Краткое описание основных функций Web-интерфейса управления контроллеров

Руководство пользователя

Редакция 2.2.0

OpenWrt
Wireless Freedom

Код документа: TN-UG-OWRT-LUCI-R2
Дата сборки: 5 мая 2020 г.
Страниц в документе: 164

http://owen.ru

Документ выполнен в системе разработки документации TanoDoc 0.9.1-25

Содержание

Список иллюстраций

Перечень сокращений и условных обозначений

ARP	Address Resolution Protocol	34
ASCII	American Standard Code for Information Interchange	62, 102
BPDU	Bridge Protocol Data Unit	90, 92, 95, 96
CA	Certification Authority	82, 160
CPU	Central Processing Unit	9, 145
CSV	Comma-Separated Values	77
DDNS	Dynamic DNS	3, 5, 7, 8, 10, 13, 79–87, 158–162
DHCP	Dynamic Host Configuration Protocol	4, 8, 9, 13, 20–22, 32, 107, 108, 110–113, 118, 119, 121, 123, 124
DNS	Domain Name System	3, 4, 11, 13, 22, 79, 85, 110, 113, 114, 118, 119, 121, 139, 140, 162
F2FS	Flash-Friendly File System	50
FAT	File Allocation Table	11, 12
FAT32	File Allocation Table 32	53
FIFO	First In First Out	47
FQDN	Fully Qualified Domain Name	142
FTP	File Transfer Protocol	2, 3, 5, 6, 9, 13, 15, 25–27, 99–103, 155–157
HTTP	HyperText Transfer Protocol	13, 14, 26, 27, 67, 97, 98
HTTPS	HyperText Transfer Protocol Secure	14, 26, 27, 67, 68, 82, 83, 97, 98, 160
ICMP	Internet Control Message Protocol	9, 132, 136, 149
ID	IDentifier	80
IGMP	Internet Group Management Protocol	108
IP	Internet Protocol	8, 10, 20–22, 34, 40, 59, 79, 80, 82–85, 97, 100, 110, 113–115, 119, 121, 123, 125, 128, 133, 136, 137, 139, 151, 155, 160–162
IPv4	Internet Protocol version 4	21, 22, 32, 34, 84, 105, 110, 113, 126, 128, 136, 139, 140, 158
IPv6	Internet Protocol version 6	9, 34, 84, 85, 105, 107, 110, 111, 113, 126, 128, 136, 139, 140
LAN	Local Area Network	20–22, 151, 155
MAC	Media Access Control	31, 32, 34, 90, 105, 110, 111, 133, 136
MMC	MultiMedia Card	51
MSS	Maximum Segment Size	128
MTU	Maximum Transmission Unit	110, 111
NAT	Network Address Translation	115, 133
NDP	Neighbor Discovery Protocol	113
NTFS	New Technology File System	53
NTP	Network Time Protocol	13, 15, 18, 19, 42
OPC	Open Platform Communications	11
OPC UA	OPC Unified Architecture	27
PID	Process IDentifier	142
PPP	Point-to-Point Protocol	31
RA	Router Advertisement	113

RNDIS	Remote Network Driver Interface Specification	24, 31, 73
RSS	Resident Set Size	9, 145, 146
RSTP	Rapid Spanning Tree Protocol	8, 13, 22, 88–91, 93–95, 108
SFTP	SSH File Transfer Protocol	43
SSH	Secure SHell	2, 5, 6, 9, 12, 13, 15, 24–27, 43–45, 151, 152
SSL	Secure Sockets Layer	3, 7, 60, 62, 63, 68–70, 164
STP	Spanning Tree Protocol	8, 13, 22, 88–91, 93–95, 108
TCN	Topology Change Notification	92, 96
TCP	Transmission Control Protocol	9, 24, 26, 27, 37, 40, 44, 62, 67, 85, 132, 133, 136, 149, 150
TTL	Time To Live	149
UDP	User Datagram Protocol	27, 37, 40, 85, 114, 121, 132, 133, 136
ULA	Unique Local Address	105
URL	Uniform Resource Locator	82, 84, 160, 161
USB	Universal Serial Bus	6, 24, 29–31, 51, 73
UTC	Universal Time Coordinated	137
UTP	Unshielded Twisted Pair	151, 155
UUID	Universally Unique IDentifier	51, 52
VFAT	Virtual File Allocation Table	50, 53
VPN	Virtual Private Network	31
VSZ	Virtual Set siZe	9, 145, 147
WAN	Wide Area Network	20–22, 26
ПЛК	Программируемый Логический Контроллер	66

1 Введение

В данном документе описываются основные страницы Web-интерфейса управления LuCI. Web-интерфейс управления LuCI является стандартной (используемой по умолчанию) системой Web-управления для операционной системы OpenWrt[1].

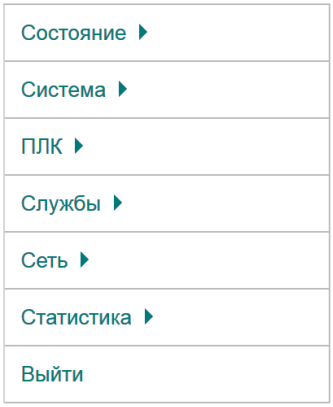


Рис. 1-1: Главное меню Web-интерфейса управления LuCI

В разделе 2 даётся описание мастера настройки, позволяющего выполнить первичную настройку основных параметров за несколько простых шагов.

В разделе 3 (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 3.2), активных маршрутов и правил (раздел 3.3), системного журнала (раздел 3.4), журнала ядра (раздел 3.5), и страницы для просмотра графиков в реальном времени для некоторых системных параметров (раздел 3.6).

В разделе 4 (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 монтированием 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 5 (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) а также страница с подробной информацией о запущенном в текущий момент пользовательском приложении CODESYS (см. раздел 5.4).

В разделе 6 (раздел меню «Службы») содержатся страницы настроек различных служб и приложений. Например, HTTP-сервер, служба STP/RSTP, служба DDNS, FTP-сервер.

В разделе 7 (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 страница настроек данной службы.

[1] https://openwrt.org/

1.1 Подключение к Web-интерфейсу LuCI

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

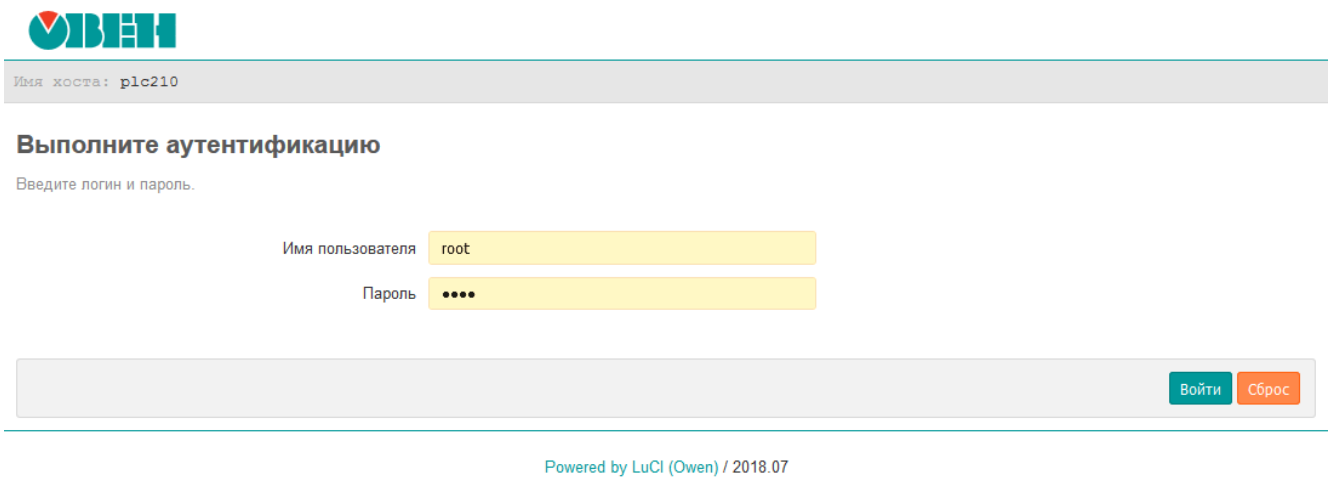


Рис. 1-2: Страница аутентификации

По умолчанию, для аутентификации необходимо использовать следующие учётные данные:

- имя пользователя — «root»;
- пароль — «owen».

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.

В том случае, если вход в систему выполняется первый раз, то после успешной аутентификации, пользователю будет предложено выполнить настройку устройства при помощи мастера настройки (см. рисунок 2-1), работа с которым подробно описана в разделе 2.

1.2 Автоматическое обновление информации

На многих страницах веб-интерфейса LuCI 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 ВКЛЮЧЕНО» (см. рисунок 1-3(а)). Автоматическое обновление данных может быть отключено путём нажатия на надпись «АВТООБНОВЛЕНИЕ ВКЛЮЧЕНО». В этом случае надпись изменится на «АВТООБНОВЛЕНИЕ ВЫКЛЮЧЕНО», как показано на рисунке 1-3(б).

(а) Автоматическое обновление включено

(б) Автоматическое обновление выключено

Рис. 1-3: Автоматическое обновление данных страницы

Интервал автоматического обновления информации по умолчанию равен 5 секундам и может быть настроен во вкладке «Дополнительные» страницы «Общие настройки» раздела главного меню «Система» (см. раздел 4.1.4).

2 Мастер настройки

Данный раздел отсутствует в Web-интерфейсе управления контроллеров СПК.

Мастер настройки позволяет выполнить конфигурацию основных параметров устройства за несколько простых шагов.

При первом запуске устройства, после выполнения входа в систему (см. раздел 1.1), будет выведено окно с предложением запуска мастера настройки, как показано на рисунке 2-1.

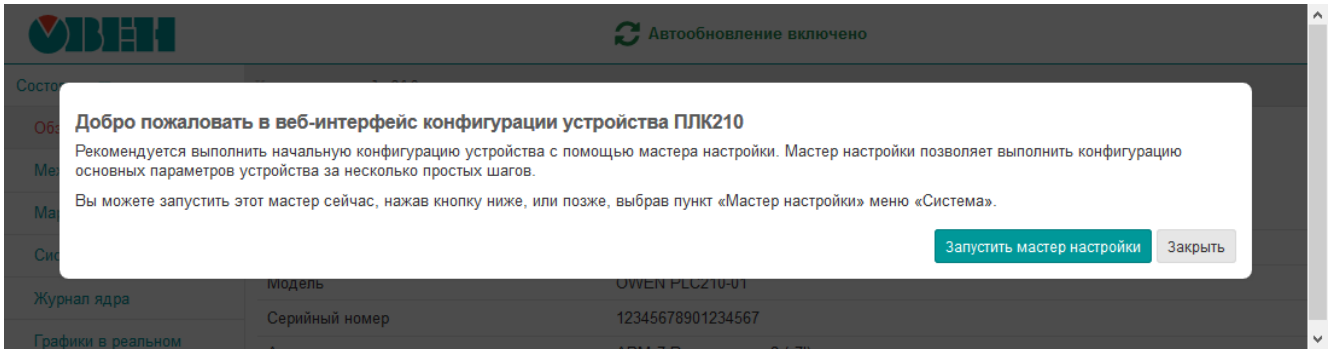


Рис. 2-1: Запуск «Мастера настройки» при первом включении устройства

Для запуска мастера настройки необходимо нажать кнопку «Запустить мастер настройки».

В дальнейшем мастер настройки можно запустить вручную при помощи пункта меню «Мастер настройки» главного меню «Система» (см. раздел 4.10).

Конфигурация параметров в мастере настройки разделена на следующие шаги:

1) выбор языка интерфейса (раздел 2.1);
2) установка пароля доступа к устройству (раздел 2.2);
3) конфигурация параметров хоста (раздел 2.3);
4) настройка даты и времени, включая конфигурацию клиента и сервера NTP (раздел 2.4);
5) выбор схемы сетевых портов (раздел 2.5);
6) настройка сетевых интерфейсов (раздел 2.6);
7) настройка службы SSH (раздел 2.7);
8) настройка службы FTP (раздел 2.8);
9) настройка правил межсетевого экрана (раздел 2.9).

В верхней части страницы мастера настроек расположена информация о ходе выполнения настройки в виде списка шагов, в котором обозначены уже пройденные шаги, текущий шаг и оставшиеся шаги до завершения настройки (см. рисунок 2-2).

В нижней части страницы мастера настроек расположена панель кнопок управления (см. рисунок 2-2).

Кнопка «Закрыть мастер настройки» выполняет немедленное завершение работы мастера настройки, без применения параметров текущего шага.

