства, как пакет, пришедший извне.
- «IP-адрес источника петли (Loopback)» — определяет, использовать внешний или внутренний IP-адрес для отражённого трафика.
- «Соответствие помощнику» — определяет соответствие помощнику отслеживания соединений (conntrack helper).
- «Соответствие метки» — позволяет сопоставлять трафик с определённой меткой брандмауэра или диапазоном меток.
- «Соответствие по ограничениям» — ограничивает сопоставление трафика указанной скоростью (rate limiting).
- «Дополнительные аргументы» — позволяет передать дополнительные аргументы команде iptables.

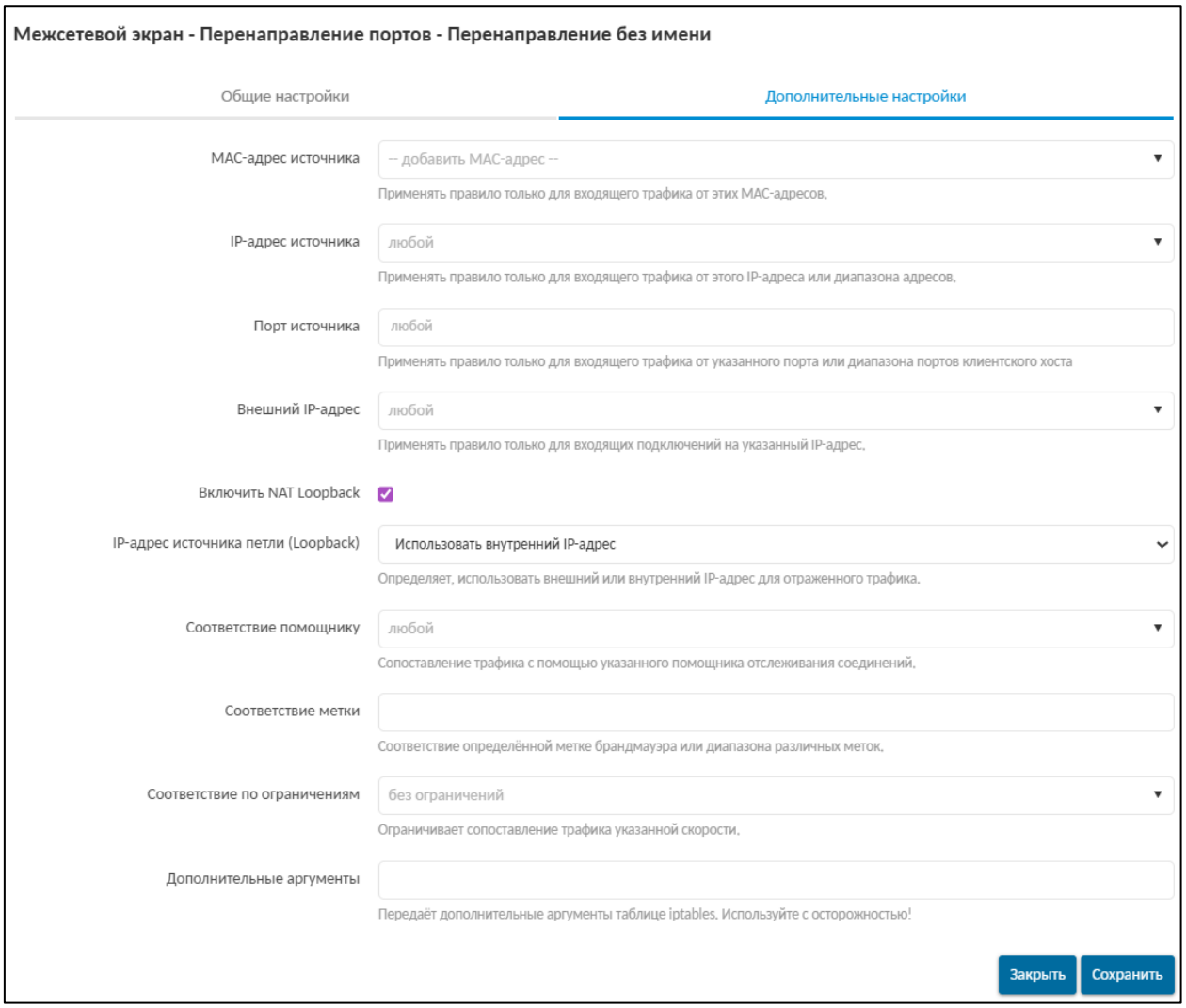


Рисунок 6-56 Перенаправление портов. Дополнительные настройки

6.5.3.2 Удаление правил перенаправления портов

Для удаления правила перенаправления портов предназначена кнопка «Удалить» (см. рисунок 6-54), расположенная в строке соответствующего правила.

6.5.4 Правила для трафика

Управление правилами для трафика межсетевого экрана осуществляется на вкладке «Правила для трафика» страницы «Межсетевой экран» (см. рисунок 6-57).

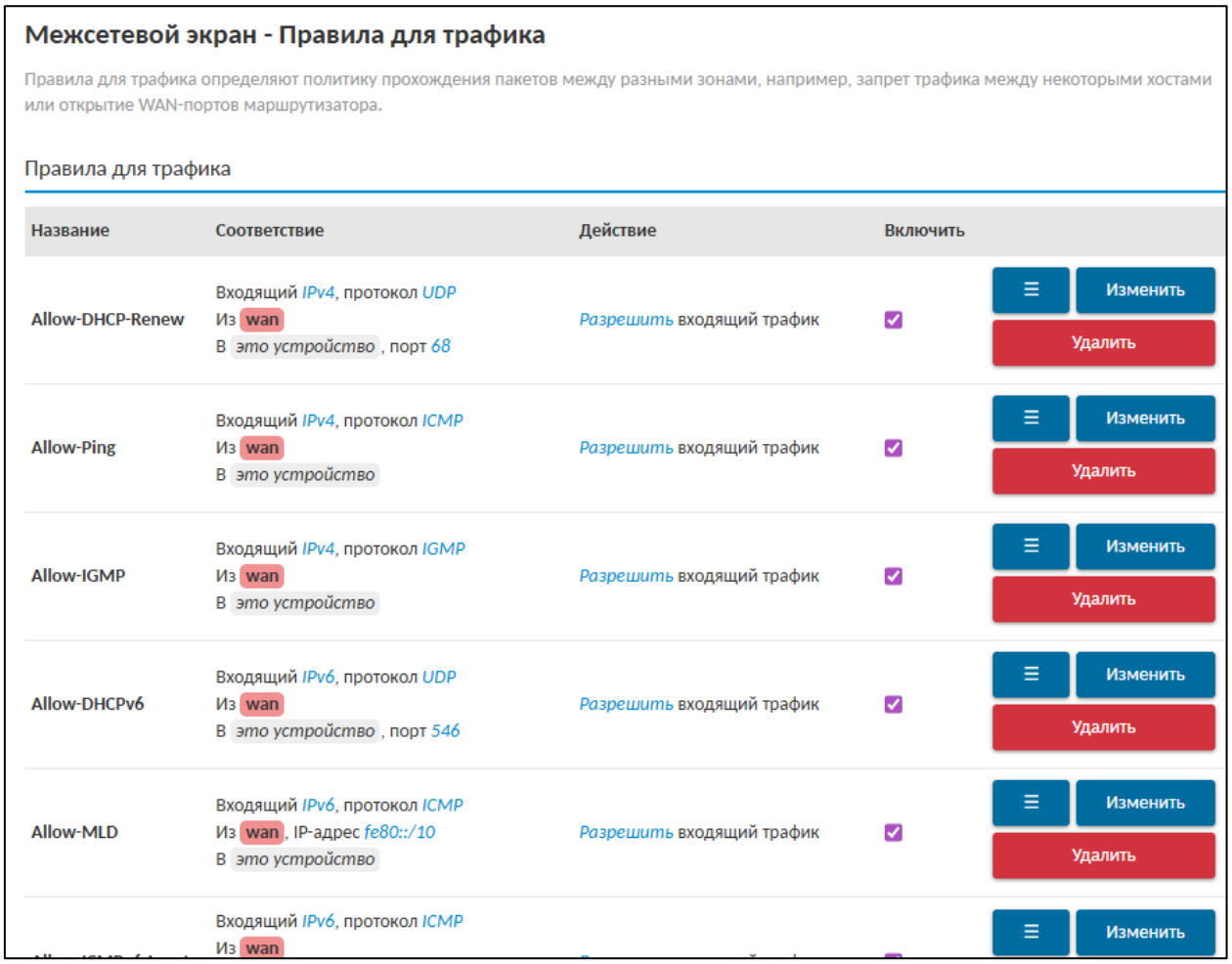


Рисунок 6-57: Правила для трафика межсетевого экрана

В самом начале страницы приведена таблица «Правила для трафика» с перечисленными уже созданными правилами для трафика. Таблица имеет следующие столбцы:

- «Название» — уникальное имя правила.
- «Соответствие» — в данном столбце приведены условия для входящего трафика, при совпадении которых данное правило будет применяться.
- «Действие» — действие, применяемое для трафика данного правила.
- «Включить» — позволяет включить или отключить данное правило.

6.5.4.1 Редактирование правил для трафика

Страница редактирования правила для трафика открывается при нажатии кнопки «Изменить» в строке соответствующего правила (см. раздел 7.5.4). Страница разделена на вкладки: «Общие настройки», «Дополнительные настройки» и «Временные ограничения».

Вкладка «Общие настройки» содержит основные параметры правила для трафика:

- «Название» — уникальное символьное имя правила (например, «Allow-DHCP-Renew»).
- «Протокол» — выбор протокола трафика, к которому применяется правило.
- «Зона источника» — выбор зоны, из которой поступает трафик для данного правила.
- «Адрес источника» — позволяет указать один или несколько IP-адресов источника трафика.
- «Порт источника» — позволяет указать порт или диапазон портов источника трафика. Доступно только для протоколов UDP и TCP.
- «Зона назначения» — выбор назначения трафика для правила.
- «Адрес назначения» — позволяет указать IP-адрес или диапазон адресов назначения.
- «Порт назначения» — позволяет указать порт/диапазон портов назначения.
- «Действие» — выбор действия, применяемого для трафика, соответствующего правилу.

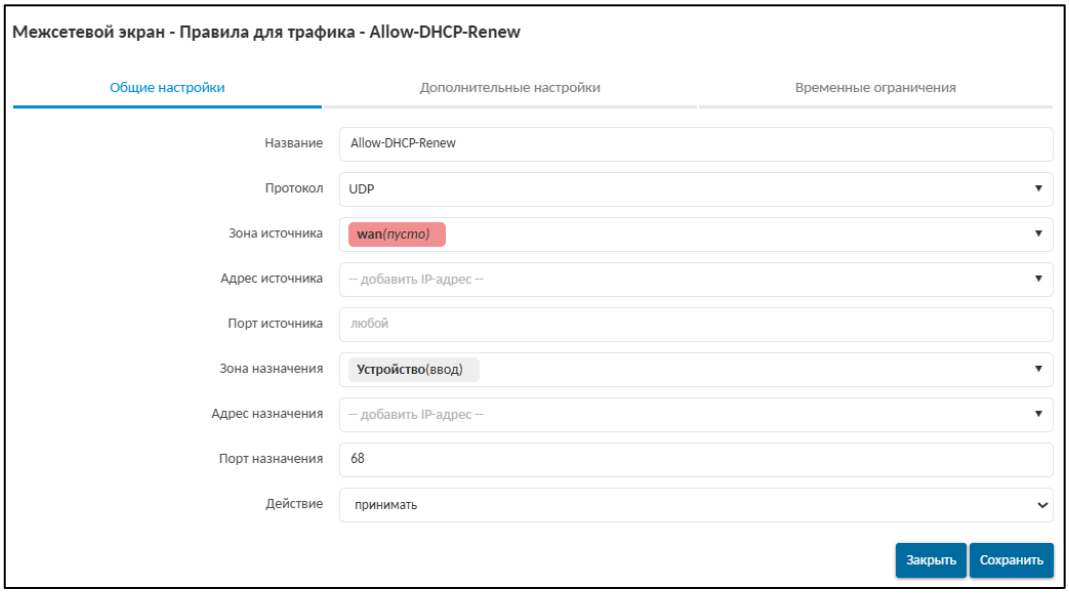


Рисунок 6-58: Правила для трафика. Общие настройки

Вкладка «Дополнительные настройки» содержит параметры, специфичные для конкретного протокола или типа правила.

- «Соответствие устройству» — позволяет сопоставлять трафик с указанным сетевым устройством (интерфейсом).
- «Использовать протокол» — выбор версии IP-протокола для данного правила. Доступные варианты:
- «MAC-адрес источника» — позволяет указать один или несколько MAC-адресов источника трафика.
- «Соответствие помощнику» — сопоставление трафика с помощью указанного помощника отслеживания соединений (conntrack helper).
- «Соответствие метки» — сопоставление трафика с определённой меткой брандмауэра или диапазоном меток.
- «Соответствие DSCP» — сопоставляет трафик с указанной DSCP-маркировкой (Differentiated Services Code Point).
- «Соответствие по ограничениям» — ограничивает сопоставление трафика указанной скоростью (rate limiting).
- «Дополнительные аргументы» — позволяет передать дополнительные аргументы команде iptables.