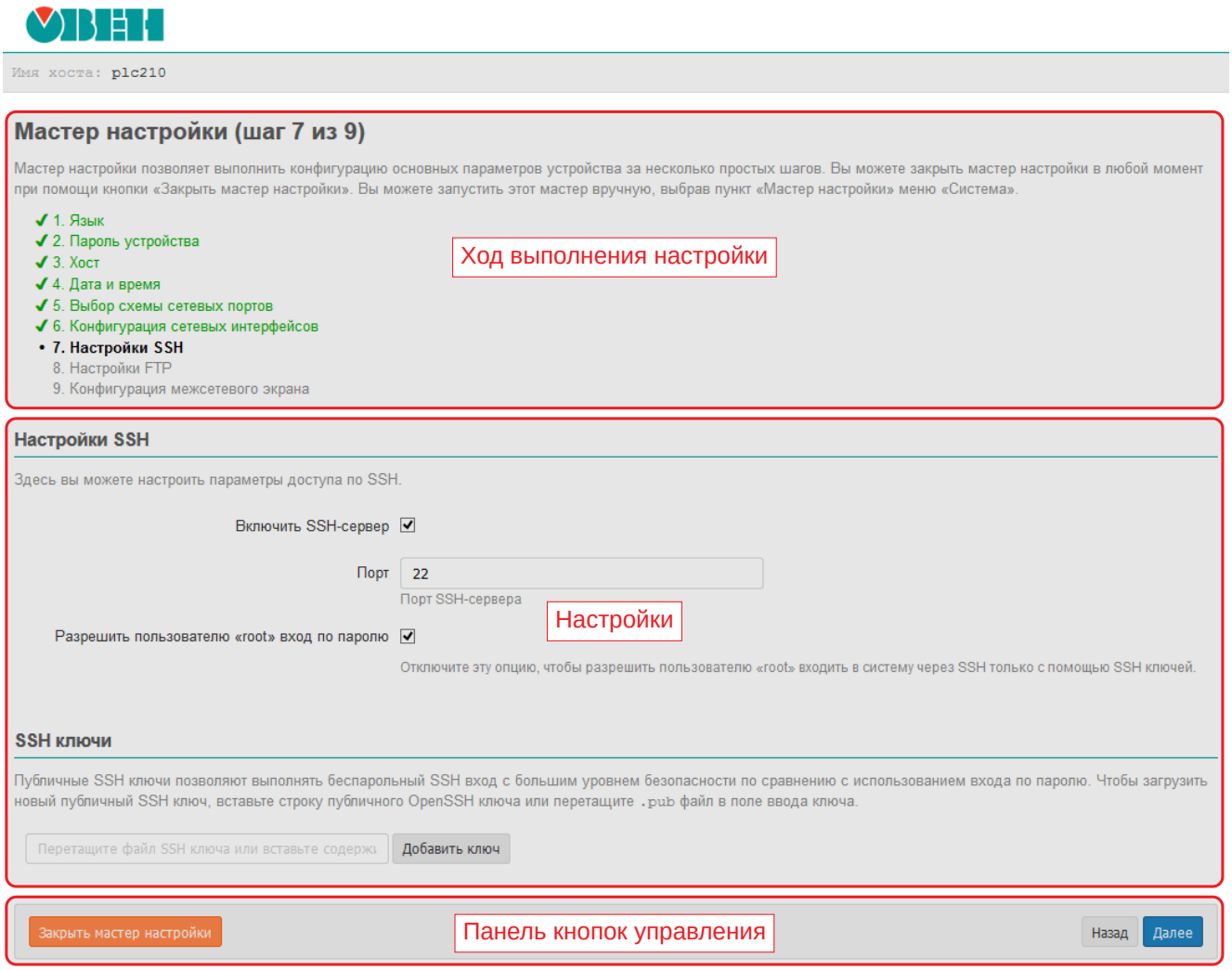


Рис. 2-2: Мастер настройки. Элементы управления

Закрытие мастера настройки при помощи кнопки «Закрыть мастер настройки» не восстанавливает исходные параметры конфигурации (активные до запуска мастера настройки).

Кнопка «Назад» (отсутствует на первом шаге) выполняет переход к предыдущему шагу. Сконфигурированные параметры текущего шага при этом не применяются.

Применение выбранных параметров на каждом шаге выполняется непосредственно после нажатия кнопки «Далее» (или «Завершить», для последнего шага).

Между областью хода выполнения настройки (см. рисунок 2-2) и панелью кнопок управления расположены сами элементы настроек параметров каждого из шагов (область «Настройки» на рисунке 2-2). В последующих разделах приводится описание этих настроек для каждого шага мастера настройки.

2.1 Шаг 1: Язык

На этом шаге мастера настройки предлагается выполнить настройку языка веб-интерфейса LuCI. Элементы страницы настроек языка показаны на рисунке 2-3.

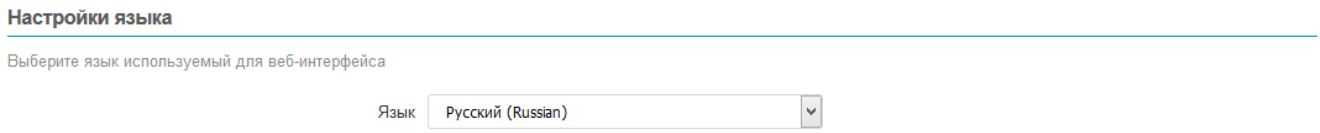


Рис. 2-3: Мастер настройки. Настройки языка интерфейса

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

В дальнейшем установку (смену) языка интерфейса можно выполнить во вкладке «Язык» пункта меню «Общие настройки» главного меню «Система» (см. раздел 4.1.3).

2.2 Шаг 2: Пароль устройства

На этом шаге мастера настройки предлагается выполнить установку (смену) пароля доступа к устройству (см. рисунок 2-4).

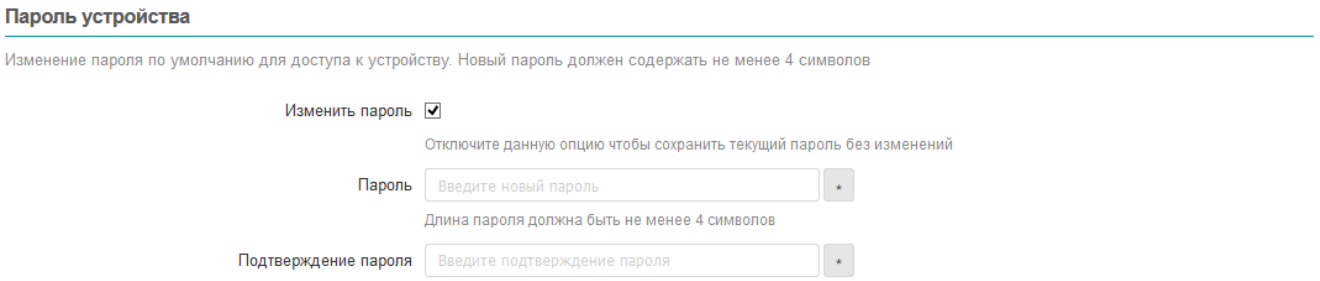


Рис. 2-4: Мастер настройки. Установка пароля устройства

При необходимости установки нового пароля нужно отметить опцию «Изменить пароль» и ввести новый пароль в поле «Пароль». В поле «Подтверждение пароля» необходимо повторить ввод нового пароля. Пароли в полях «Пароль» и «Подтверждение пароля» должны совпадать.

Если смена пароля не требуется (необходимо оставить текущий пароль без изменений), тогда опцию «Изменить пароль» нужно отключить.

В дальнейшем установку (смену) пароля доступа к устройству можно выполнить во вкладке «Пароль устройства» пункта меню «Управление» главного меню «Система» (см. раздел 4.3.1).

2.3 Шаг 3: Хост

На данном шаге мастера настройки выполняется конфигурация параметров хоста устройства (см. рисунок 2-5).

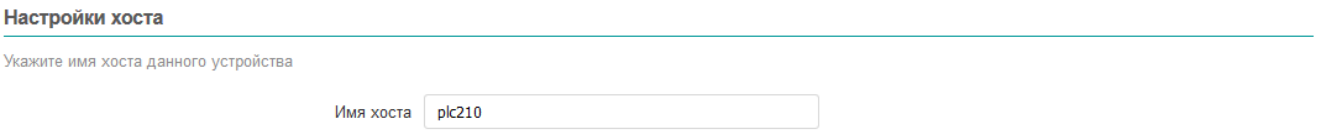
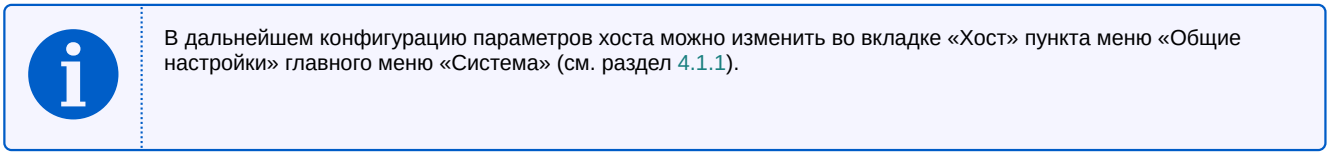


Рис. 2-5: Мастер настройки. Настройка параметров хоста

Для настройки доступен только один параметр — имя хоста.



В дальнейшем конфигурацию параметров хоста можно изменить во вкладке «Хост» пункта меню «Общие настройки» главного меню «Система» (см. раздел 4.1.1).

2.4 Шаг 4: Дата и время

На данном шаге мастера настройки выполняется конфигурация параметров локального времени устройства, а также параметров синхронизации времени при помощи службы NTP (см. рисунок 2-6)

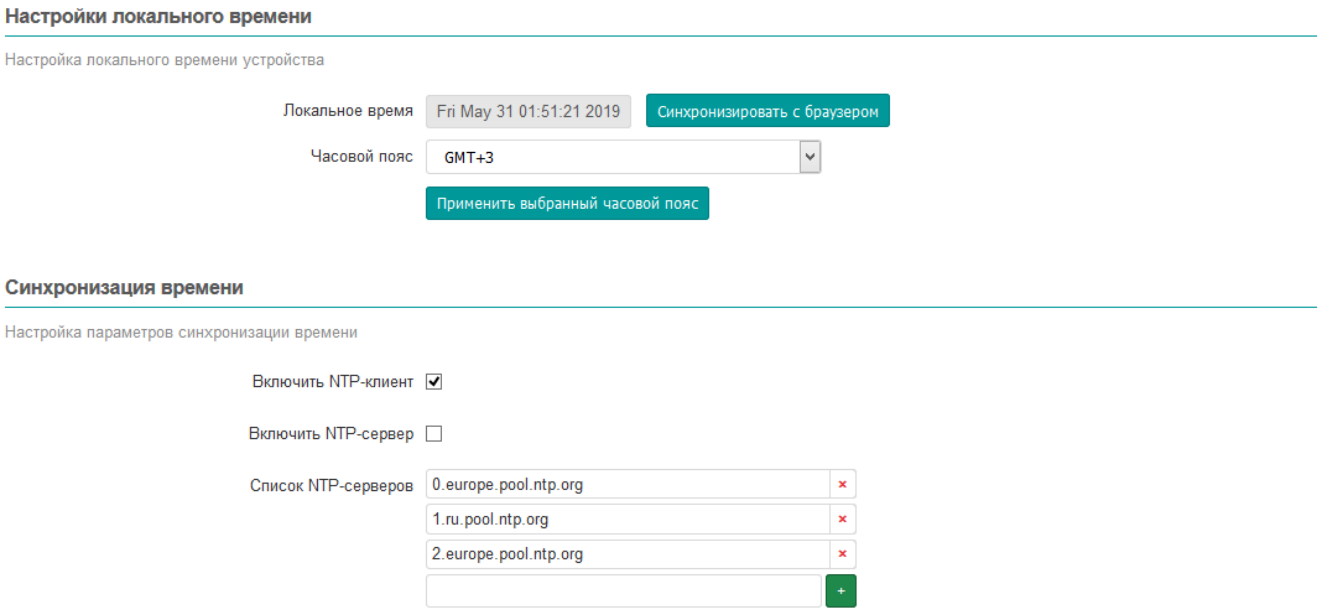
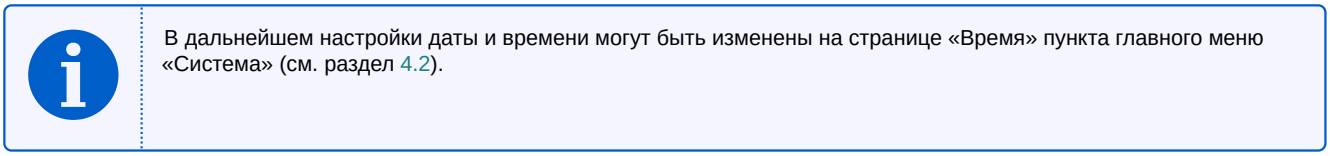


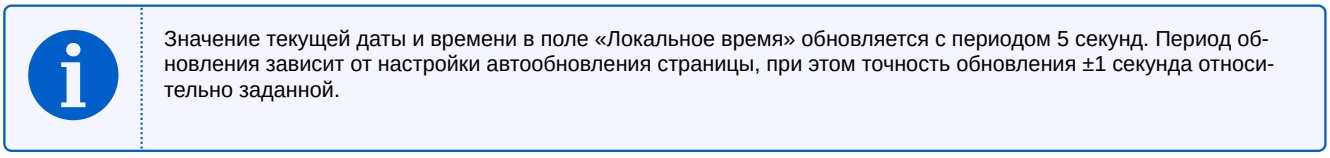
Рис. 2-6: Мастер настройки. Настройка даты и времени



В дальнейшем настройки даты и времени могут быть изменены на странице «Время» пункта главного меню «Система» (см. раздел 4.2).

2.4.1 Настройки локального времени

В подразделе настроек локального времени (см. рисунок 2-6) в поле «Локальное время» отображается текущее локальное время и дата.



Значение текущей даты и времени в поле «Локальное время» обновляется с периодом 5 секунд. Период обновления зависит от настройки автообновления страницы, при этом точность обновления ±1 секунда относительно заданной.

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 поля «Локальное время», дата и время будут установлены в новые значения.

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 нажать кнопку «Применить выбранный часовой пояс» и дождаться следующего обновления значения поля «Локальное время».

2.4.2 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.

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

2.5 Шаг 5: Выбор схемы сетевых портов

На данном шаге мастера настройки выполняется выбор схемы сетевых портов устройства (см. рисунки 2-7 и 2-8). Схема сетевых портов определяет роль каждого из физических сетевых портов устройства.

2.5.1 Выбор схемы сетевых портов ПЛК210

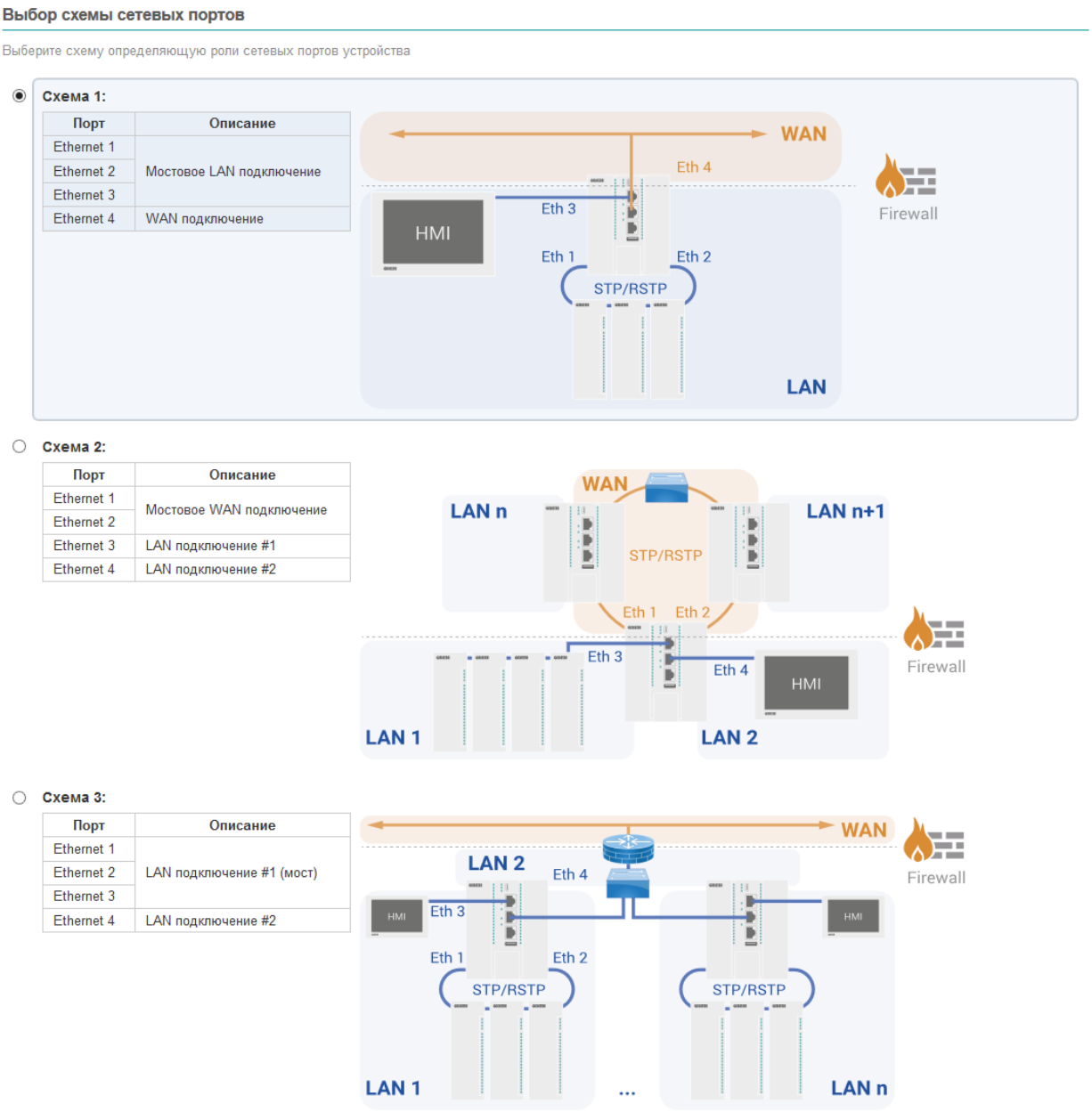


Рис. 2-7: Мастер настройки. Выбор схемы сетевых портов для ПЛК210

Для контроллера ПЛК210 доступны три схемы сетевых портов (см. рисунок 2-7):

1) Схема №1.

   Порты Ethernet 1, Ethernet 2 и Ethernet 3 объединены в мостовое подключение к локальной сети (LAN).

   Порт Ethernet 4 используется как отдельный изолированный сетевой интерфейс для подключения к глобальной сети (WAN), защищённый межсетевым экраном.

2) Схема №2.

   Порты Ethernet 1 и Ethernet 2 объединены в мостовое подключение к глобальной сети (WAN), защищённое межсетевым экраном.

   Порты Ethernet 3 и Ethernet 4 являются отдельными изолированным сетевыми интерфейсами для подключения к локальным сетям (LAN).

3) Схема №3.

   Порты Ethernet 1, Ethernet 2 и Ethernet 3 объединены в мостовое подключение к локальной сети (LAN).

   Порт Ethernet 4 является отдельным изолированным сетевым интерфейсом для подключения к отдельной локальной сети (LAN).

Схема 3 не имеет защищённого межсетевым экраном подключения к глобальной сети (WAN).

2.5.2 Выбор схемы сетевых портов ПЛК200

Для контроллера ПЛК200 доступны три схемы сетевых портов (см. рисунок 2-8):

1) Схема №1. Порт Ethernet 1 подключен к локальной сети (LAN).

   Порт Ethernet 2 используется как отдельный изолированный сетевой интерфейс для подключения к глобальной сети (WAN), защищённый межсетевым экраном.

   Данная схема позволяет разделить сеть на две зоны, обеспечивая одно пространство IP-адресов для порта Ethernet 1.

Рекомендуется установить динамический IP-адрес и включить режим DHCP для порта Ethernet 2.

IP-адрес в зоне LAN рекомендуется настраивать как статический.

2) Схема №2.

   Порты Ethernet 1 и Ethernet 2 объединены в мостовое подключение к локальной сети (LAN).

3) Схема №3.

   Порт Ethernet 1 подключен к локальной сети (LAN 1).

   Порт Ethernet 2 является отдельным сетевым интерфейсом для подключения к отдельной локальной сети (LAN 2 и LAN 3).

В случае подключения к глобальной сети (WAN) рекомендуется использовать промышленный маршрутизатор с поддержкой функции межсетевого экрана.

В случае подключения к глобальной сети (WAN) рекомендуется использовать промышленный маршрутизатор с поддержкой функции межсетевого экрана.

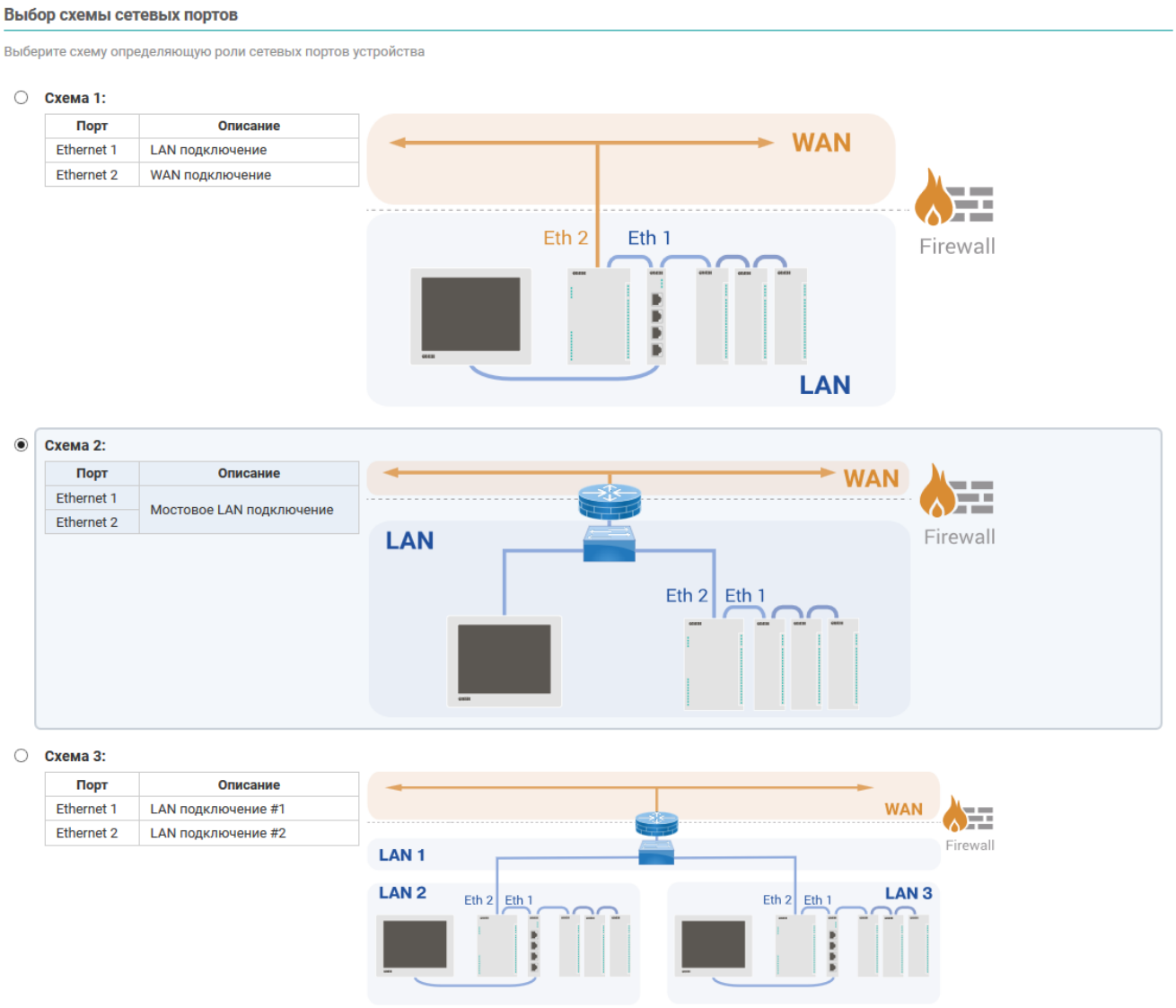


Рис. 2-8: Мастер настройки. Выбор схемы сетевых портов для ПЛК200

2.6 Шаг 6: Конфигурация сетевых интерфейсов

На данном шаге выполняется конфигурация сетевых интерфейсов в соответствии с выбранной схемой сетевых портов на предыдущем шаге (см. раздел 2.5). В зависимости от выбранной схемы сетевых портов, каждый настраиваемый интерфейс может быть одного из следующих типов:

- мостовое LAN подключение;
- мостовое WAN подключение;
- отдельный интерфейс для LAN подключения;
- отдельный интерфейс для WAN подключения.