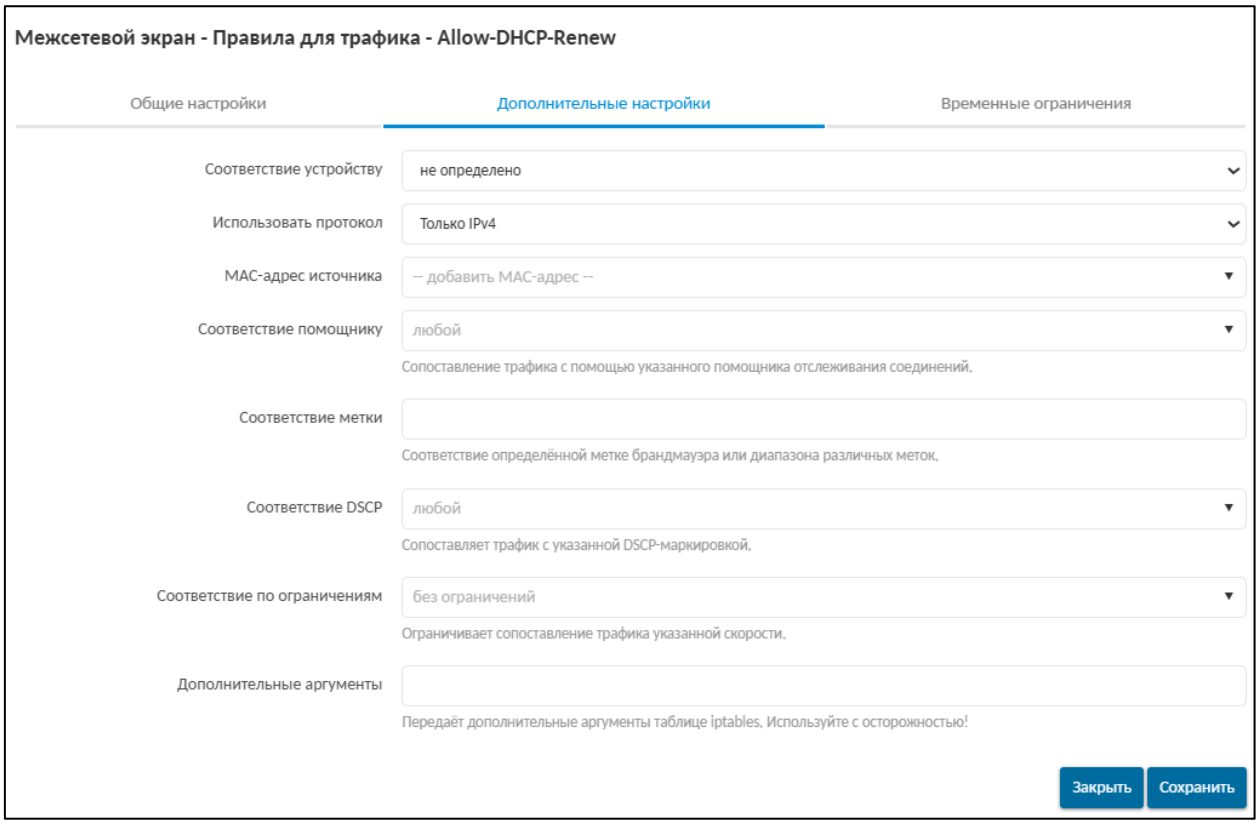


Рисунок 6-59: Правила для трафика. Дополнительные настройки

Вкладка «Временные ограничения» содержит настройки периода действия правила:

- «Дни недели» — позволяет указать дни недели, в которые правило должно применяться.
- «Дни месяца» — позволяет указать дни месяца, в которые правило должно применяться.
- «Время начала (чч:мм:сс)» — время начала действия правила.
- «Время окончания (чч:мм:сс)» — время окончания действия правила.
- «Дата начала (год-мес-день)» — дата начала действия правила.
- «Дата окончания (год-мес-день)» — дата окончания действия правила.
- «Время UTC» — если данная настройка включена, время действия правила указывается в UTC.

Рисунок 6-70: Правила для трафика. Временные ограничения

6.5.4.2 Удаление правил для трафика

Для удаления правила для трафика предназначена кнопка «Удалить», расположенная в строке соответствующего правила.

6.5.5 Правила NAT

На вкладке «Правила NAT» страницы «Межсетевой экран» производится настройка правил трансляции сетевых адресов (Network Address Translation). Правила NAT позволяют точно контролировать IP-адрес источника в исходящем или перенаправляемом трафике, а также выполнять преобразование адресов для определённых условий.

Внешний вид вкладки показан на рисунке 6-71.

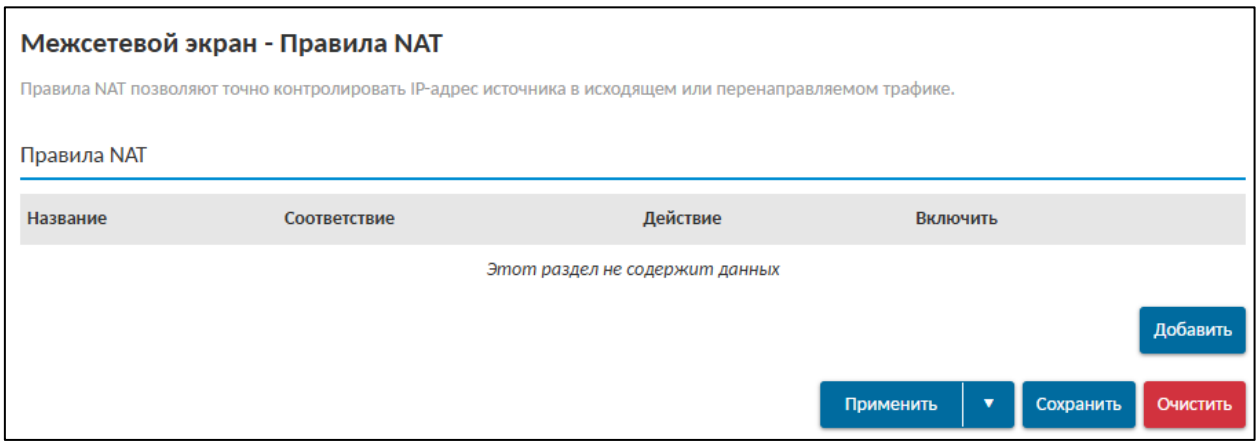


Рисунок 6-71: Правила NAT

В подразделе «Правила NAT» отображается таблица уже созданных правил NAT. Таблица имеет следующие столбцы:

- «Название» — уникальное символьное имя правила NAT;
- «Соответствие» — условия, при которых данное правило применяется;
- «Действие» — действие, выполняемое при совпадении условий;
- «Включить» — позволяет включить или отключить данное правило.

Добавление, изменение и удаление правил:

- «Добавить» — кнопка для создания нового правила NAT. При её нажатии открывается страница редактирования параметров правила (аналогично другим разделам межсетевого экрана).
- «Изменить» — для редактирования существующего правила необходимо нажать кнопку «Изменить» в строке соответствующего правила (подразумевается, но на скриншоте не показана).
- «Удалить» — для удаления правила предназначена кнопка «Удалить» в строке соответствующего правила.

6.5.6 Пользовательские правила

На вкладке «Пользовательские правила» настроек межсетевого экрана (см. рисунок 6-72) расположено поле ввода, в котором можно указывать произвольные команды iptables. Данные команды будут автоматически выполняться после каждой перезагрузки службы межсетевого экрана следом за загрузкой правил по умолчанию.

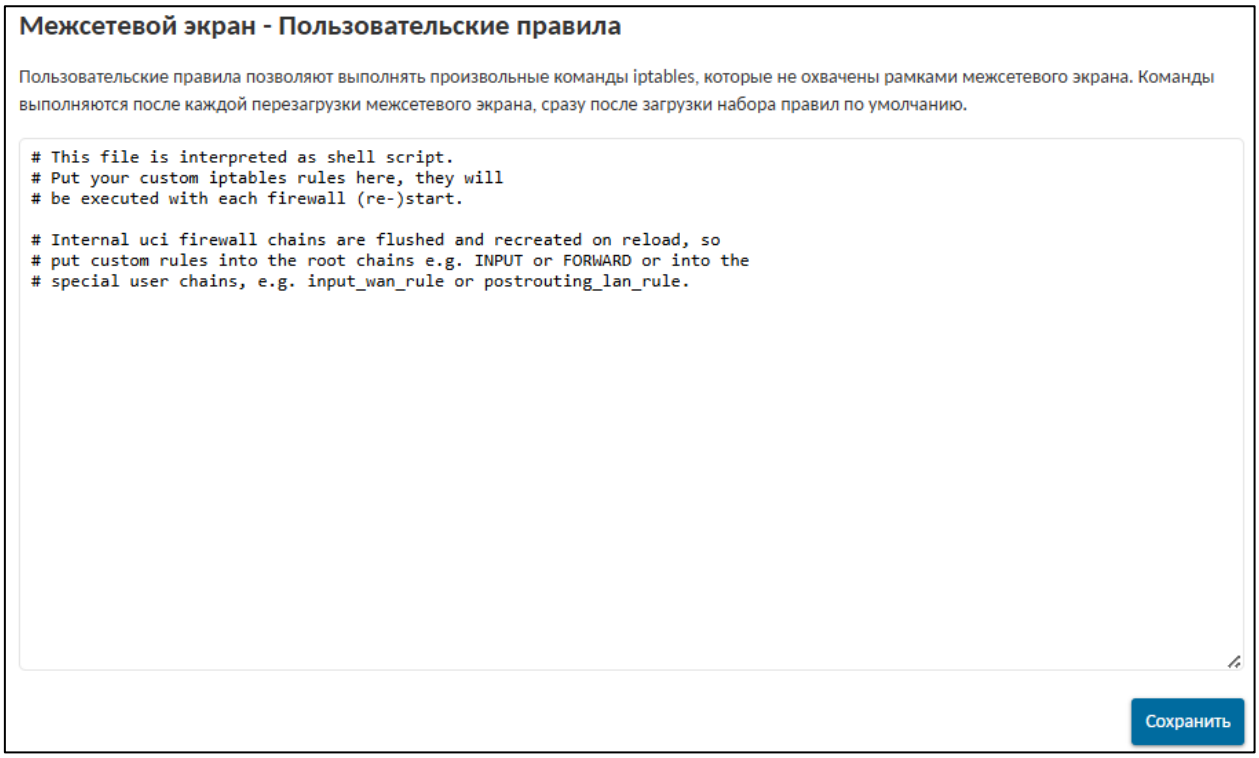


Рисунок 6-72: Пользовательские правила межсетевого экрана

7 VPN

В данном разделе описывается настройка VPN-подключений с использованием OpenVPN.

Внешний вид страниц показан на рисунках 7-1…7-4.

7.1 OpenVPN

Страница «OpenVPN» раздела «VPN» позволяет управлять экземплярами OpenVPN-серверов и клиентов, создавать новые конфигурации и загружать готовые файлы .ovpn.

7.1.1 Экземпляры OpenVPN

В подразделе «Экземпляры OpenVPN» (см. рисунок 7-1) отображается таблица всех настроенных экземпляров OpenVPN с их текущим состоянием.

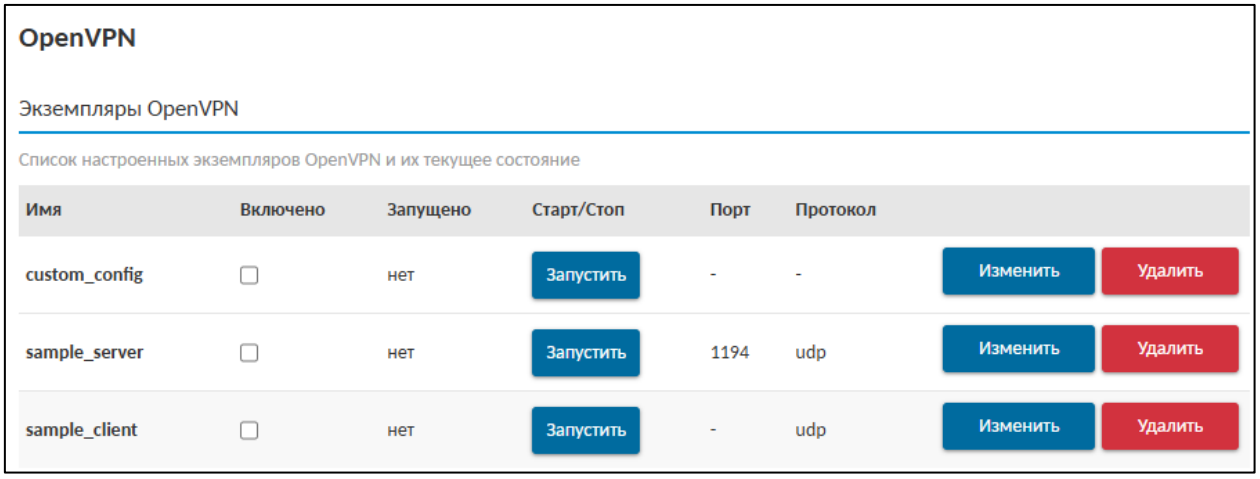


Рисунок 7-1: VPN. Экземпляры OpenVPN

Таблица имеет следующие столбцы:

- «Имя» — пользовательское имя экземпляра;
- «Включено» — флаг, указывающий, активирован ли данный экземпляр;
- «Запущено» — текущее состояние экземпляра;
- «Старт/Стоп» — кнопка для запуска или остановки экземпляра;
- «Порт» — номер TCP/UDP порта, используемого экземпляром;
- «Протокол» — используемый протокол;
- «Изменить» — кнопка для редактирования параметров экземпляра;

– «Удалить» — кнопка для удаления экземпляра.