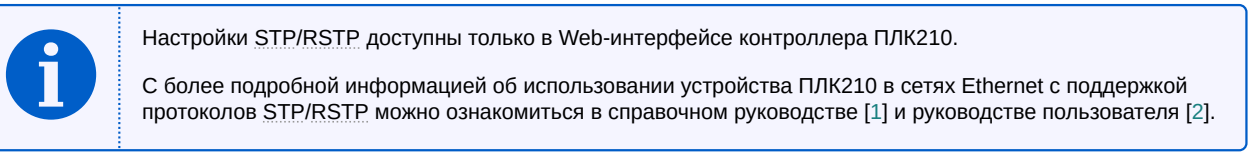
Для интерфейсов всех типов доступны следующие настройки:

- «Протокол» — протокол интерфейса. Возможен выбор из следующих протоколов:
  - «Статический адрес» — IP-адрес и маска подсети указываются вручную;
  - «Клиент DHCP» — IP-адрес и маска подсети назначаются автоматически с использованием DHCP протокола.
- «IPv4-адрес» — IP-адрес сетевого интерфейса для IP протокола версии 4. Данная настройка доступна только при выборе протокола «Статический адрес».
- «Маска сети IPv4» — маска подсети для IP протокола версии 4. Данная настройка доступна только при выборе протокола «Статический адрес».

- «Широковещательный IPv4-адрес» — широковещательный адрес сети для IP протокола версии 4. Широковещательный адрес сети можно не указывать (оставить поле пустым), в этом случае он будет вычислен автоматически на основании значений IP-адреса и маски сети. Данная настройка доступна только при выборе протокола «Статический адрес».

Для интерфейсов мостовых подключений (мостовое LAN и WAN подключения) доступны следующие дополнительные настройки:

- «Версия STP/RSTP» — версия протокола связного дерева (Spanning Tree) для моста:
  - «RSTP» — использовать протокол RSTP (Rapid Spanning Tree Protocol).
  - «STP» — использовать протокол STP (Spanning Tree Protocol).
  - «Отключено» — функции связного дерева отключены.



Настройки STP/RSTP доступны только в Web-интерфейсе контроллера ПЛК210.

С более подробной информацией об использовании устройства ПЛК210 в сетях Ethernet с поддержкой протоколов STP/RSTP можно ознакомиться в справочном руководстве [1] и руководстве пользователя [2].

Для интерфейсов подключения к глобальной сети WAN (мостовое или отдельный интерфейс) доступны следующие дополнительные настройки:

- «IPv4-адрес шлюза» — IP-адрес шлюза для IP протокола версии 4. Данная настройка доступна только при выборе протокола «Статический адрес».
- «Использовать собственные DNS сервера» — настройка позволяет указать собственные адреса DNS-серверов для данного сетевого интерфейса.

Для интерфейсов подключения к локальной сети LAN (мостовое или отдельный интерфейс) доступна возможность включения DHCP-сервера, которая представлена следующими дополнительными настройками (данные настройки доступны только при выборе протокола «Статический адрес»):

- «Включить DHCP-сервер» — включает службу DHCP-сервера на сетевом интерфейсе.
- «Предел адресов DHCP» — максимальное количество адресов, выдаваемых в аренду DHCP-сервером. Данная настройка доступна только если выбрана опция «Включить DHCP-сервер».
- «Стартовый адрес DHCP» — начальный адрес аренды. Данная настройка доступна только если выбрана опция «Включить DHCP-сервер».
- «Время аренды адреса DHCP» — время истечения срока аренды арендованных адресов. Минимальное значение — 2 минуты (120 секунд). Данная настройка доступна только если выбрана опция «Включить DHCP-сервер».

На рисунках 2-9, 2-10 и 2-11 показаны страницы настроек сетевых интерфейсов для схем №1, №2 и №3 сетевых портов ПЛК210.

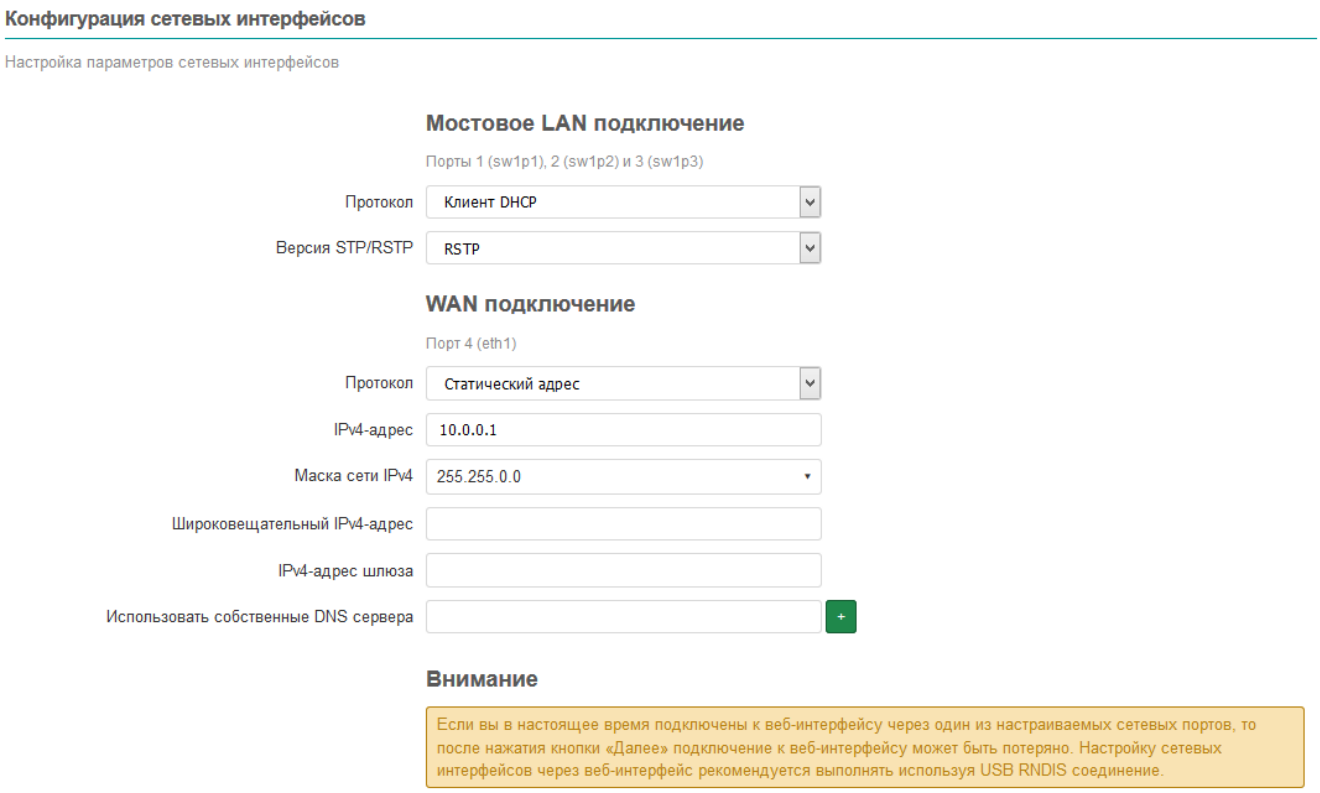


Рис. 2-9: Мастер настройки. Настройка сетевых интерфейсов для схемы №1

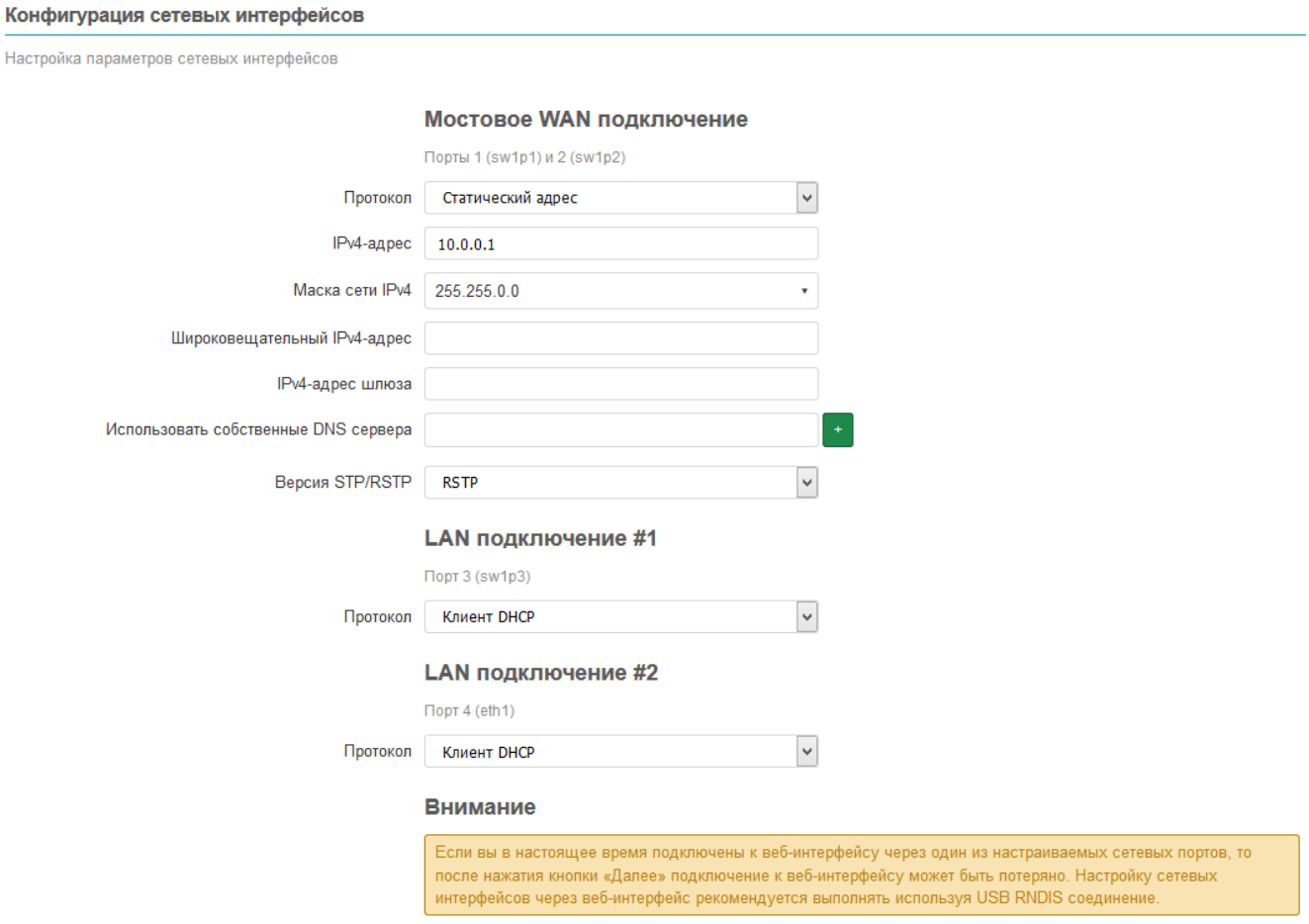


Рис. 2-10: Мастер настройки. Настройка сетевых интерфейсов для схемы №2

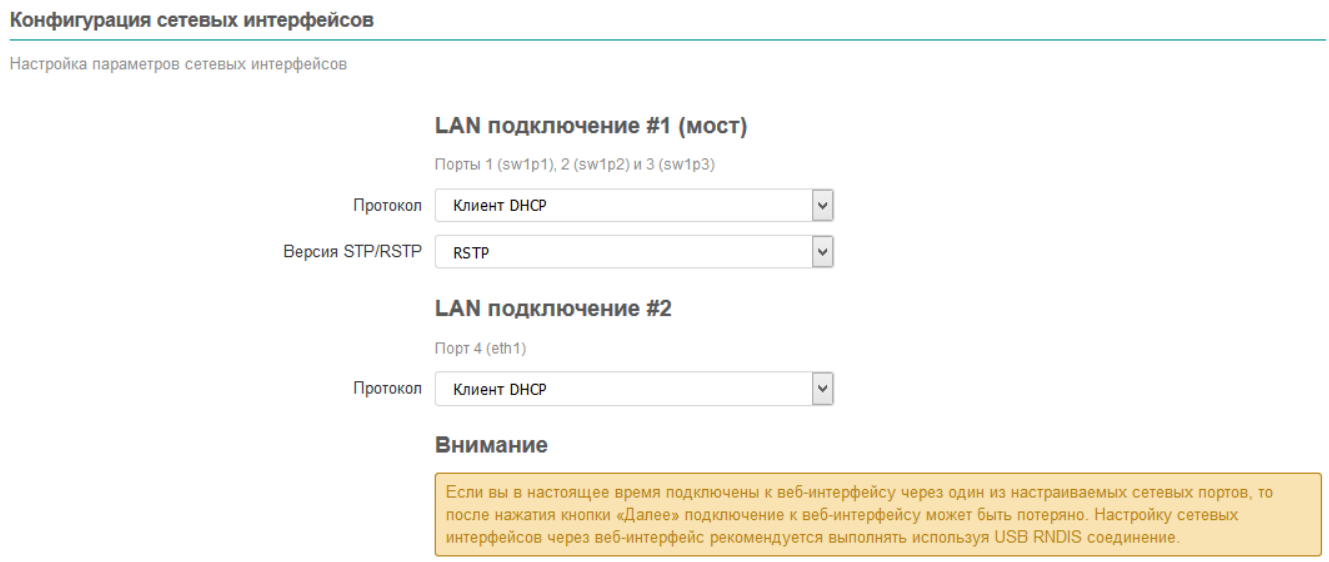


Рис. 2-11: Мастер настройки. Настройка сетевых интерфейсов для схемы №3

Следует помнить, что если подключение к веб-интерфейсу выполняется через один из настраиваемых сетевых портов, то после нажатия кнопки «Далее» подключение к веб-интерфейсу может быть потеряно.

Настройку сетевых интерфейсов через веб-интерфейс рекомендуется выполнять используя USB RNDIS соединение.

2.7 Шаг 7: Настройки SSH

На данном шаге мастера настройки выполняется настройка параметров доступа к устройству с использованием SSH протокола (см. рисунок 2-12).

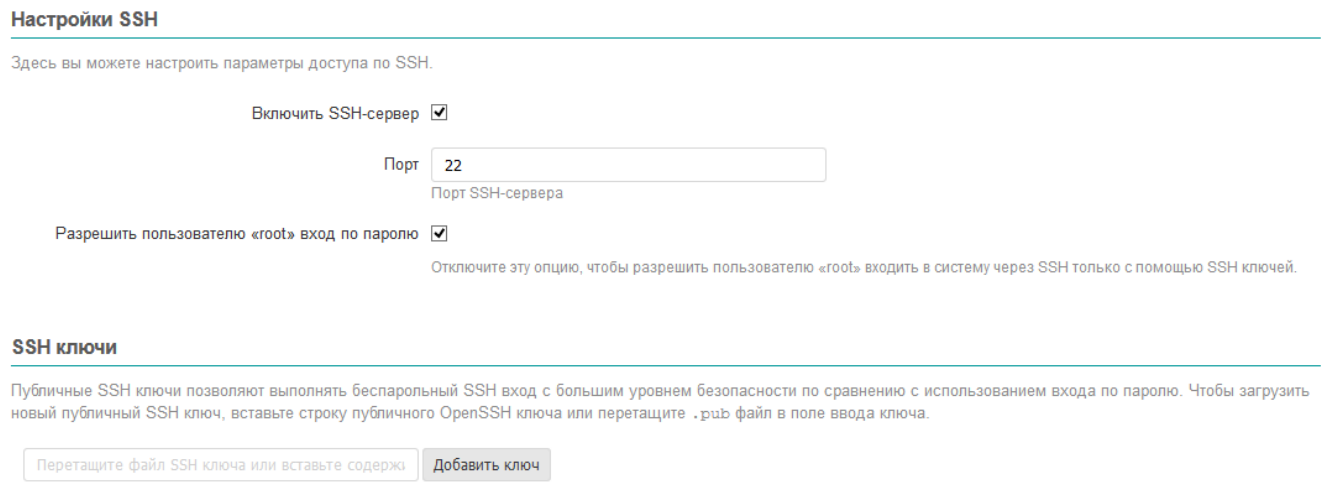


Рис. 2-12: Мастер настройки. Настройка SSH

Настройка «Включить SSH-сервер» предназначена для включения или отключения автоматического запуска службы SSH-сервера при запуске системы.

Номер TCP-порта, на котором будет запущена служба SSH-сервера указывается в поле «Порт».

Настройка «Разрешить пользователю „root“ вход по паролю» определяет возможность авторизации с использованием пароля при подключении через SSH. Если данная настройка отключена, то авторизация по паролю для пользователя «root» будет отключена. В этом случае, вход в систему через SSH возможен только с использованием SSH ключей (см. раздел 2.7.1).

В дальнейшем настройка службы SSH сервера может быть изменена на вкладке «Доступ по SSH» страницы «Управление» пункта главного меню «Система» (см. раздел 4.3.2), а управление SSH ключами — на вкладке «SSH-ключи» той же страницы.

2.7.1 SSH ключи

В подразделе настроек SSH «SSH ключи» возможно добавить один или несколько публичных SSH ключей. Эти SSH ключи будут использованы для выполнения авторизации.

Для добавления нового публичного ключа необходимо вставить строку публичного SSH ключа или перетащить «.pub» файл в поле ввода ключа и нажать кнопку «Добавить». Успешно добавленный SSH ключ будет отображён на странице, как показано на рисунке 2-13.

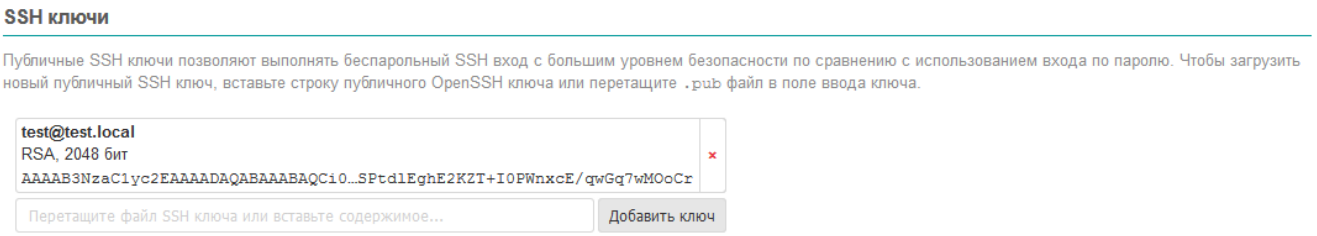


Рис. 2-13: Мастер настройки. Добавление SSH ключей

Для удаления добавленного ключа, необходимо нажать кнопку с красным крестиком справа от информации о ключе.

2.8 Шаг 8: Настройки FTP

На данном шаге мастера настройки выполняется настройка параметров FTP-сервера (см. рисунок 2-14).

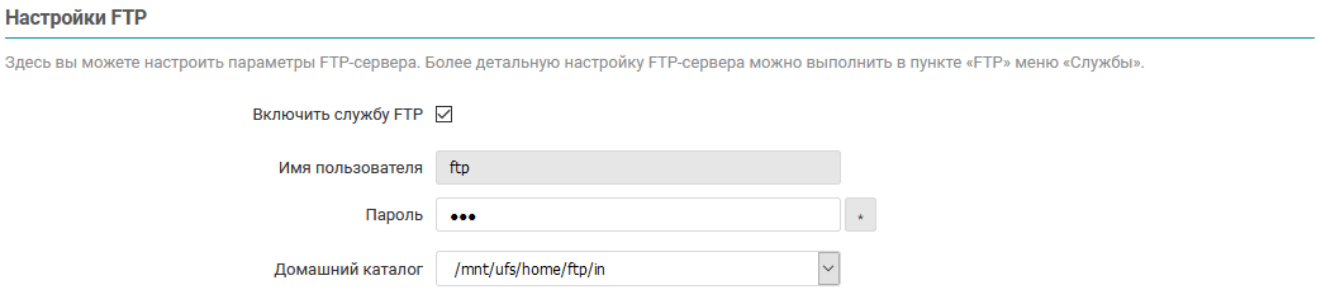


Рис. 2-14: Мастер настройки. Настройка FTP

Настройка «Включить службу FTP» предназначена для включения или отключения автоматического запуска службы FTP-сервера при запуске системы.

Имя пользователя для доступа к содержимому FTP-сервера указано в поле «Имя пользователя» и не может быть изменено. Пароль для пользователя указывается в поле «Пароль».

В выпадающем списке «Домашний каталог» выбирается путь к домашнему каталогу FTP-сервера.

В дальнейшем настройки службы FTP-сервера можно изменить на странице «FTP» раздела главного меню «Службы» (см. раздел 6.4).

2.9 Шаг 9: Конфигурация межсетевого экрана

На данном шаге мастера настройки выполняется настройка правил межсетевого экрана для подключения к глобальной сети (WAN).

В том случае, если при выполнении настройки была выбрана схема сетевых портов без подключения к глобальной сети (WAN), настройки межсетевого экрана будут не доступны. В этом случае, область настроек данного шага будет выглядеть так, как показано на рисунке 2-15.

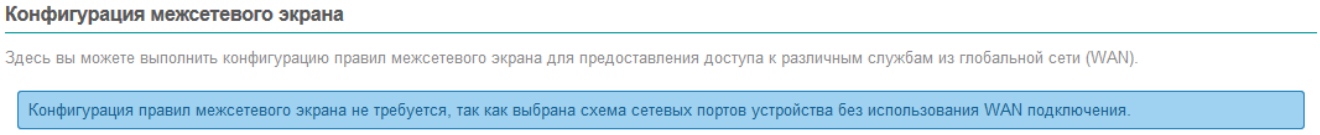


Рис. 2-15: Мастер настройки. Настройка межсетевого экрана

Для схемы сетевых портов с подключением к глобальной сети (WAN) настройки межсетевого экрана для данного шага будут выглядеть так, как показано на рисунке 2-16.

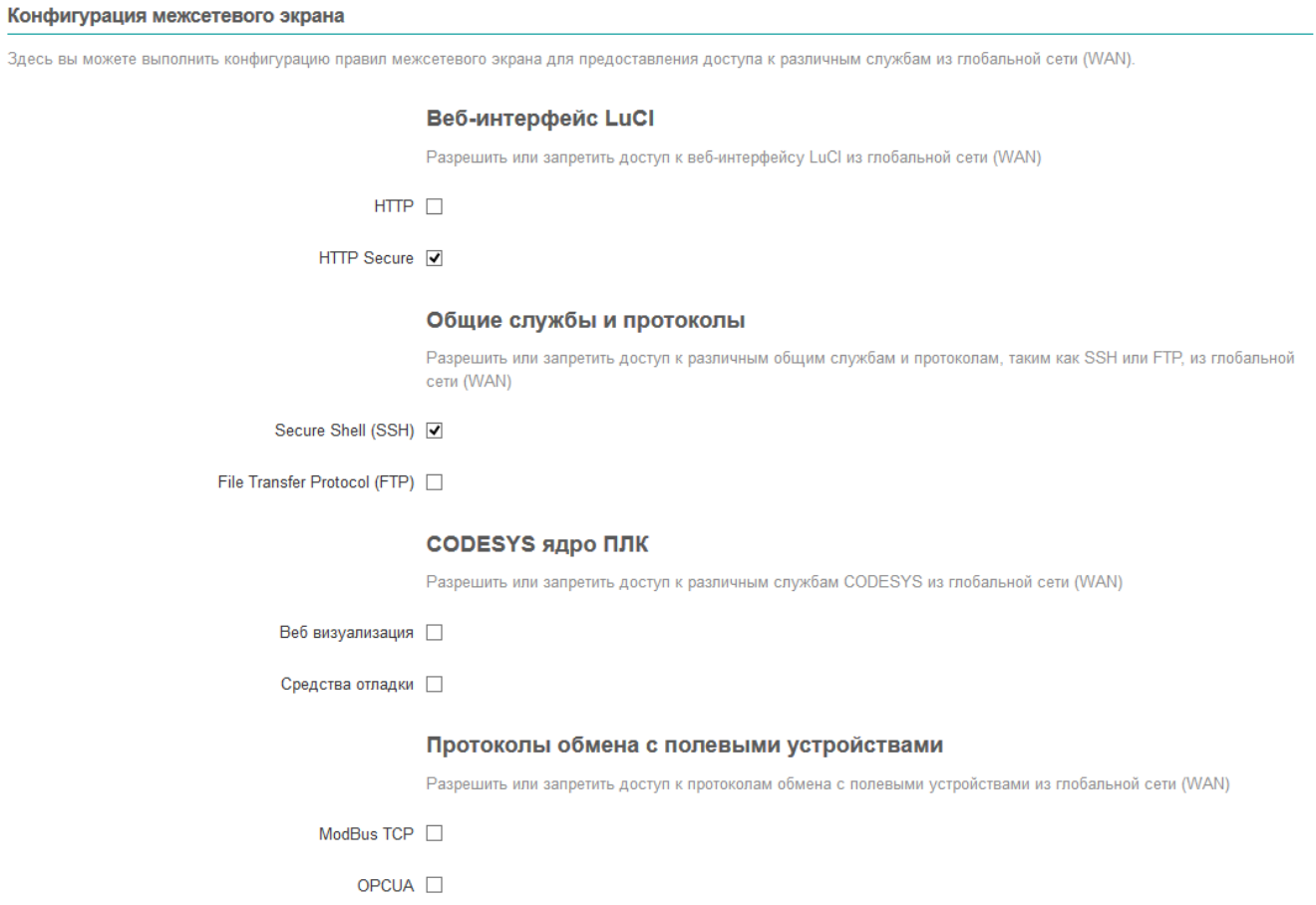


Рис. 2-16: Мастер настройки. Настройка межсетевого экрана

Каждая настройка позволяет открыть доступ из глобальной сети (WAN) к определённым службам (если настройка включена — доступ разрешён, если выключена — доступ запрещён):

- «HTTP» — доступ к веб-интерфейсу LuCI по протоколу HTTP (по умолчанию TCP порт 80).
- «HTTP Secure» — доступ к веб-интерфейсу LuCI по протоколу HTTPS (по умолчанию TCP порт 443).
- «Secure Shell (SSH)» — доступ к устройству по протоколу SSH (по умолчанию TCP порт 22).
- «File Transfer Protocol (FTP)» — доступ к устройству по протоколу FTP (по умолчанию TCP порты 21 и 10050–10100).
- «Веб визуализация» — доступ к веб-визуализации CODESYS (по умолчанию TCP порты 8080 и 8443).