7.1.1.1 Редактирование экземпляра OpenVPN

Страница редактирования экземпляра OpenVPN (см. рисунок 7-2) открывается при нажатии кнопки «Изменить» в строке соответствующего экземпляра (см. рисунок 7-1). На странице представлены основные параметры конфигурации OpenVPN.

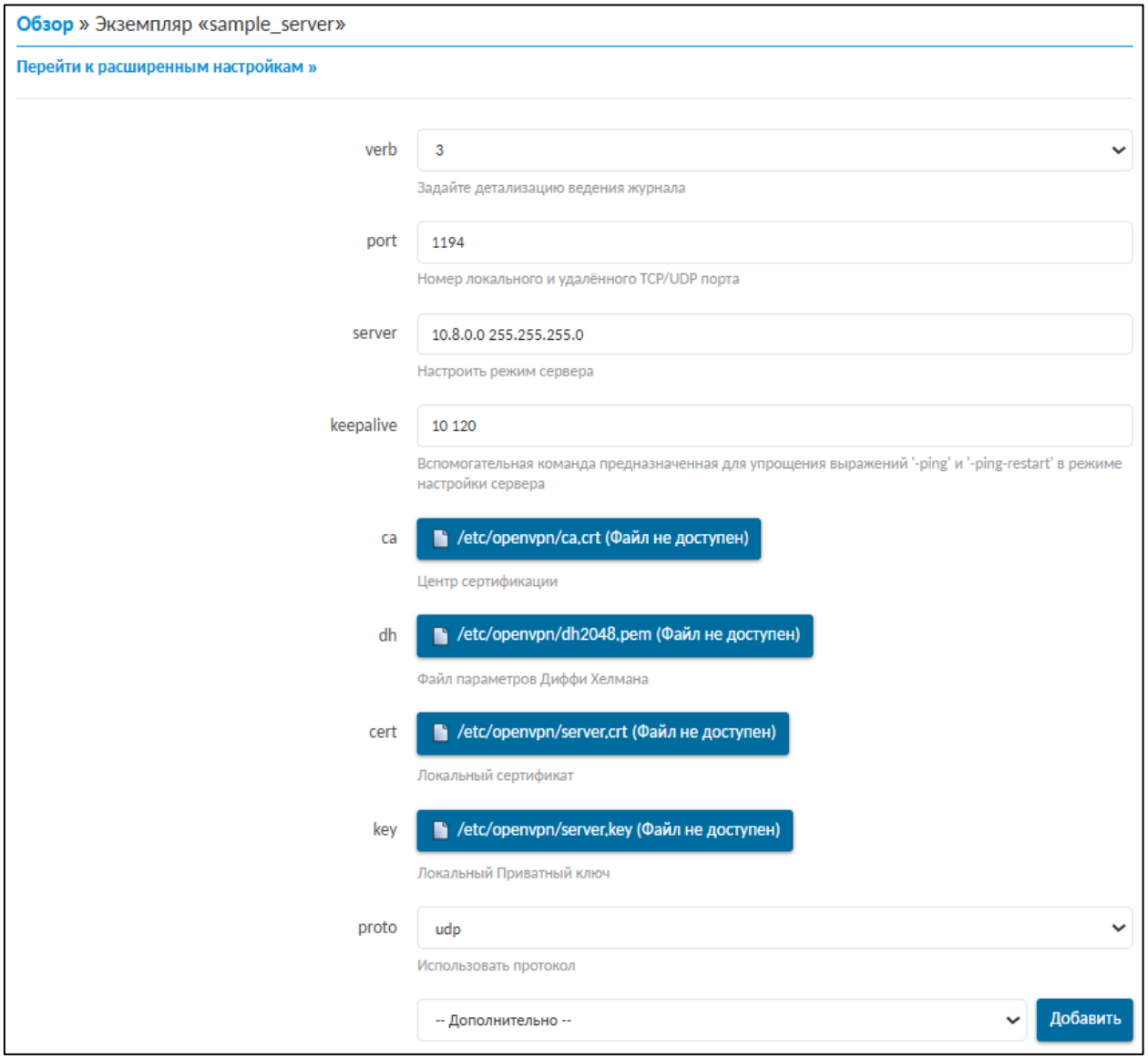


Рисунок 7-2: VPN. Редактирование экземпляра OpenVPN (на примере «sample_server»)

– «verb» — уровень детализации ведения журнала;
– «port» — номер локального TCP/UDP порта для входящих соединений или удалённого порта;

– «server» — настройка режима сервера. Указывается сеть и маска подсети для клиентов;
– «keepalive» — вспомогательная команда для упрощения выражений ping и ping-restart. Указываются два значения: интервал пинга и таймаут перезапуска;
– «ca» — путь к файлу центра сертификации (Certificate Authority). При отсутствии файла отображается сообщение «Файл не доступен».
– «dh» — путь к файлу параметров Диффи-Хеллмана;
– «cert» — путь к локальному сертификату;
– «key» — путь к локальному приватному ключу;
– «proto» — выбор протокола для соединения;
– «Дополнительно» — выпадающий список дополнительных настроек.

7.1.2 Конфигурация на основе шаблонов

В подразделе «Конфигурация на основе шаблонов» (см. рисунок 7-3) можно быстро создать новый экземпляр OpenVPN, выбрав один из предустановленных шаблонов.

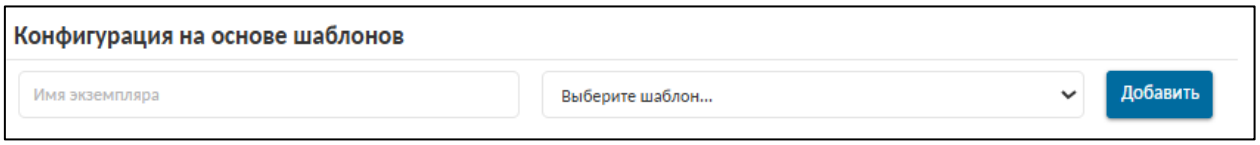


Рисунок 7-3: VPN. Конфигурация на основе шаблонов

– «Имя экземпляра» — поле для ввода имени создаваемого экземпляра;
– «Выберите шаблон…» — пример шаблона из выпадающего списка. Доступны различные шаблоны для сервера и клиента.;
– «Добавить» — кнопка для создания экземпляра на основе выбранного шаблона.

7.1.3 Загрузка конфигурационного файла OVPN

В подразделе «Загрузка конфигурационного файла OVPN» (см. рисунок 7-4) можно загрузить готовый конфигурационный файл OpenVPN (с расширением .ovpn) для создания нового экземпляра.

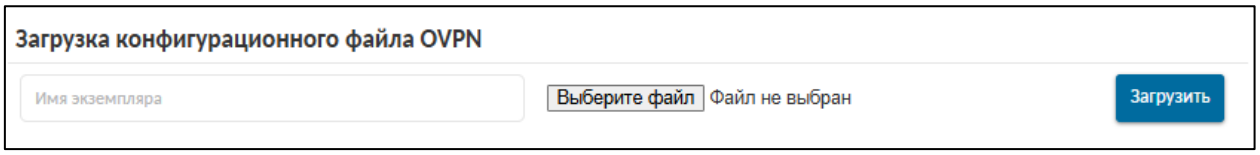


Рисунок 7-4: VPN. Загрузка конфигурационного файла OVPN

– «Имя экземпляра» — поле для ввода имени создаваемого экземпляра;
– «Выберите файл» — кнопка для выбора .ovpn-файла на локальном компьютере;
– «Загрузить» — кнопка для загрузки выбранного файла на устройство и создания экземпляра OpenVPN на его основе.

8 Статистика

Раздел «Статистика» главного меню Web-интерфейса позволяет просматривать графики системных параметров, собранные службой collectd и визуализированные с помощью RRDtool. Здесь отображается информация об использовании процессора, сетевых интерфейсов, загрузке системы, оперативной памяти и температуре устройства.

Внешний вид страницы показан на рисунках 8-1…8-8.

8.1 Графики

Страница «Графики» раздела «Статистика» (см. рисунок 8-1) предназначена для просмотра графиков статистики. В верхней части страницы расположены элементы управления для выбора хоста, временного интервала и частоты обновления.

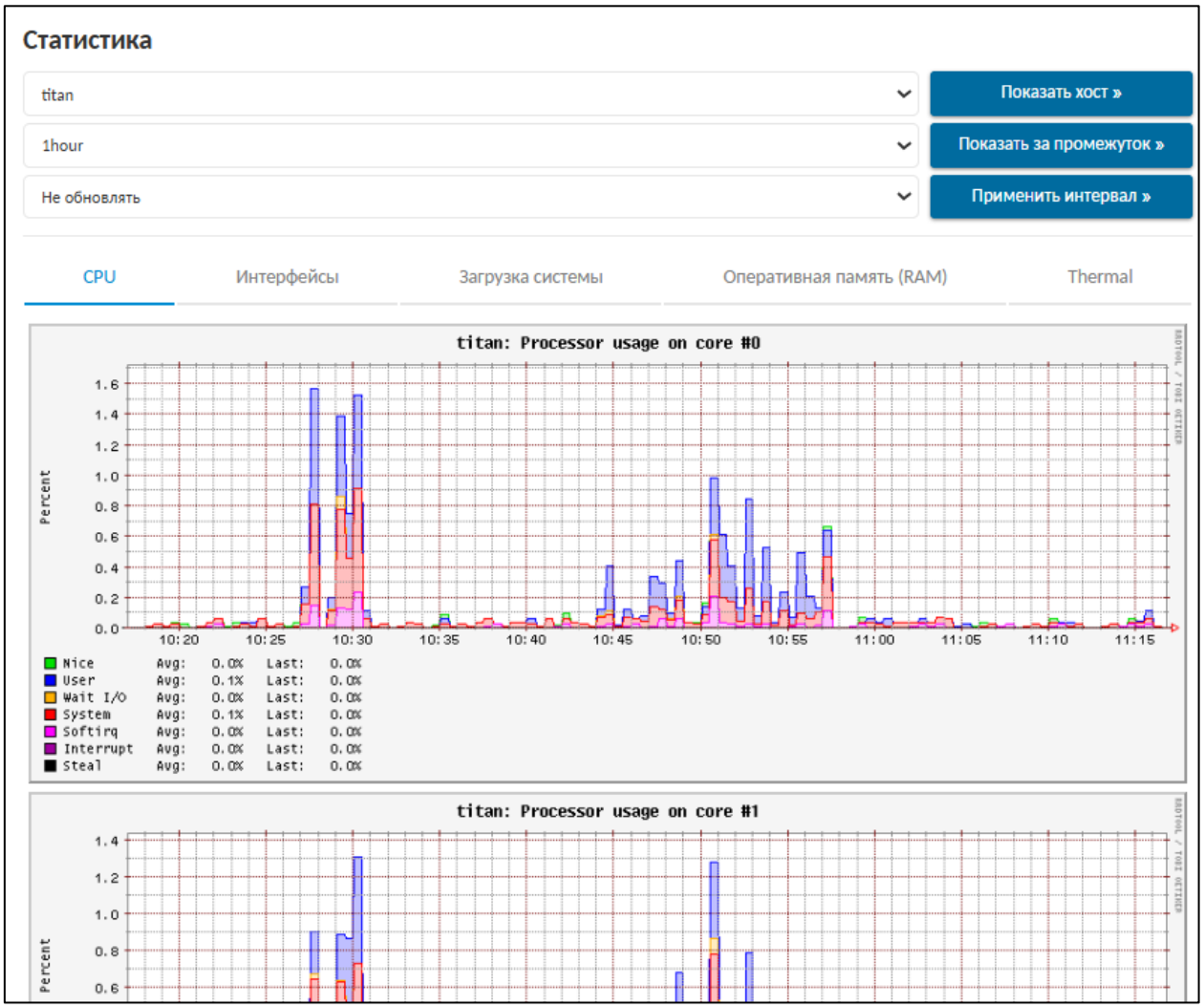


Рисунок 8-1: Статистика. Общий вид страницы графиков

8.1.1 Подраздел «Статистика»

В верхней части страницы (см. рисунок 8-2) расположены элементы управления.