- «Средства отладки» — отладочные средства CODESYS (по умолчанию TCP порт 11740, UDP порт 1740).
- «ModBus TCP» — доступ к ModBus TCP интерфейсу CODESYS (по умолчанию TCP/UDP порт 502).
- «OPC UA» — доступ к OPC UA интерфейсу CODESYS (по умолчанию TCP/UDP порт 4840).

В дальнейшем настройки межсетевого экрана можно изменить на странице «Межсетевой экран» раздела главного меню «Сеть» (см. раздел 7.5).

Любые открытые порты во внешнюю (глобальную) сеть могут представлять серьёзную угрозу безопасности.

Открывая во внешнюю сеть доступ к веб-интерфейсу LuCI по протоколам HTTP или HTTPS, следует обязательно позаботиться об установке сложного пароля для входа (см. раздел 2.2).

Открывая во внешнюю сеть доступ к веб-визуализации CODESYS, средствам отладки CODESYS, шинам OPC UA или ModBus TCP, следует понимать, что данные службы будут доступны любому во внешней сети без какой-либо авторизации.

Открывая во внешнюю сеть доступ по протоколу SSH, следует обязательно позаботиться о безопасном пароле или включить авторизацию только с использованием SSH ключей, то есть запретить вход по паролю (см. раздел 2.7).

Открывая во внешнюю сеть доступ по протоколу FTP, следует обязательно позаботиться о безопасном пароле (см. раздел 2.8).

3 Состояние

3.1 Обзор

На странице «Обзор» раздела «Состояние» отображается сводная информация о текущем состоянии устройства. Внешний вид страницы «Обзор» показан на рисунке 3-1.

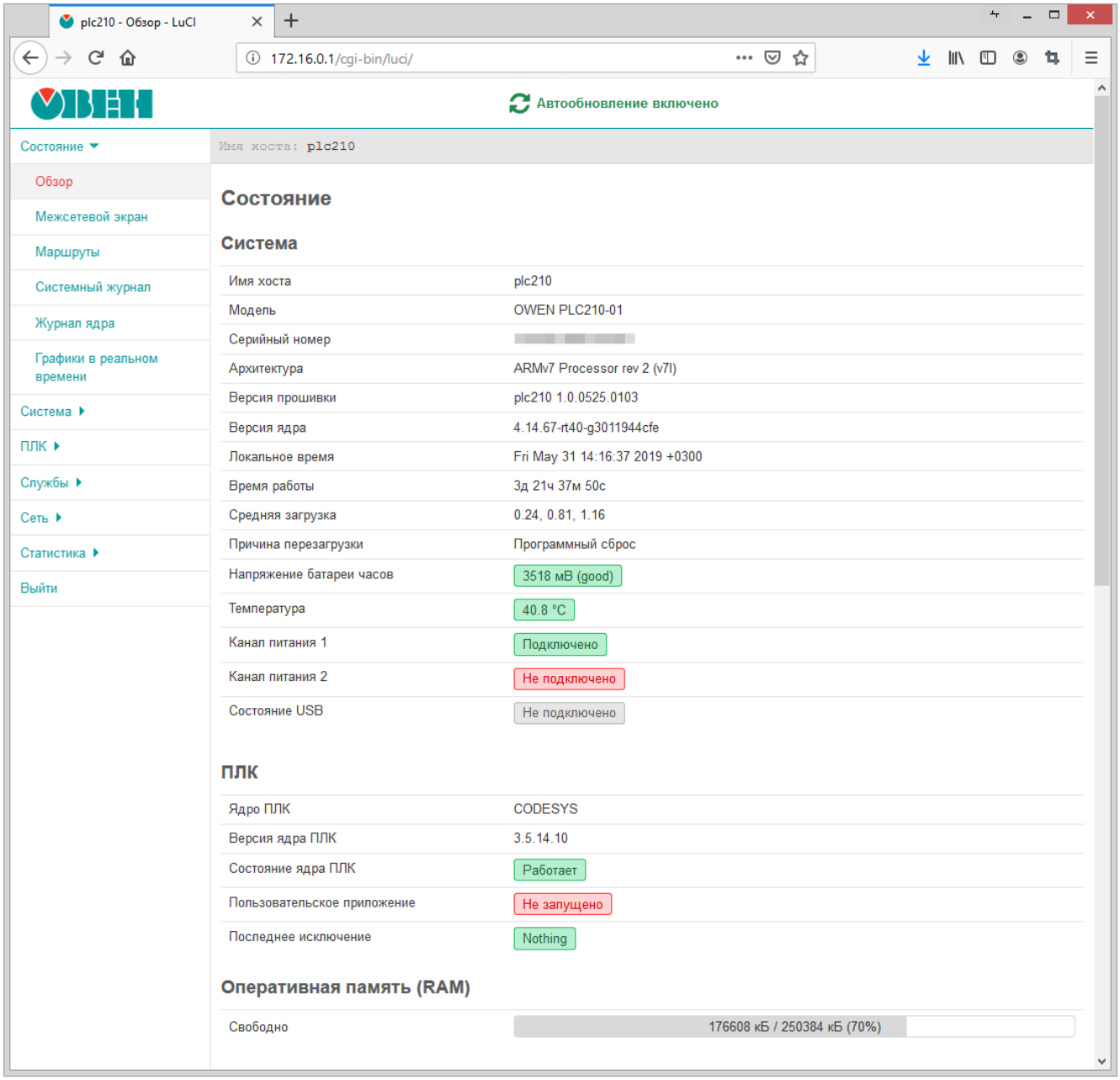


Рис. 3-1: Страница «Обзор»

Страница «Обзор» разделена на несколько подразделов:

- «Система» (см. раздел 3.1.1);
- «ПЛК» (см. раздел 3.1.2);
- «Оперативная память (RAM)» (см. раздел 3.1.3);
- «Состояние портов сетевых интерфейсов» (см. раздел 3.1.4);
- «Сеть» (см. раздел 3.1.5);
- «Активные DHCP аренды» (см. раздел 3.1.6).

3.1.1 Подраздел «Система»

Имя хоста	plc210
Модель	OWEN PLC210-01
Серийный номер	
Архитектура	ARMv7 Processor rev 2 (v7l)
Версия прошивки	plc210 1.0.0525.0103
Версия ядра	4.14.67-rt40-g3011944cfe
Локальное время	Fri May 31 13:45:26 2019 +0300
Время работы	3д 21ч 6м 39с
Средняя загрузка	1.53, 0.65, 0.43
Причина перезагрузки	Программный сброс
Напряжение батареи часов	3518 мВ (good)
Температура	40.1 °C
Канал питания 1	Подключено
Канал питания 2	Не подключено
Состояние USB	Не подключено

Рис. 3-2: Состояние. Подраздел «Система»

В подразделе «Система» страницы «Обзор» (см. рисунок 3-2) приводятся основные параметры системы:

- «Имя хоста» — имя системы (имя хоста);
- «Модель» — модель устройства;
- «Серийный номер» — серийный номер устройства;
- «Архитектура» — модель и архитектура процессора;
- «Версия прошивки» — версия прошивки;
- «Версия ядра» — версия ядра операционной системы;
- «Локальное время» — текущие дата и время;
- «Время работы» — время работы устройства (с момента включения);
- «Средняя загрузка» — текущие значения средней загрузки [3] (средние значения за 1, 5 и 15 минут);
- «Причина перезагрузки» — описание причины последней перезагрузки;
- «Напряжение батареи часов» — значение напряжения батареи часов (значение измеряется при включении, далее — один раз в сутки)[1];
- «Температура» — значение датчика температуры, установленного на плате устройства[2];
- «Канал питания 1», «Канал питания 2» — состояние 1-го и 2-го каналов питания[3];
- «Состояние USB» — состояние USB подключения. В данной строке отображается информация о скорости подключённого USB устройства (см. рисунок 3-3), а также информация о перегрузке по току, в случае её возникновения (см. рисунок 3-4)[4].

Подключено High-speed устройство

Рис. 3-3: Состояние. Подраздел «Система». Информация о скорости подключения USB устройстве

[1] Параметр отсутствует в Web-интерфейсе управления контроллеров СПК.
[2] Параметр отсутствует в Web-интерфейсе управления контроллеров СПК.
[3] Параметр отсутствует в Web-интерфейсе управления контроллеров СПК. В Web-интерфейсе управления контроллеров ПЛК200 присутствует только параметр «Канал питания 1».
[4] Параметр отсутствует в Web-интерфейсе управления контроллеров ПЛК200.

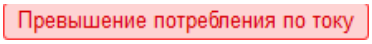


Рис. 3-4: Состояние. Подраздел «Система». Информация о перегрузке по току на USB интерфейсе

3.1.2 Подраздел «ПЛК»

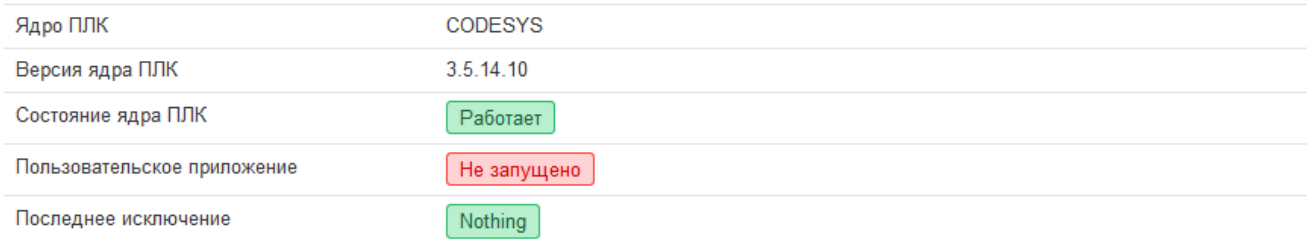


Рис. 3-5: Состояние. Подраздел «ПЛК»

В подразделе «ПЛК» страницы «Обзор» (см. рисунок 3-5) приводятся параметры функций ПЛК устройства:

- «Ядро ПЛК» — наименование используемого ядра ПЛК;
- «Версия ядра ПЛК» — версия используемого ядра ПЛК;
- «Состояние ядра ПЛК» — состояние ядра ПЛК. Может принимать значения:
  - «Работает» — ядро ПЛК запущено и работает;
  - «Остановлено» — ядро ПЛК остановлено и не работает.
- «Пользовательское приложение» — краткая информация о пользовательском приложении. Может принимать одно из следующих значений:
  - «Работает» — пользовательское приложение запущено и работает;
  - «Не запущено» — пользовательское приложение не запущено;
  - «Остановлено» — пользовательское приложение остановлено;
  - «Исключение» — работа пользовательского приложения была прервана из-за произошедшего исключения. Информация о последнем произошедшем исключении приведена в поле «Последнее исключение».

  Если пользовательское приложение загружено, выводится следующая дополнительная информация о приложении (см. пример на рисунке 3-6):
  - «Имя» — название (имя) приложения;
  - «Автор» — автор приложения;
  - «Версия» — версия приложения;
  - «Изменено» — дата и время последнего изменения приложения.

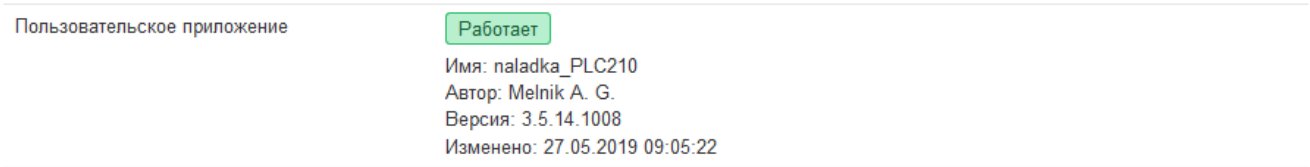


Рис. 3-6: Состояние. Подраздел «ПЛК». Информация о запущенном пользовательском приложении

- «Последнее исключение» — информация о последнем произошедшем исключении.

3.1.3 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 3-7.