Рисунок 8-2: Статистика. Элементы управления

– «Показать хост» — выпадающий список для выбора хоста, статистику которого необходимо отобразить;
– «Показать за промежуток» — выпадающий список для выбора временного интервала отображения графиков (см. рисунок 8-3);
– «Применить интервал» — кнопка для применения выбранного временного интервала;
– «Не обновлять» — выпадающий список для выбора частоты автоматического обновления графиков (см. рисунок 8-4);

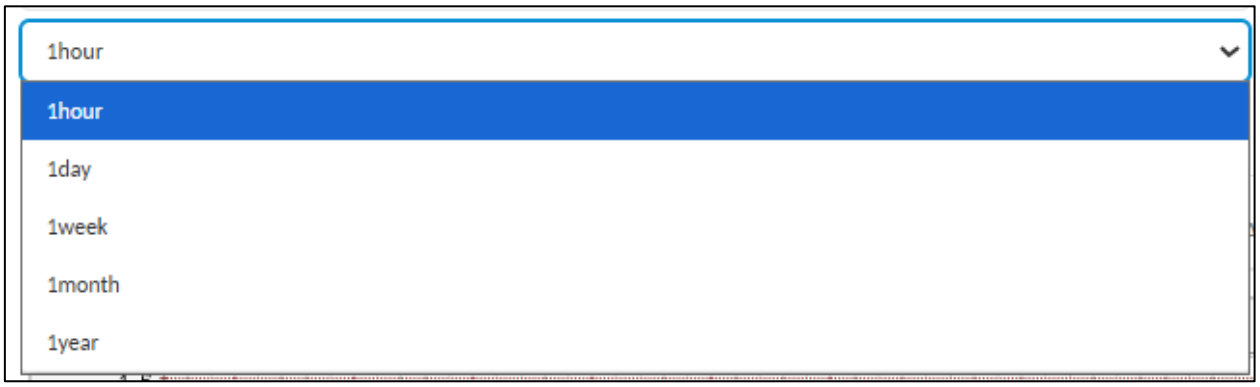


Рисунок 8-3: Статистика. Выпадающий список выбора временного интервала

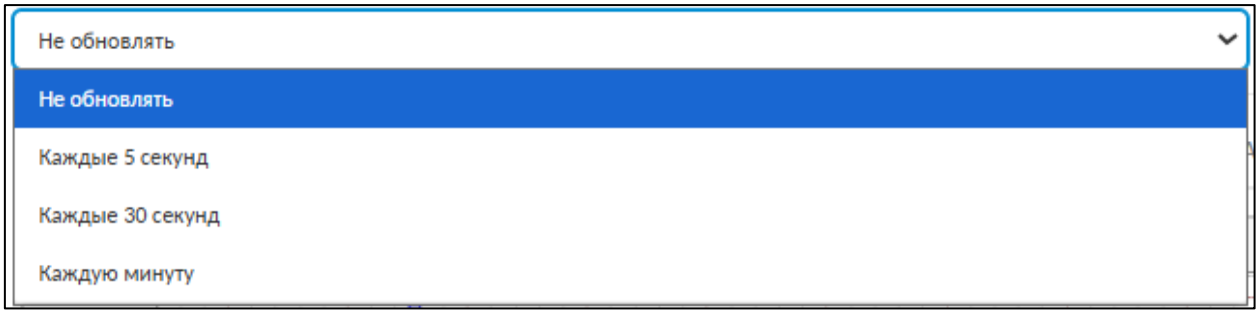


Рисунок 8-4: Статистика. Выпадающий список выбора частоты обновления

8.1.2 Подраздел «CPU»

В подразделе «CPU» (см. рисунок 8-5) отображается график использования процессора для каждого ядра. На графике показано распределение времени процессора по типам операций:

– Nice — время, затраченное на процессы с изменённым приоритетом;
– User — время выполнения пользовательских процессов;
– Wait I/O — время ожидания операций ввода-вывода;
– System — время выполнения системных вызовов;
– Softirq — время обработки программных прерываний;
– Interrupt — время обработки аппаратных прерываний;
– Steal — время, «украденное» гипервизором (для виртуальных машин).

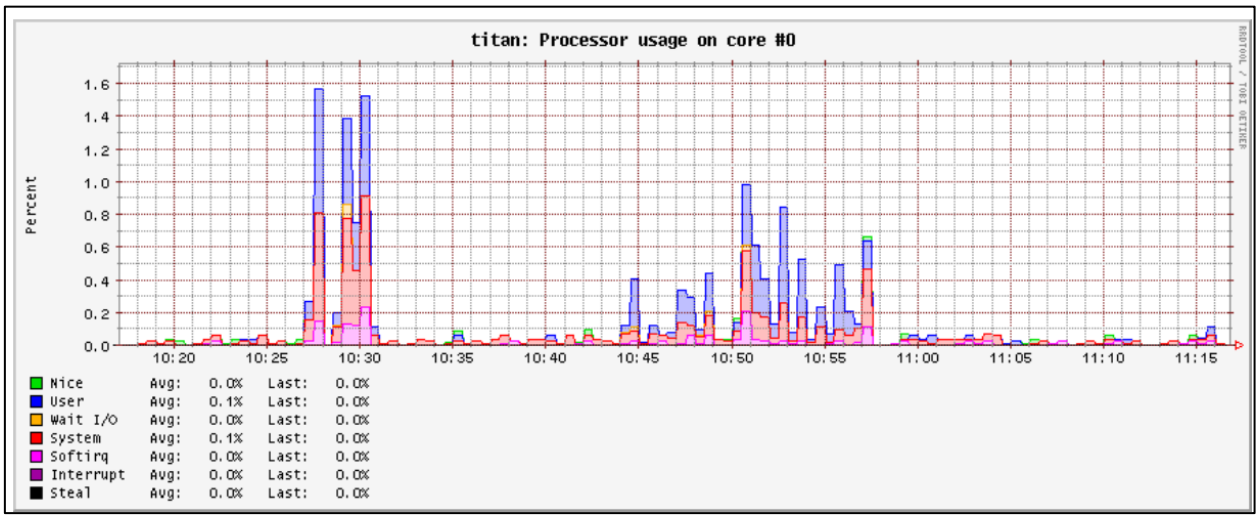


Рисунок 8-5: Статистика. График использования CPU (пример для core #0)

8.1.3 Подраздел «Интерфейсы»

В подразделе «Интерфейсы» (см. рисунок 8-6) отображаются графики сетевой активности для каждого физического интерфейса (eth0, eth1). Для каждого интерфейса строится два графика:

Верхний график — скорость передачи и приёма данных в байтах/с:

– TX — исходящий трафик;
– RX — входящий трафик.

Нижний график — количество пакетов в секунду и ошибки:

– Processed TX — исходящие пакеты;
– Processed RX — входящие пакеты;
– Errors TX — ошибки передачи;
– Errors RX — ошибки приёма.

Рисунок 8-6: Статистика. Графики сетевого интерфейса (пример для eth1)

8.1.4 Подраздел «Загрузка системы»

В подразделе «Загрузка системы» (см. рисунок 8-7) отображается график средней загрузки системы за различные промежутки времени:

– Средняя загрузка за 1 минуту;
– Средняя загрузка за 5 минут;
– Средняя загрузка за 15 минут.

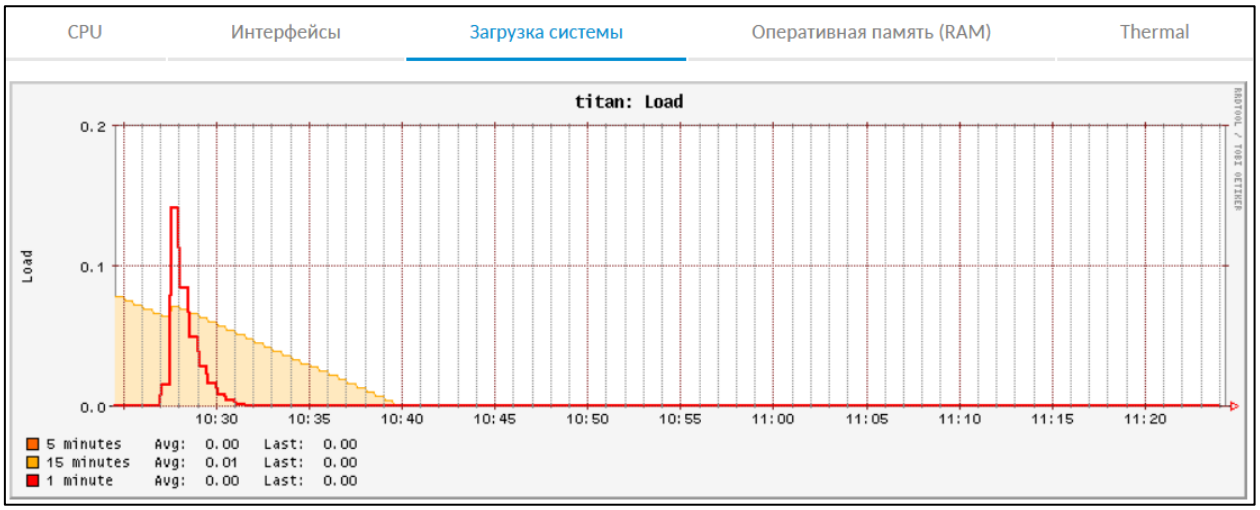


Рисунок 8-7: Статистика. График загрузки системы

8.1.5 Подраздел «Оперативная память (RAM)»

В подразделе «Оперативная память (RAM)» (см. рисунок 8-8) отображается график использования оперативной памяти с разбивкой по типам:

– Free — свободная память;

– Buffered — память, используемая для буферов;

– Cached — кэшированная память;

– Used — используемая память.

Для каждого типа отображается среднее (Avg) и последнее (Last) значения.

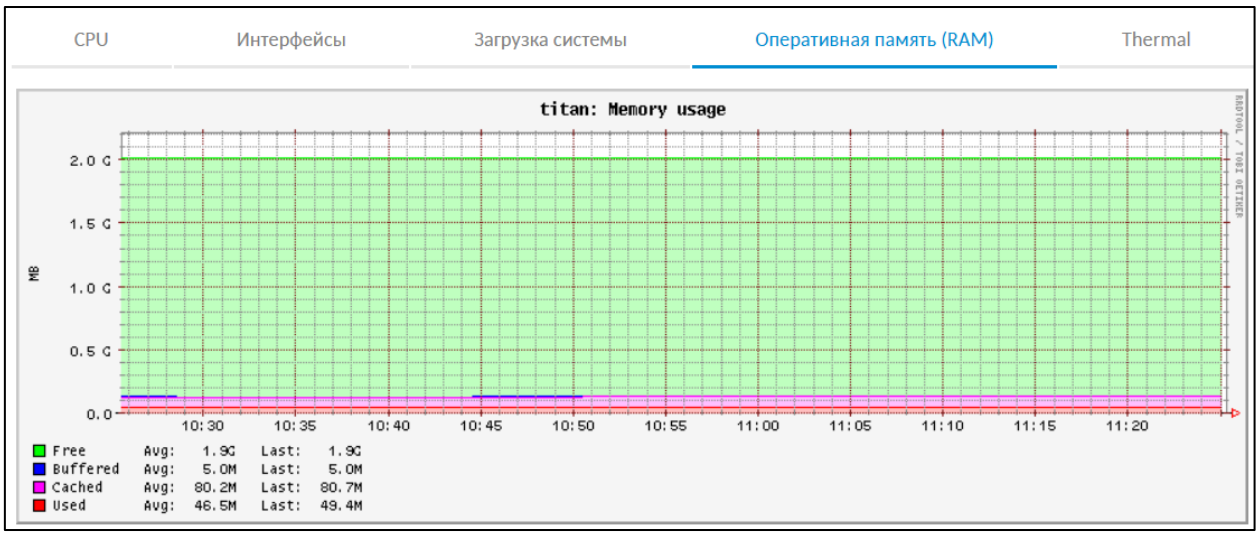


Рисунок 8-8: Статистика. График использования оперативной памяти

8.1.6 Подраздел «Thermal»

В подразделе «Thermal» (см. рисунок 8-9) отображаются графики температуры устройства для каждого температурного датчика (thermal_zone0, thermal_zone1 и др.). График показывает изменение температуры в градусах Цельсия с течением времени.

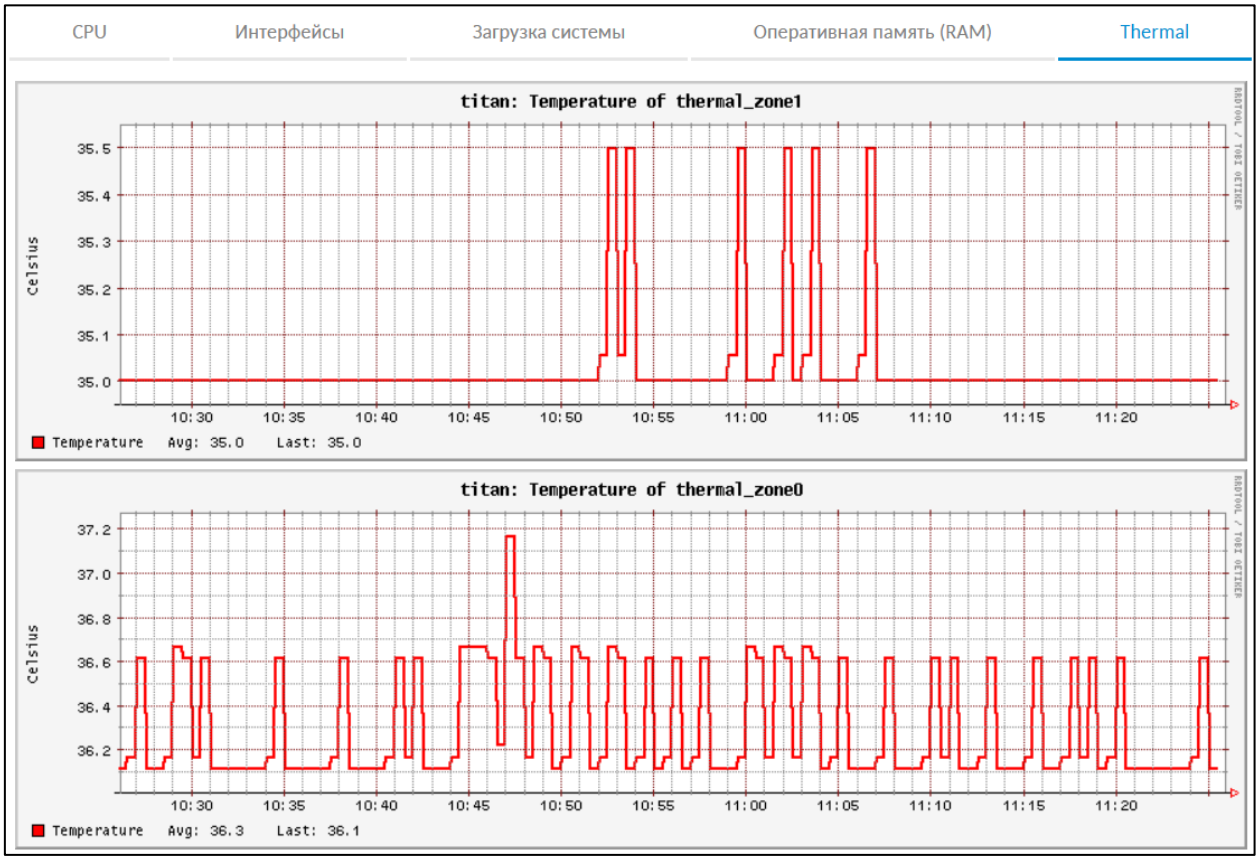


Рисунок 8-9: Статистика. Графики температуры (thermal_zone0 и thermal_zone1)

8.2 Настройка статистики (collectd)

Страница «Настройки collectd» раздела «Статистика» позволяет сконфигурировать службу сбора статистики, а также включить/настроить необходимые плагины.