Рис. 3-7: Состояние. Подраздел «Оперативная память (RAM)»

3.1.4 Подраздел «Состояние портов сетевых интерфейсов»

В подразделе «Состояние портов сетевых интерфейсов» страницы «Обзор» приводится таблица всех портов сетевых интерфейсов в виде таблицы (см. рисунок 3-8).

Количество сетевых интерфейсов может отличаться в зависимости от модели контроллера.

Имя и MAC-адрес	Состояние подключения	Интерфейс	В составе моста	Зоны межсетевого экрана	Получение (RX)	Передача (TX)
Ethernet 1 :42:6C:4C	Не подключено	sw1p1	br-lan (LAN), порт 1	lan	–	–
Ethernet 2 :42:6C:4E	100 Мбит/с, полный дуплекс	sw1p2	br-lan (LAN), порт 2	lan	9.90 МБ (213640 пакетов)	4.98 МБ (17170 пакетов)
Ethernet 3 :42:6C:4F	100 Мбит/с, полный дуплекс	sw1p3	br-lan (LAN), порт 3	lan	7.71 МБ (167581 пакетов)	318 Б (6 пакетов)
Ethernet 4 :42:6C:4D	100 Мбит/с, полный дуплекс	eth1 (WAN)	–	wan	139.88 МБ (616094 пакетов)	511.68 КБ (4741 пакетов)
USB RNDIS 48:6F:73:74:50:43	Подключено	usb0 (USB0)	–	–	24.29 МБ (328930 пакетов)	55.44 МБ (323294 пакетов)

Рис. 3-8: Состояние. Подраздел «Состояние портов сетевых интерфейсов»

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			

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 подключения, если такая информация доступна для данного интерфейса.

Дополнительно, в данном столбце отображается иконка, которая определяет тип и текущее состояние подключения. 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 сетевой интерфейс (если таковой имеется). При нажатии на имя виртуального интерфейса произойдёт переход к странице настройки соответствующего сетевого интерфейса (см. раздел 7.1.1).
- «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.

3.1.5 Подраздел «Сеть»

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

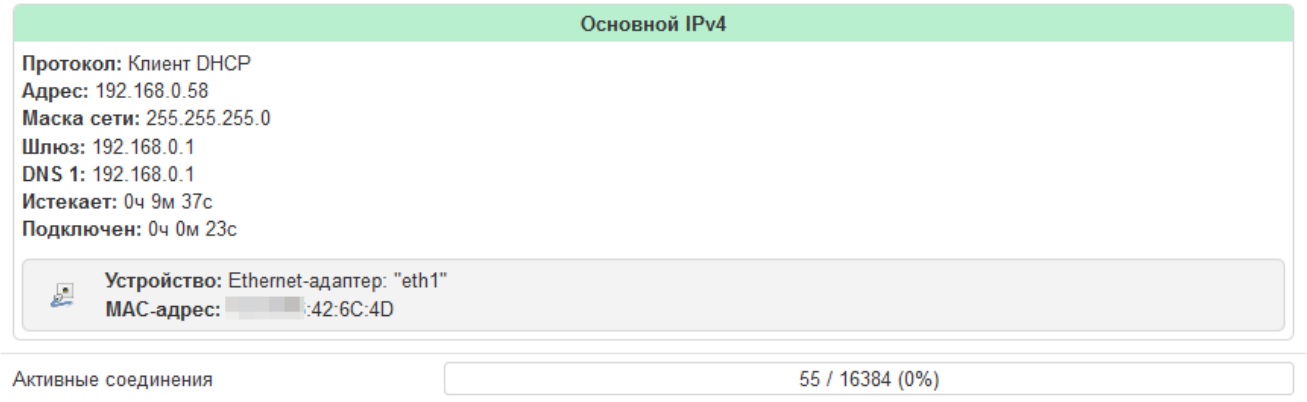


Рис. 3-9: Состояние. Подраздел «Сеть»

Кроме того, внизу подраздела «Сеть» страницы «Обзор» отображается текущее и максимально возможное количество сетевых соединений в виде шкалы (см рисунок 3-9).

3.1.6 Подраздел «Активные DHCP аренды»

В подразделе «Активные DHCP аренды» страницы «Обзор» приводится таблица активных арендованных DHCP адресов (см. рисунок 3-10).

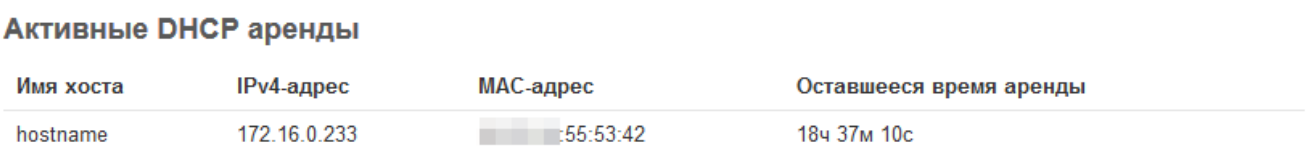


Рис. 3-10: Состояние. Подраздел «Активные DHCP аренды»

Каждая строка таблицы соответствует одному арендованному адресу. Таблица имеет следующие столбцы:

- «Имя хоста» — имя хоста клиента, которому выдан адрес в аренду;
- «IPv4-адрес» — IPv4 адрес, выданный клиенту в аренду;
- «MAC-адрес» — аппаратный MAC адрес клиента, получившего адрес в аренду;
- «Оставшееся время аренды» — оставшееся время аренды выданного адреса.

3.2 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 3-11.

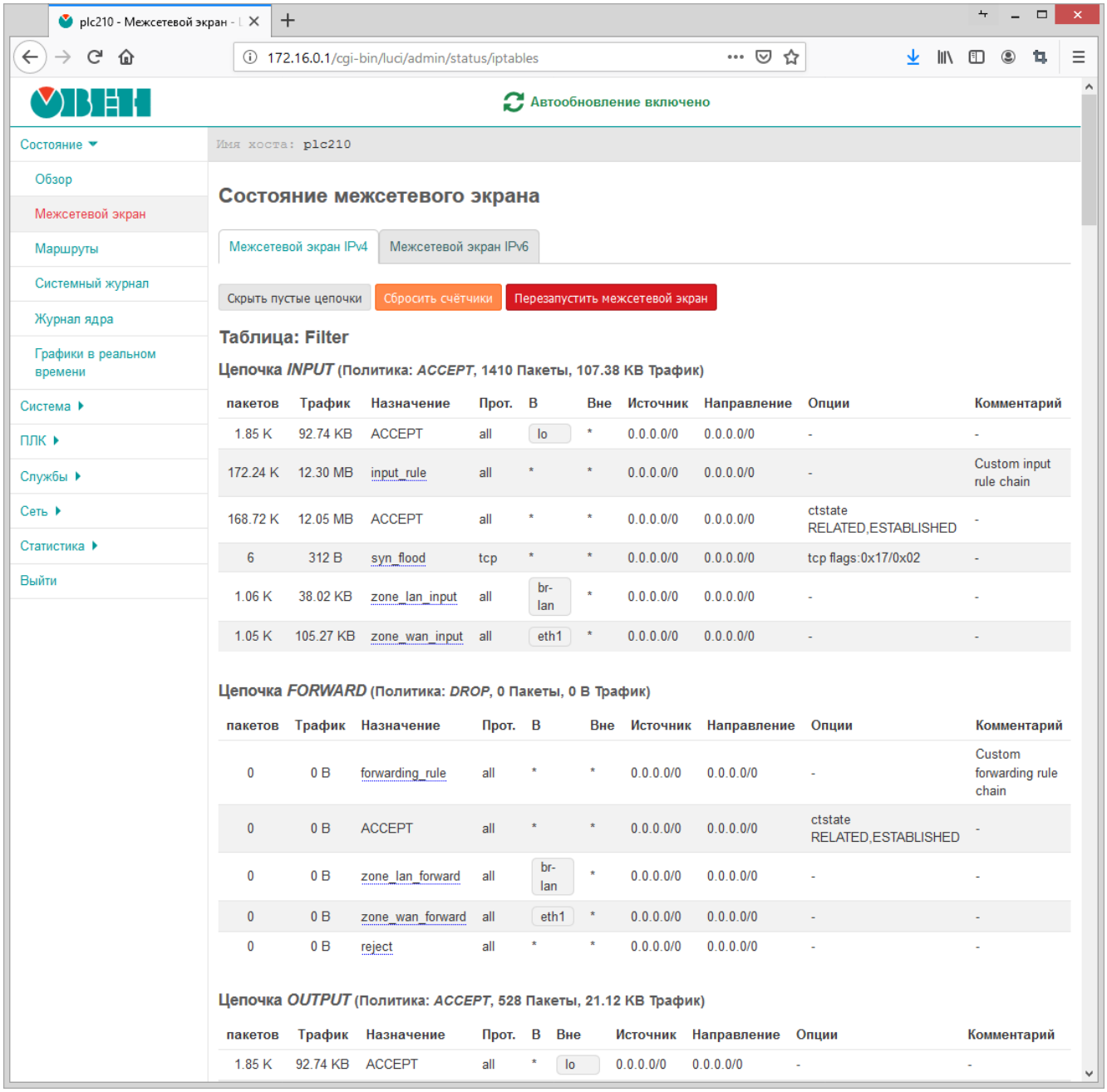


Рис. 3-11: Страница «Межсетевой экран»

Для понимания приведённых данных в таблицах на странице «Межсетевой экран» рекомендуется ознакомиться с документацией к межсетевому экрану netfilter для ядер Linux [4] и к утилите управления iptables [5].

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

3.3 Маршруты

На странице «Маршруты» 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» показан на рисунке 3-12.

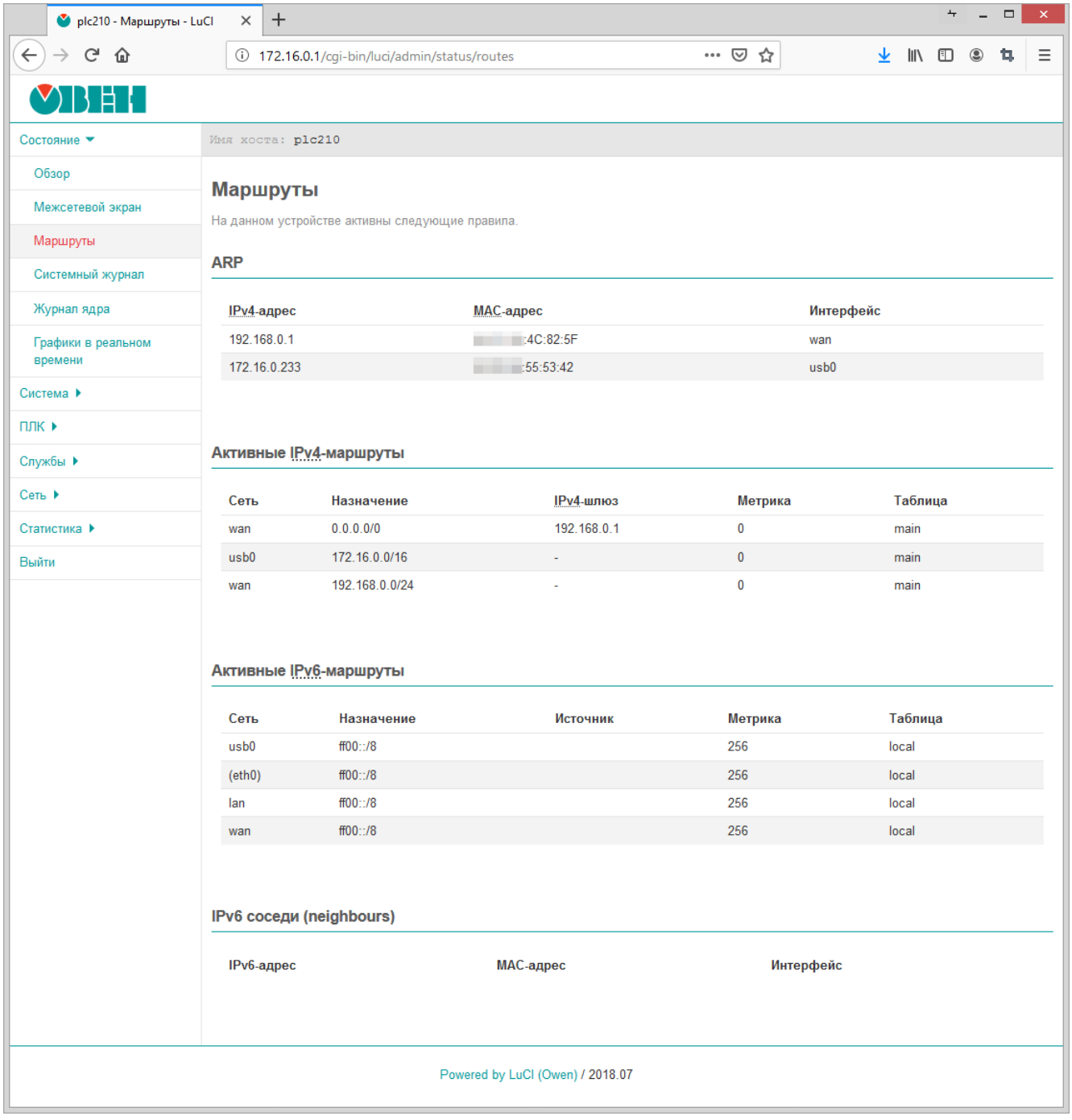


Рис. 3-12: Страница «Маршруты»

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

3.4 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 3-13.