8.2.1 Настройки collectd

На вкладке «Настройки collectd» (см. рисунок 8-10) задаются общие параметры службы сбора статистики.

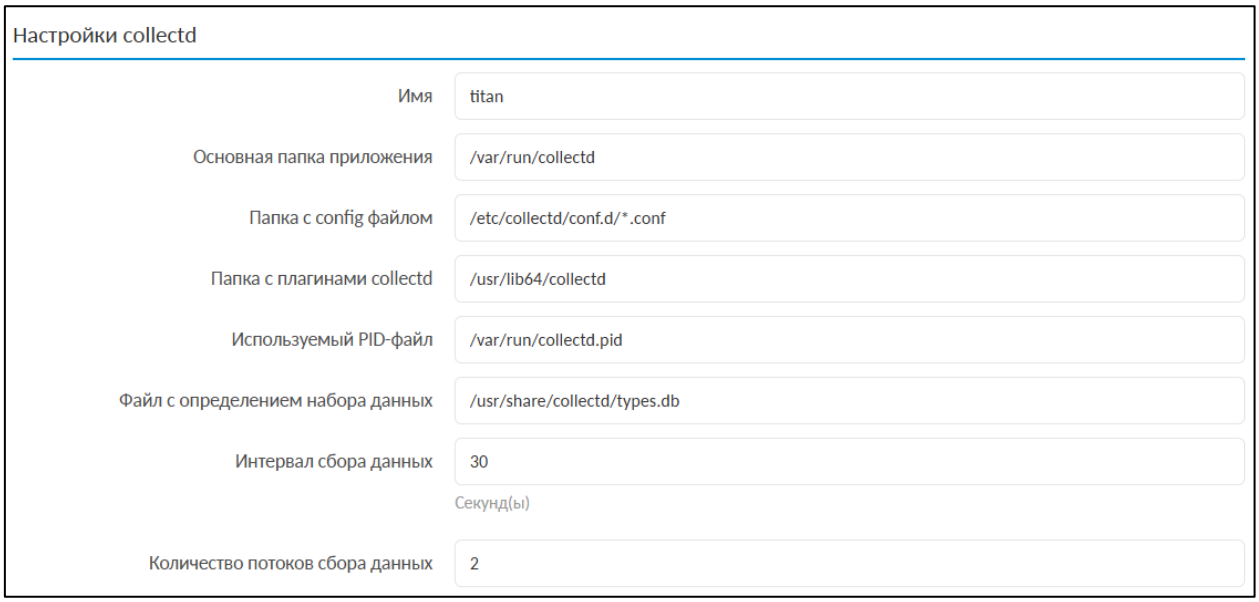


Рисунок 8-10: Настройки collectd. Общие параметры

- «Имя» — имя хоста, под которым статистика будет сохраняться;
- «Основная папка приложения» — путь к рабочей папке службы collectd;
- «Папка с config файлом» — путь к папке с конфигурационными файлами плагинов;
- «Папка с плагинами collectd» — путь к папке с установленными плагинами;
- «Используемый PID-файл» — путь к PID-файлу службы;
- «Файл с определением набора данных» — путь к файлу с описанием типов данных;
- «Интервал сбора данных» — интервал сбора данных в секундах;
- «Количество потоков сбора данных» — количество одновременно работающих потоков сбора данных.

8.2.2 Основные плагины

На вкладке «Основные плагины» (см. рисунок 8-11) отображается список плагинов для сбора системной статистики.

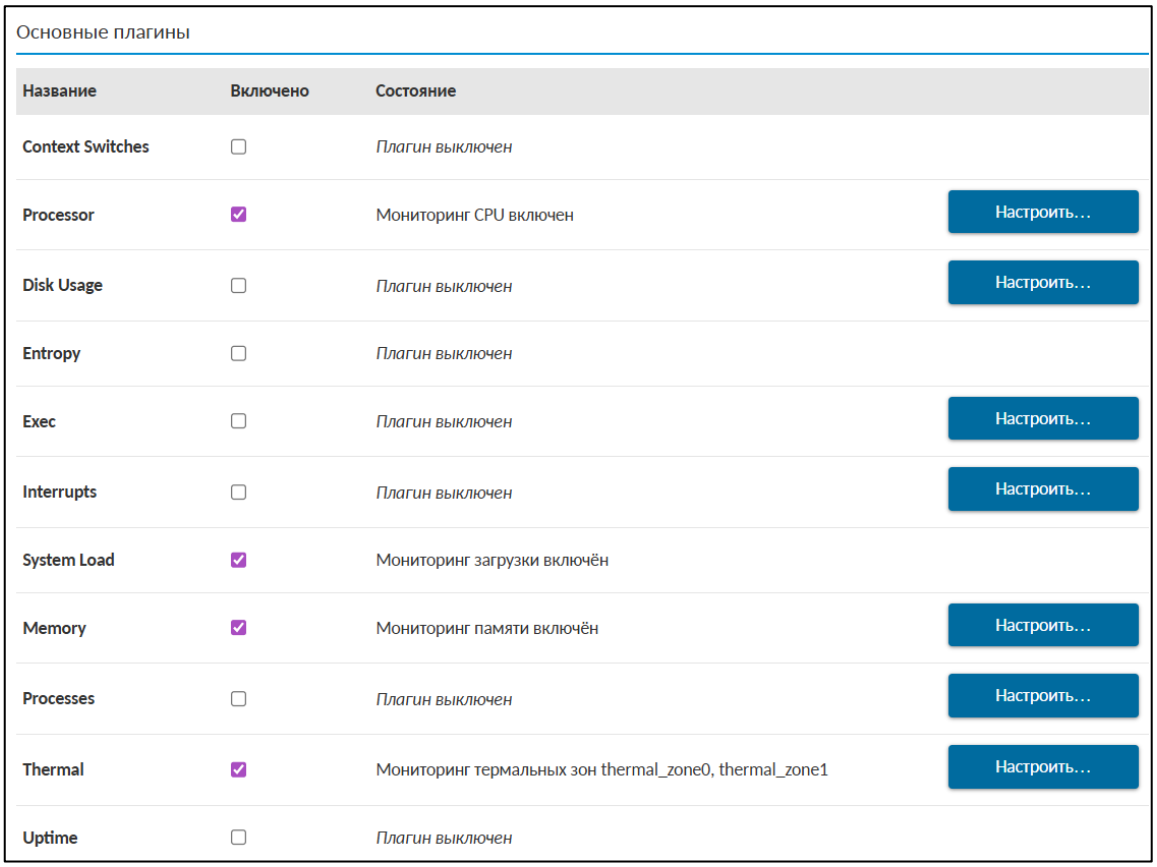


Рисунок 8-11: Настройки collectd. Основные плагины

Для каждого плагина доступна кнопка «Настроить...» (если плагин поддерживает дополнительные параметры).

8.2.2.1 Настройка плагина «CPU»

Страница настройки плагина «CPU» (см. рисунок 8-12) позволяет сконфигурировать параметры сбора статистики об использовании процессора.

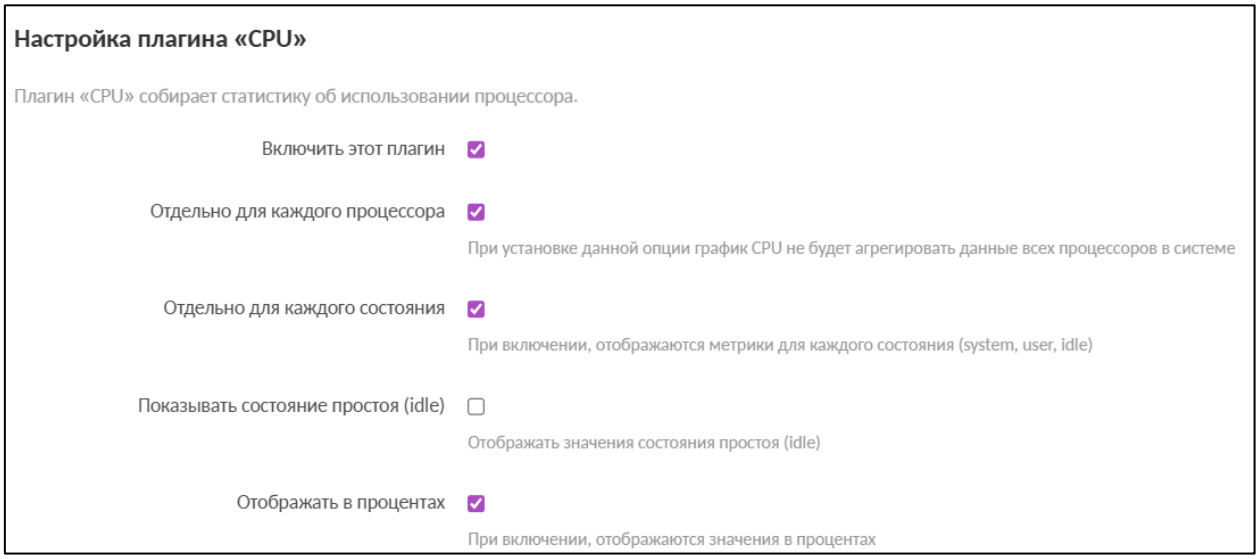


Рисунок 8-12: Настройка плагина «CPU»

– «Включить этот плагин» — флаг, включающий сбор статистики использования процессора;
– «Отдельно для каждого процессора» — при включении данной опции график CPU будет отображать данные отдельно для каждого ядра процессора, а не агрегированные данные по всем ядрам;
– «Отдельно для каждого состояния» — при включении отображаются метрики для каждого состояния процессора;
– «Показывать состояние простоя (idle)» — отображать значения состояния простоя (idle);
– «Отображать в процентах» — при включении значения отображаются в процентах.

8.2.2.2 Настройка плагина «Disk»

Страница настройки плагина «Disk» (см. рисунок 8-13) позволяет сконфигурировать параметры сбора статистики использования дисков и разделов.

Рисунок 8-13: Настройка плагина «Disk»

– «Включить этот плагин» — флаг, включающий сбор статистики использования дисков и разделов;
– «Мониторить диски и разделы» — список дисков и разделов, для которых будет собираться статистика. Можно выбрать из выпадающего списка или ввести вручную;

– «Собирать статистику со всех кроме указанных» — при включении данной опции сбор статистики будет производиться для всех дисков и разделов, кроме указанных в списке.

8.2.2.3 Настройка плагина «Exec»

Страница настройки плагина «Exec» (см. рисунок 8-14) позволяет сконфигурировать выполнение внешних команд при достижении определённых значений порогов. Плагин «Exec» выполняет внешнюю команду в случае, когда определённые значения достигают заданного порога.

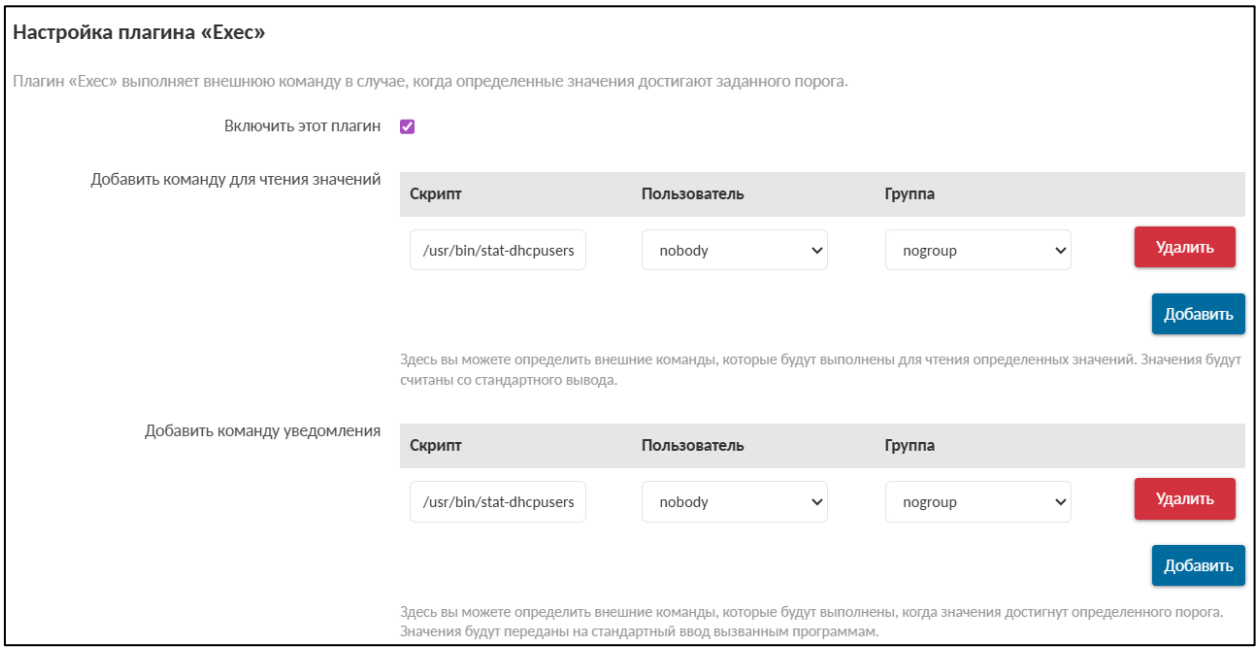


Рисунок 8-14: Настройка плагина «Exec»

В подразделе «Добавить команду для чтения значений» определяются внешние команды, которые будут выполнены для чтения определённых значений. Значения будут считаны со стандартного вывода.

Таблица команд для чтения значений имеет следующие столбцы:

– «Скрипт» — путь к исполняемому скрипту или команде.
– «Пользователь» — имя пользователя, от имени которого будет выполнена команда.
– «Группа» — имя группы, от имени которой будет выполнена команда.

В подразделе «Добавить команду уведомления» определяются внешние команды, которые будут выполнены, когда значения достигнут определённого

порога. Значения будут переданы на стандартный ввод вызванным программам.

Таблица команд уведомления имеет следующие столбцы:

- «Скрипт» — путь к исполняемому скрипту или команде.
- «Пользователь» — имя пользователя, от имени которого будет выполнена команда.
- «Группа» — имя группы, от имени которой будет выполнена команда.

8.2.2.4 Настройка плагина «IRQ» (Прерывания)

Страница настройки плагина «IRQ» (см. рисунок 8-15) позволяет сконфигурировать параметры сбора статистики по аппаратным прерываниям.

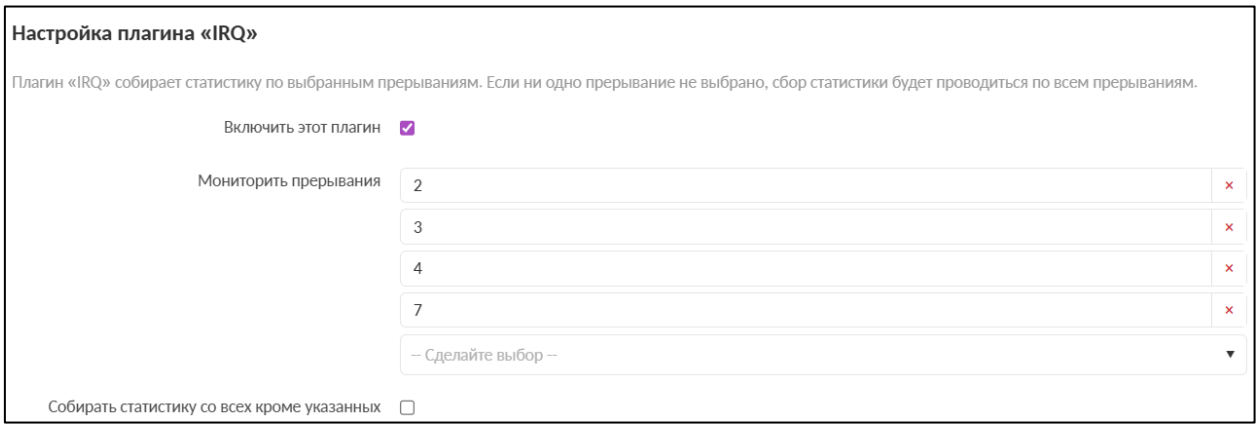


Рисунок 8-15: Настройка плагина «IRQ» (Прерывания)

Плагин «IRQ» собирает статистику по выбранным прерываниям. Если ни одно прерывание не выбрано, сбор статистики будет проводиться по всем прерываниям.

- «Включить этот плагин» — флаг, включающий сбор статистики по прерываниям.
- «Мониторить прерывания» — список номеров прерываний, для которых будет собираться статистика. Выбор осуществляется из выпадающего списка или вводом вручную. Если ни одно прерывание не указано, сбор статистики будет проводиться по всем прерываниям.

– «Собирать статистику со всех кроме указанных» — при включении данной опции сбор статистики будет производиться для всех прерываний, кроме указанных в списке.

8.2.2.5 Настройка плагина «Оперативная память (RAM)»

Страница настройки плагина «Оперативная память (RAM)» (см. рисунок 8-16) позволяет сконфигурировать параметры сбора статистики об использовании оперативной памяти.

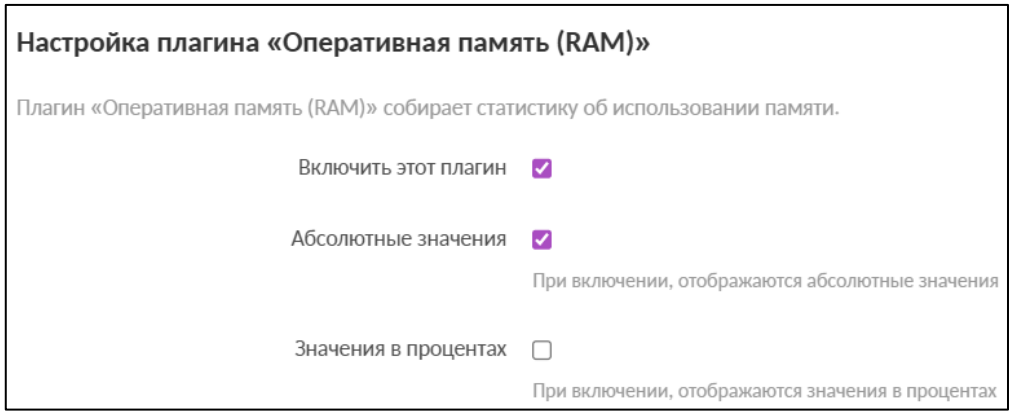


Рисунок 8-16: Настройка плагина «Оперативная память (RAM)»

– «Включить этот плагин» — флаг, включающий сбор статистики об использовании оперативной памяти;
– «Абсолютные значения» — при включении данной опции отображаются абсолютные значения использования памяти (в байтах, килобайтах и т.д.);
– «Значения в процентах» — при включении данной опции отображаются значения использования памяти в процентах от общего объёма.

8.2.2.6 Настройка плагина «Процессы»

Страница настройки плагина «Процессы» (см. рисунок 8-17) позволяет сконфигурировать параметры сбора статистики по выбранным процессам.

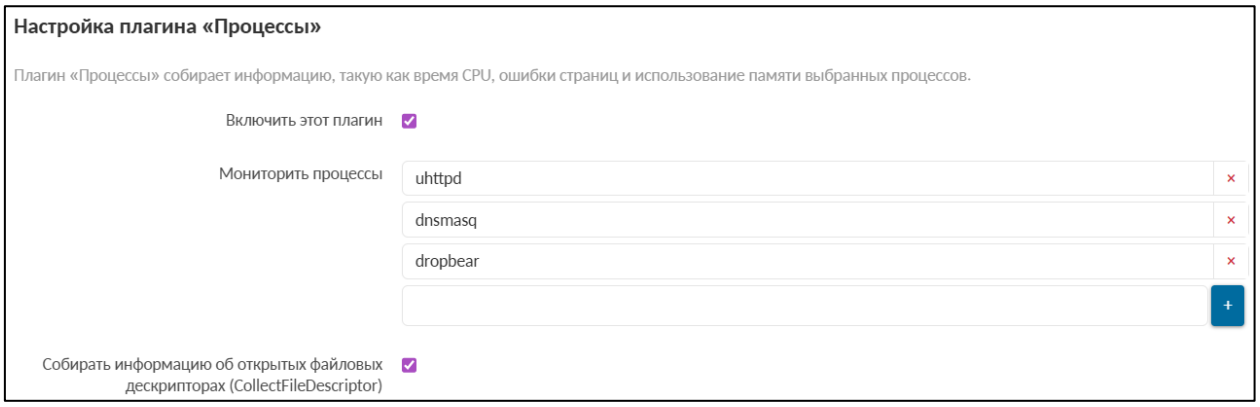


Рисунок 8-17: Настройка плагина «Процессы»

– «Включить этот плагин» — флаг, включающий сбор статистики по процессам;
– «Мониторить процессы» — список процессов, для которых будет собираться статистика. Выбор осуществляется из выпадающего списка. Можно выбрать несколько процессов;
– «Собирать информацию об открытых файловых дескрипторах (CollectFileDescriptor)» — при включении данной опции будет собираться информация о количестве открытых файловых дескрипторов для каждого отслеживаемого процесса;

8.2.2.7 Настройка плагина «Thermal»

Страница настройки плагина «Thermal» (см. рисунок 8-18) позволяет сконфигурировать параметры сбора статистики с температурных датчиков устройства.

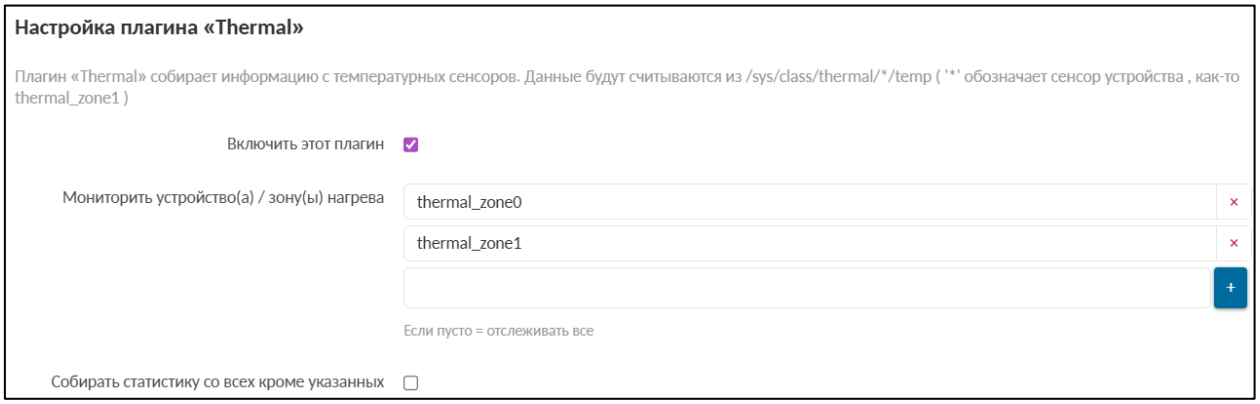


Рисунок 8-18: Настройка плагина «Thermal»

– «Включить этот плагин» — флаг, включающий сбор статистики температуры;
– «Мониторить устройство(а) / зону(ы) нагрева» — список термальных зон, для которых будет собираться статистика. Выбор осуществляется из выпадающего списка. Если поле пусто, отслеживаются все доступные термальные зоны;
– «Собирать статистику со всех кроме указанных» — при включении данной опции сбор статистики будет производиться для всех термальных зон, кроме указанных в списке.

8.2.3 Сетевые плагины

На вкладке «Сетевые плагины» (см. рисунок 8-19) отображается список плагинов для сбора сетевой статистики.

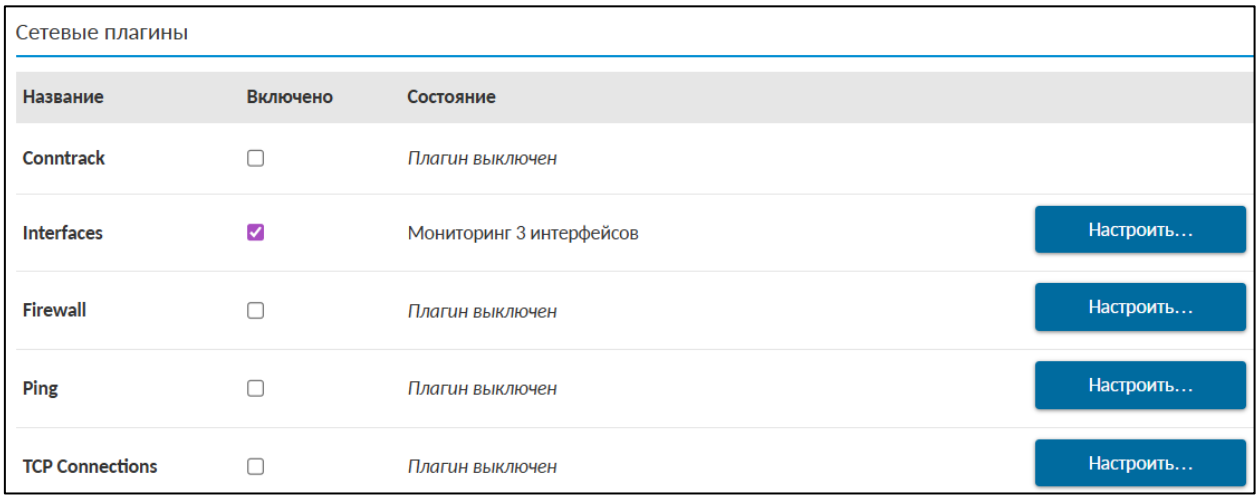


Рисунок 8-19: Настройки collectd. Сетевые плагины

Для каждого плагина доступна кнопка «Настроить...».

8.2.3.1 Настройка плагина «Интерфейсы»

Страница настройки плагина «Интерфейсы» (см. рисунок 8-20) позволяет указать, за какими сетевыми интерфейсами следует собирать статистику.

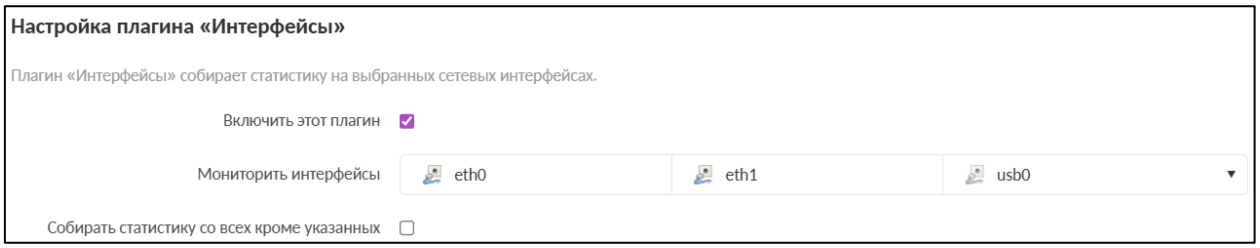


Рисунок 8-20: Настройка плагина «Интерфейсы»

– «Включить этот плагин» — флаг, включающий сбор статистики сетевых интерфейсов;
– «Мониторить интерфейсы» — список интерфейсов для мониторинга. Выбор осуществляется из выпадающего списка или вводом вручную.
– «Собирать статистику со всех кроме указанных» — при включении данной опции сбор статистики будет производиться для всех интерфейсов, кроме указанных в списке.

8.2.3.2 Настройка плагина «Firewall»

Страница настройки плагина «Firewall» (см. рисунок 8-21) позволяет собирать статистику с определённых правил межсетевого экрана.

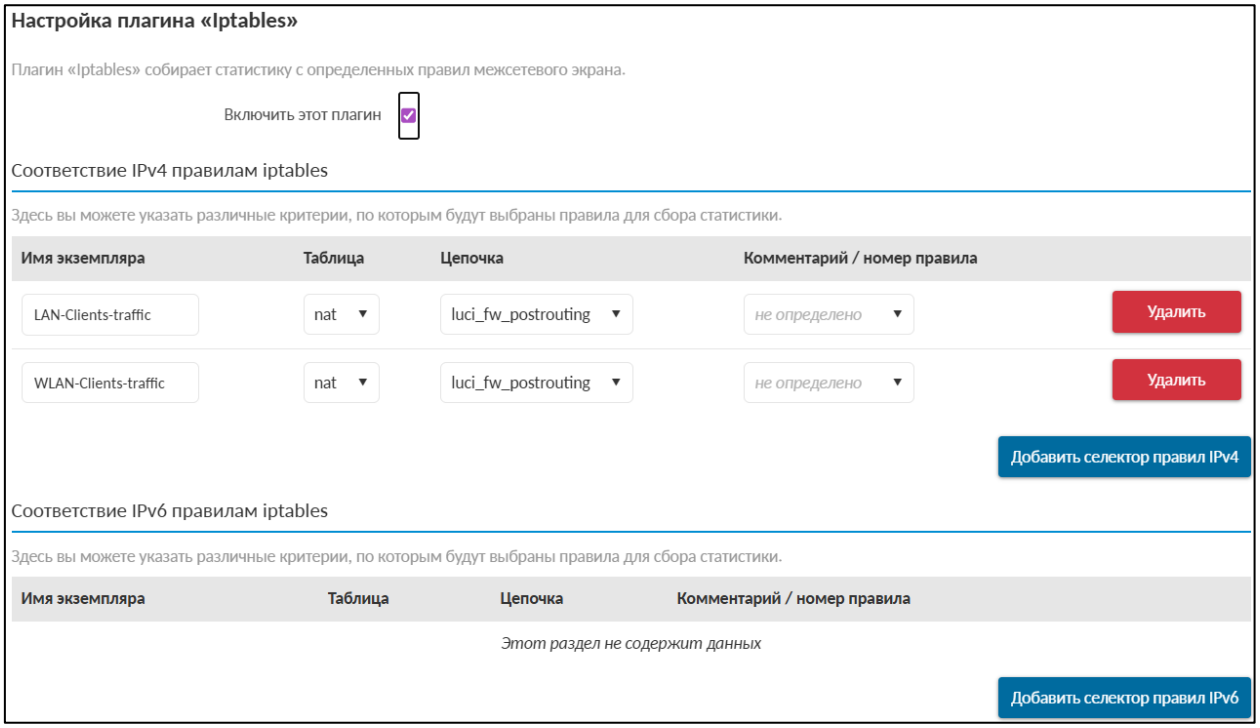


Рисунок 8-21: Настройка плагина «Firewall»

– «Включить этот плагин» — флаг, включающий сбор статистики с правил Firewall.

В подразделе «Соответствие IPv4 правилам iptables» задаются критерии для выбора правил IPv4, с которых будет собираться статистика. Таблица селекторов правил IPv4 имеет следующие столбцы:

– «Имя экземпляра» — пользовательское имя для данного селектора;
– «Таблица» — таблица iptables (filter, nat, mangle, raw);
– «Цепочка» — цепочка правил (например, luci_fw_postrouting);
– «Комментарий / номер правила» — комментарий или номер правила для выборки. Значение «не определено» означает все правила цепочки.
– «Добавить селектор правил IPv4» — добавление нового селектора для IPv4.

В подразделе «Соответствие IPv6 правилам iptables» задаются критерии для выбора правил IPv6, с которых будет собираться статистика. Таблица имеет те же столбцы, что и для IPv4.

8.2.3.3 Настройка плагина «Пинг-запрос»

Страница настройки плагина «Пинг-запрос» (см. рисунок 8-22) позволяет сконфигурировать отправку ICMP-запросов выбранным хостам и измерение времени отклика.

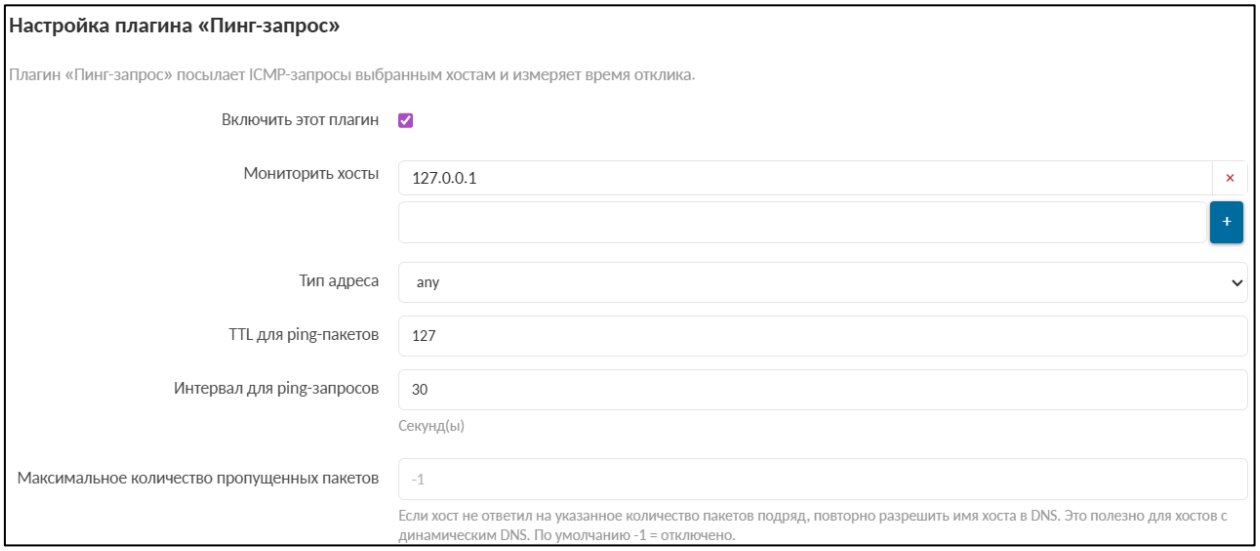


Рисунок 8-22: Настройка плагина «Пинг-запрос»

– «Включить этот плагин» — флаг, включающий отправку ICMP-запросов;
– «Мониторить хосты» — список хостов (IP-адресов или доменных имён) для пингования;
– «Тип адреса» — выбор типа адреса;
– «TTL для ping-пакетов» — значение TTL (Time To Live) для ICMP-пакетов;
– «Интервал для ping-запросов» — интервал между отправками ICMP-запросов в секундах;
– «Максимальное количество пропущенных пакетов» — если хост не ответил на указанное количество пакетов подряд, выполняется повторное разрешение имени хоста в DNS.

8.2.3.4 Настройка плагина «TCPConns»

Страница настройки плагина «TCPConns» (см. рисунок 8-23) позволяет собирать информацию об открытых TCP-соединениях на выбранных портах.

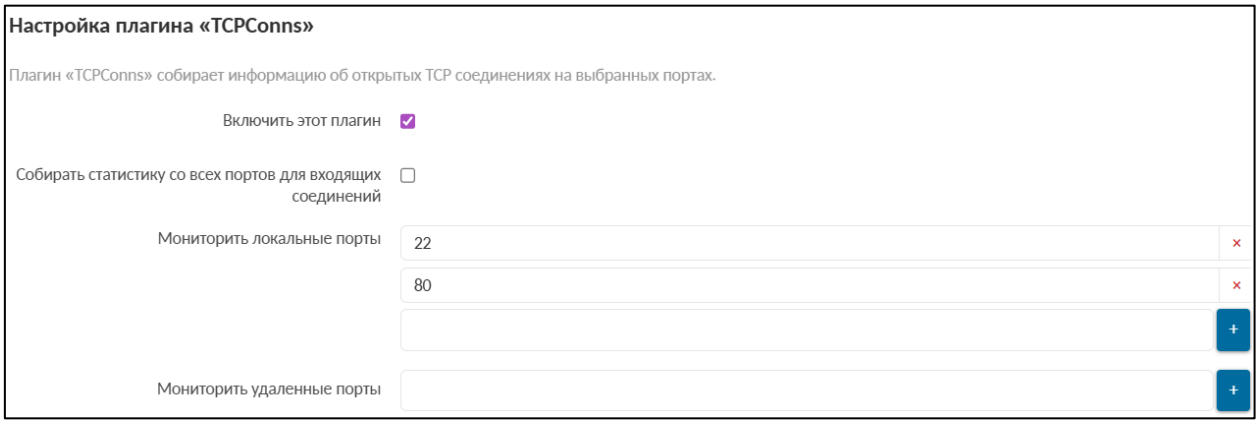


Рисунок 8-23: Настройка плагина «TCPConns»

– «Включить этот плагин» — флаг, включающий сбор информации о TCP-соединениях;
– «Собирать статистику со всех портов для входящих соединений» — при включении данной опции статистика будет собираться со всех портов для входящих подключений;

– «Мониторить локальные порты» — список локальных портов (на устройстве), для которых будет собираться статистика;
– «Мониторить удаленные порты» — список удалённых портов (на внешних хостах), для которых будет собираться статистика.

8.2.4 Плагины вывода

На вкладке «Плагины вывода» (см. рисунок 8-24) отображается список плагинов, определяющих, куда и как сохранять собранную статистику.

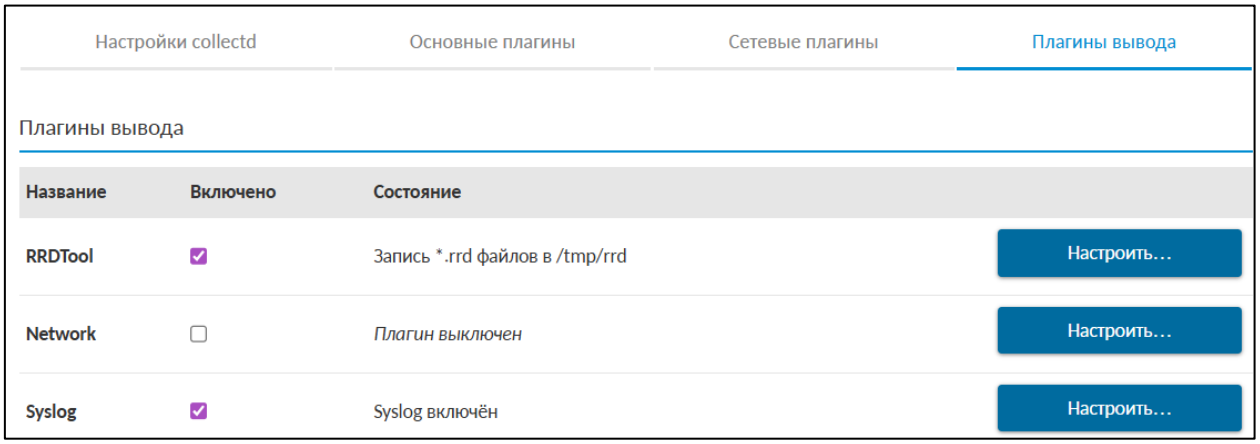


Рисунок 8-24: Настройки collectd. Плагины вывода

Для каждого плагина доступна кнопка «Настроить...».

8.2.4.1 Настройка плагина «RRDTool»

Страница настройки плагина «RRDTool» (см. рисунок 8-25а и 8-25б) позволяет сконфигурировать параметры сохранения статистики в RRD-файлы.

– «Включить этот плагин» — флаг, включающий сохранение данных в RRD;
– «Папка с данными» — путь к папке, где будут храниться .rrd файлы;
– «Базовый интервал между данными в RRD (StepSize)» — базовый интервал между точками данных в секундах;
– «Максимальное количество секунд между двумя обновлениями (HeartBeat)» — максимальное время между обновлениями данных в секундах;

– «Создавать только средние RRAs» — при включении позволяет уменьшить размер RRD-файлов (сохраняются только средние значения).

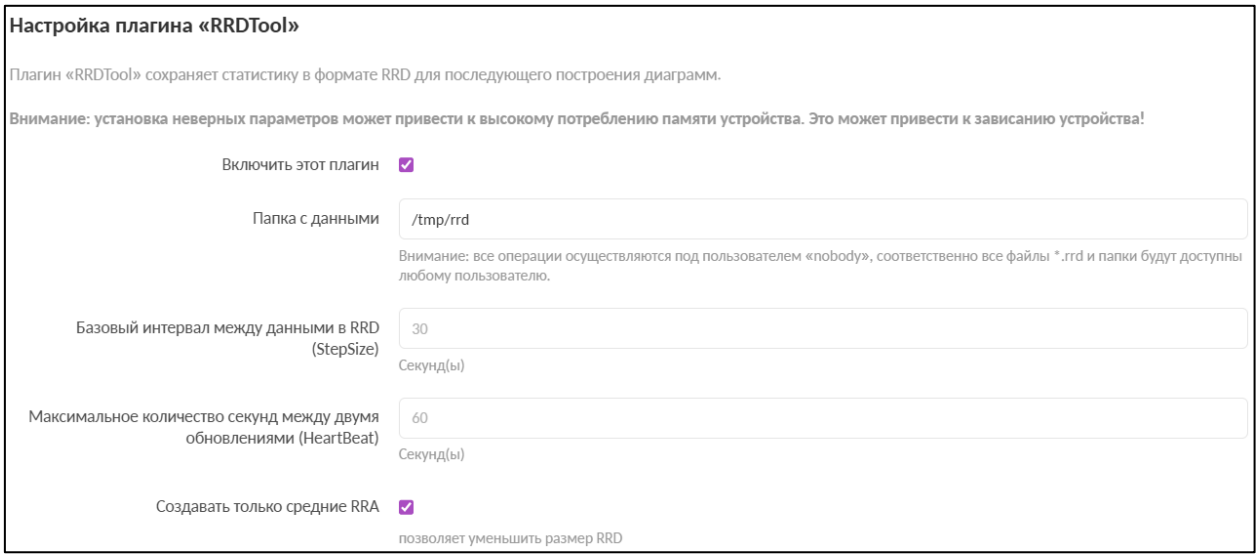


Рисунок 8-25а: Настройка плагина «RRDTool». Основные параметры

– «Сохраняемые промежутки времени» — список временных интервалов для хранения в базе данных RRD;
– «Количество «поколений» данных в архиве RRA» — количество сохраняемых точек данных;
– «Часть интервала консолидации, которая может состоять из неопределенных значений (UNKNOWN)» — доля допустимых неизвестных значений;
– «Кэшировать собранную статистику в течении» — время кэширования статистики в секундах;
– «Сбросить кэш после» — время сброса кэша в секундах.

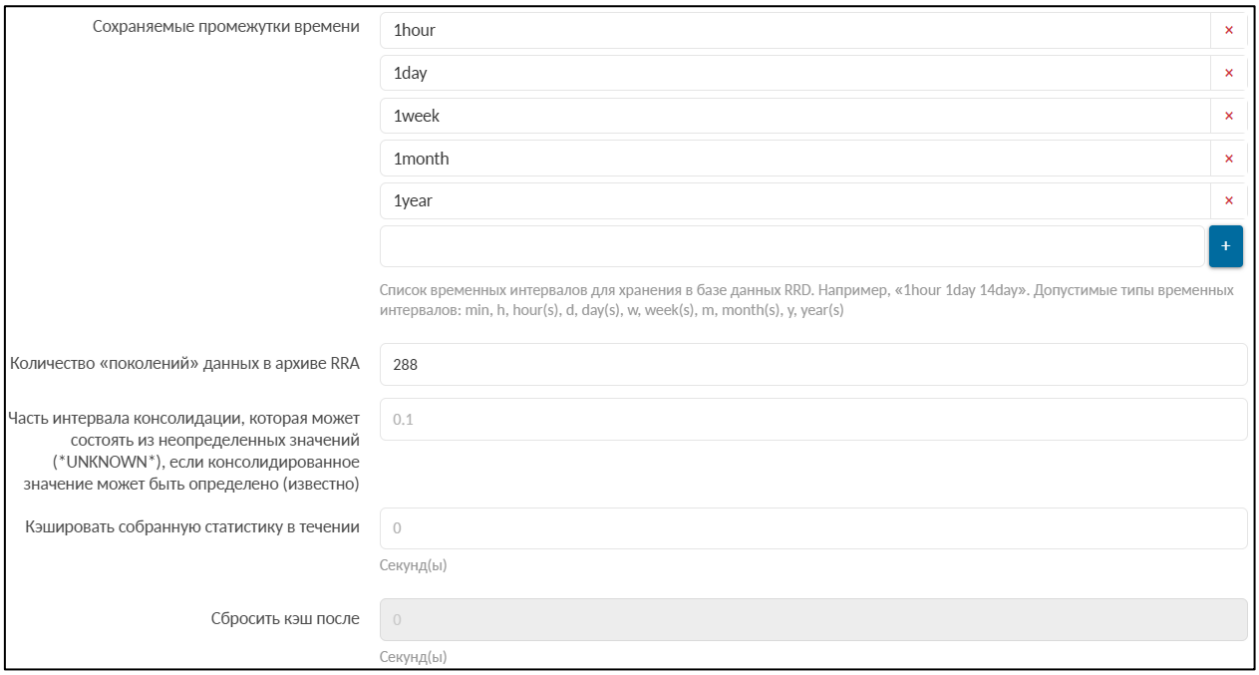


Рисунок 8-25б: Настройка плагина «RRDTool». Параметры хранения

8.2.4.1 Настройка плагина «Network»

Страница настройки плагина «Network» (при наличии, см. рисунок 8-26) позволяет отправлять статистику по сети на удалённый сервер collectd.

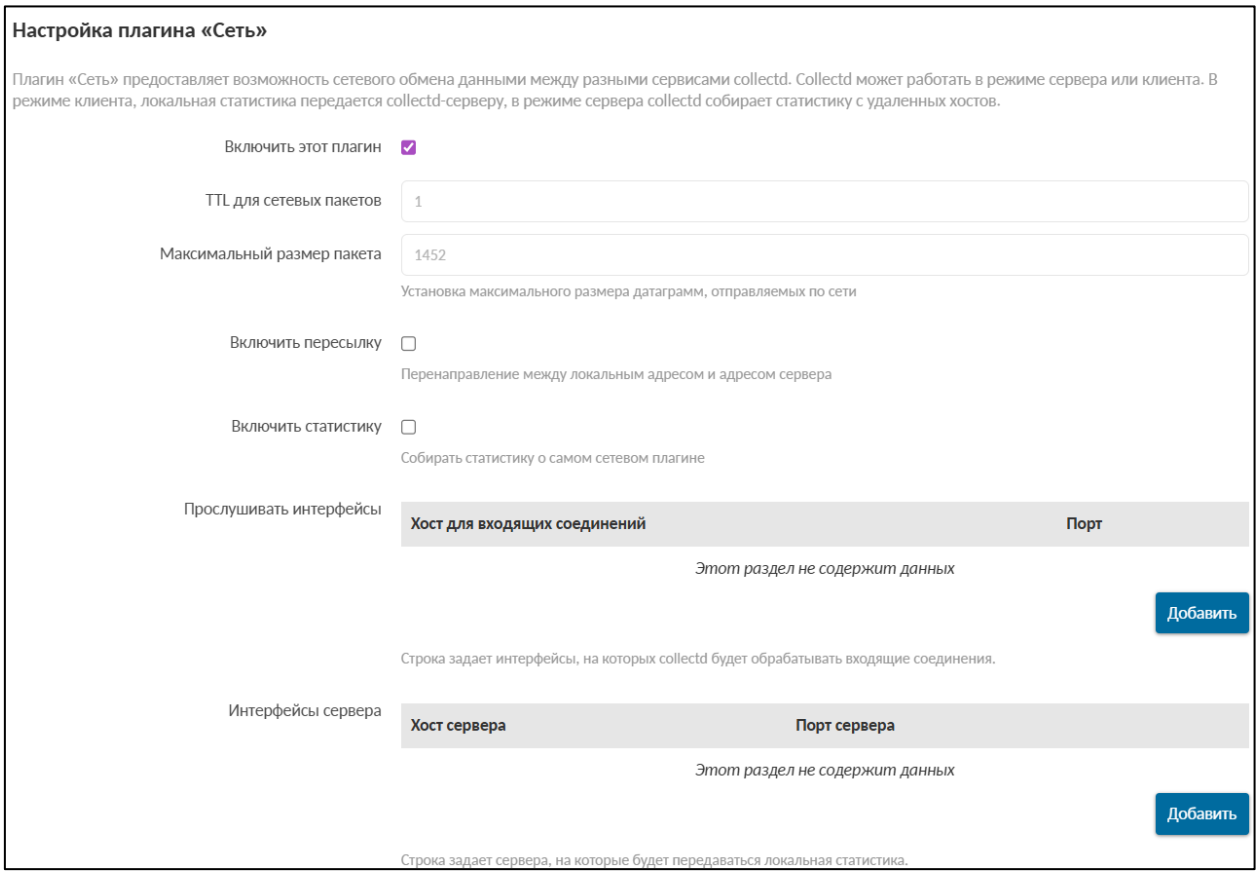


Рисунок 8-26: Настройка плагина «Network»

– «Включить этот плагин» — флаг, включающий сетевой обмен данными;
– «TTL для сетевых пакетов» — значение Time To Live для отправляемых сетевых пакетов;
– «Максимальный размер пакета» — максимальный размер датаграмм, отправляемых по сети (в байтах);
– «Включить пересылку» — при включении данной опции включается перенаправление между локальным адресом и адресом сервера;
– «Включить статистику» — при включении собирается статистика о работе самого сетевого плагина.

Прослушивать интерфейсы (режим сервера)

В подразделе «Прослушивать интерфейсы» задаются интерфейсы, на которых collectd будет обрабатывать входящие соединения (режим сервера).

Таблица содержит следующие столбцы:

– «Хост для входящих соединений» — IP-адрес или имя хоста, на котором принимаются входящие соединения;
– «Порт» — порт для приёма входящих соединений.

Интерфейсы сервера (режим клиента)

В подразделе «Интерфейсы сервера» задаются серверы, на которые будет передаваться локальная статистика (режим клиента).

Таблица содержит следующие столбцы:

– «Хост сервера» — IP-адрес или имя хоста удалённого collectd-сервера.
– «Порт сервера» — порт удалённого collectd-сервера.

8.2.4.2 Настройка плагина «Syslog»

Страница настройки плагина «Syslog» (см. рисунок 8-27) позволяет сконфигурировать отправку сообщений collectd в системный журнал.

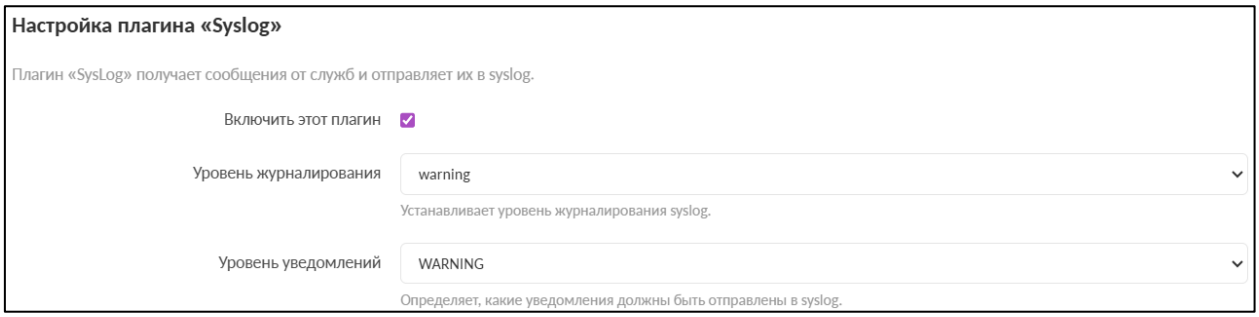


Рисунок 8-27: Настройка плагина «Syslog»

- «Включить этот плагин» — флаг, включающий отправку сообщений в syslog;
- «Уровень журналирования» — уровень детализации журналирования;
- «Уровень уведомлений» — определяет, какие уведомления должны быть отправлены в syslog.