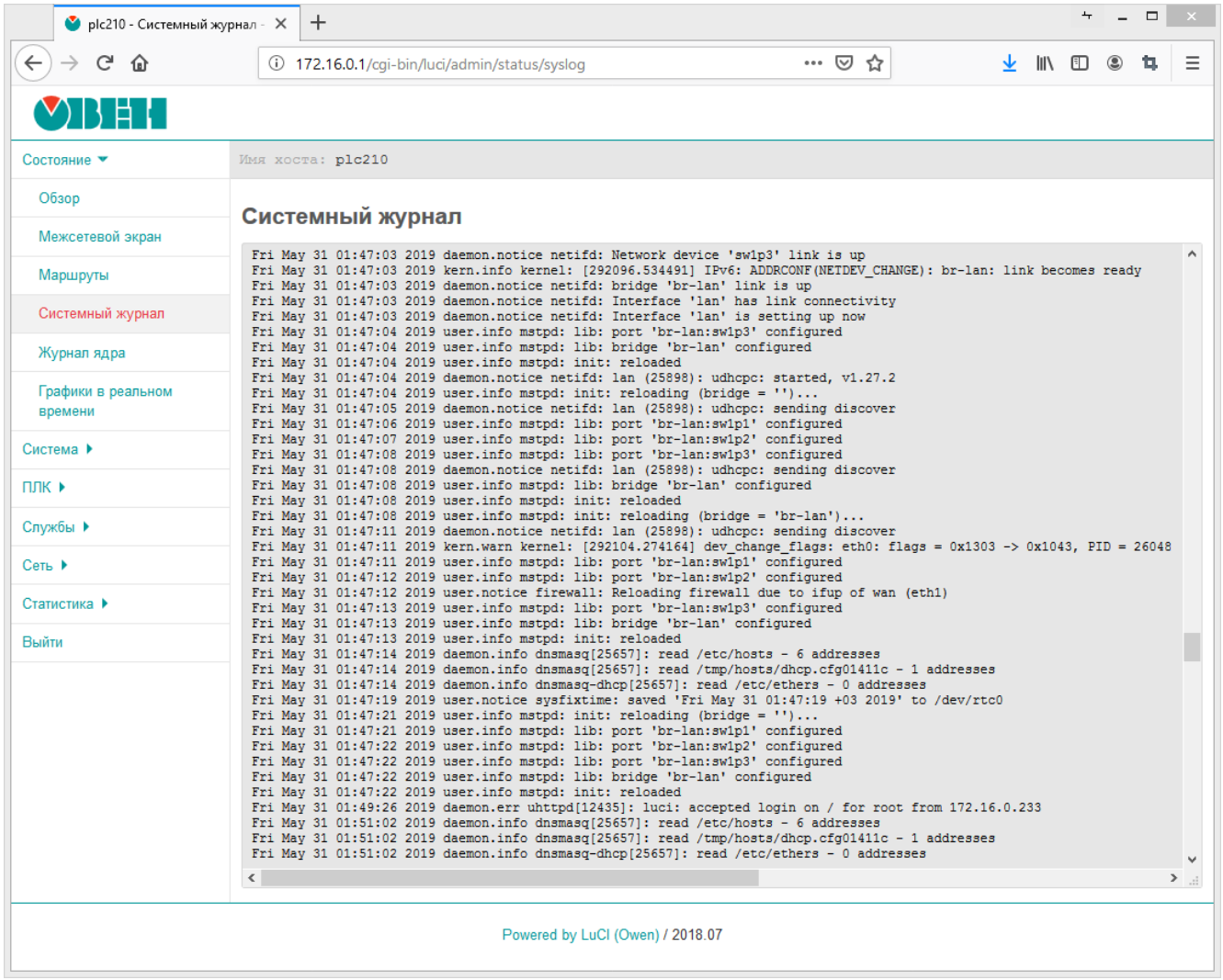


Рис. 3-13: Страница «Системный журнал»

3.5 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 3-14.

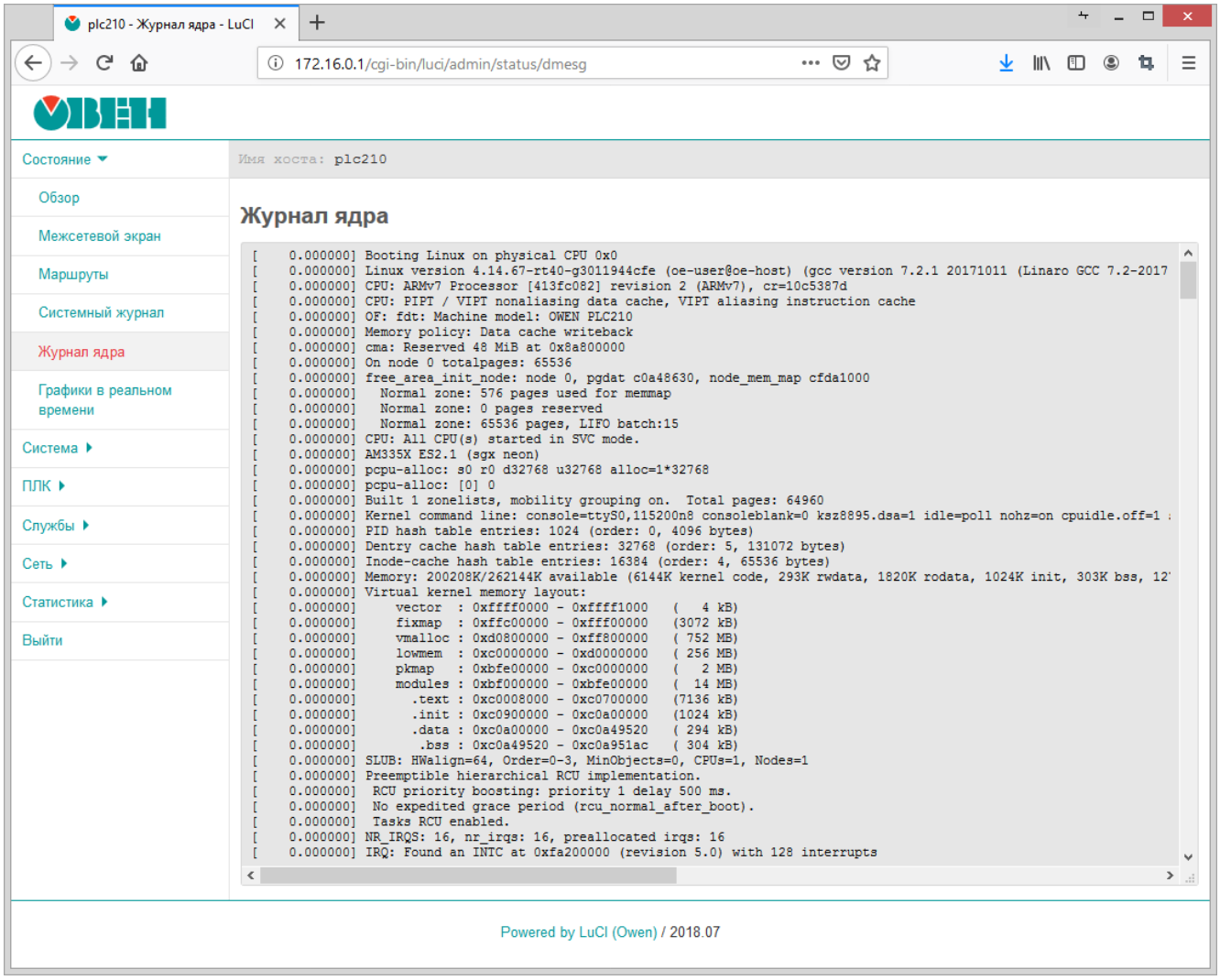


Рис. 3-14: Страница «Журнал ядра»

Основным отличием журнала ядра от системного журнала является то, что в журнале ядра не регистрируются какие-либо события от приложений и служб уровня пользователя.

3.6 Графики в реальном времени

На странице «Графики в реальном времени» раздела «Состояние» отображаются графики для некоторых системных параметров в реальном времени:

- текущая загрузка системы [3] (средние значения за 1, 5 и 15 минут);
- текущие входящий и исходящий трафик сетевых интерфейсов;
- текущие активные UDP и TCP соединения, включая полный список всех соединений.

Внешний вид страницы «Графики в реальном времени» для различных графиков показан на рисунках 3-15, 3-16 и 3-17.

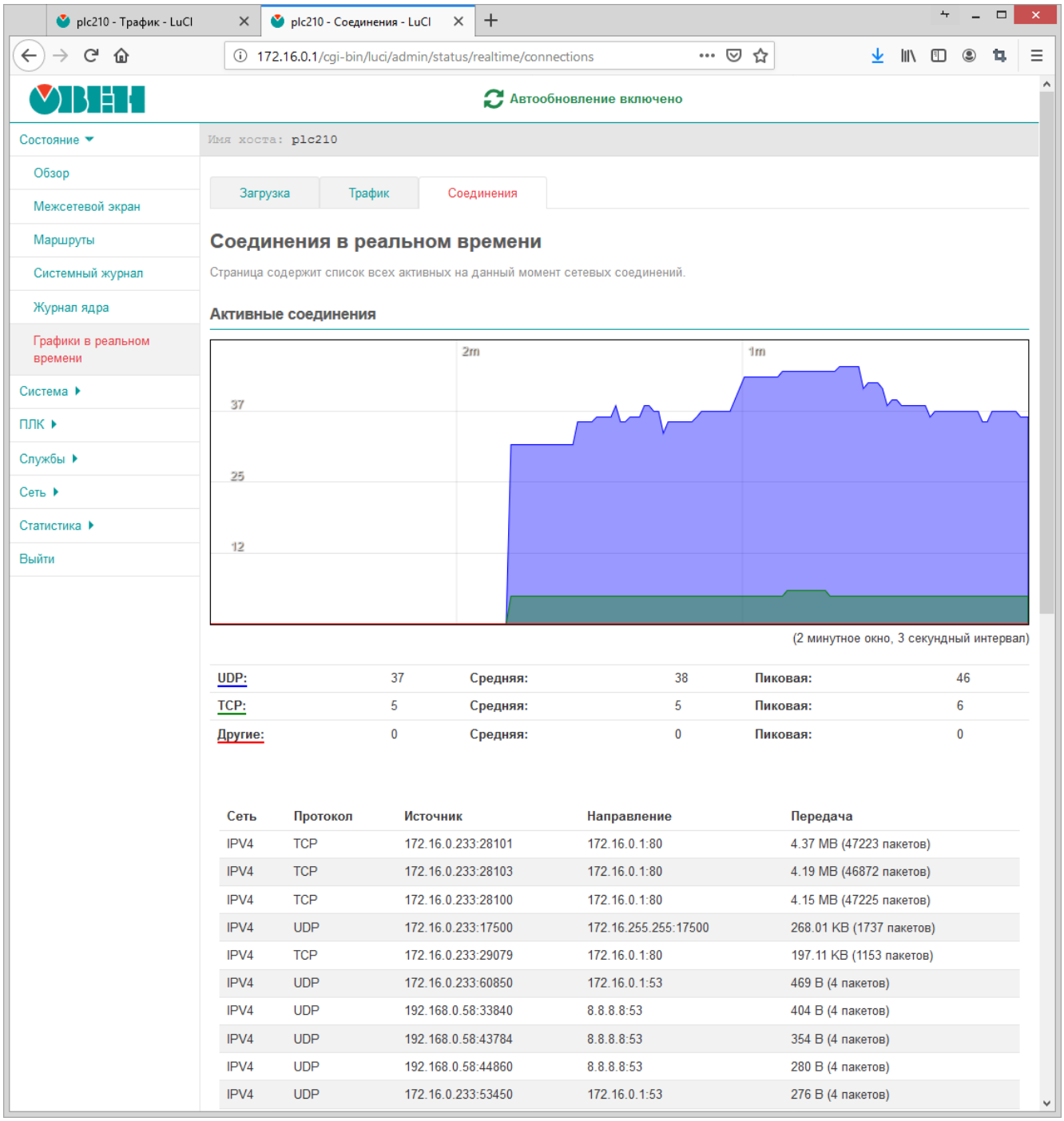


Рис. 3-15: Страница «Графики в реальном времени». График активных соединений

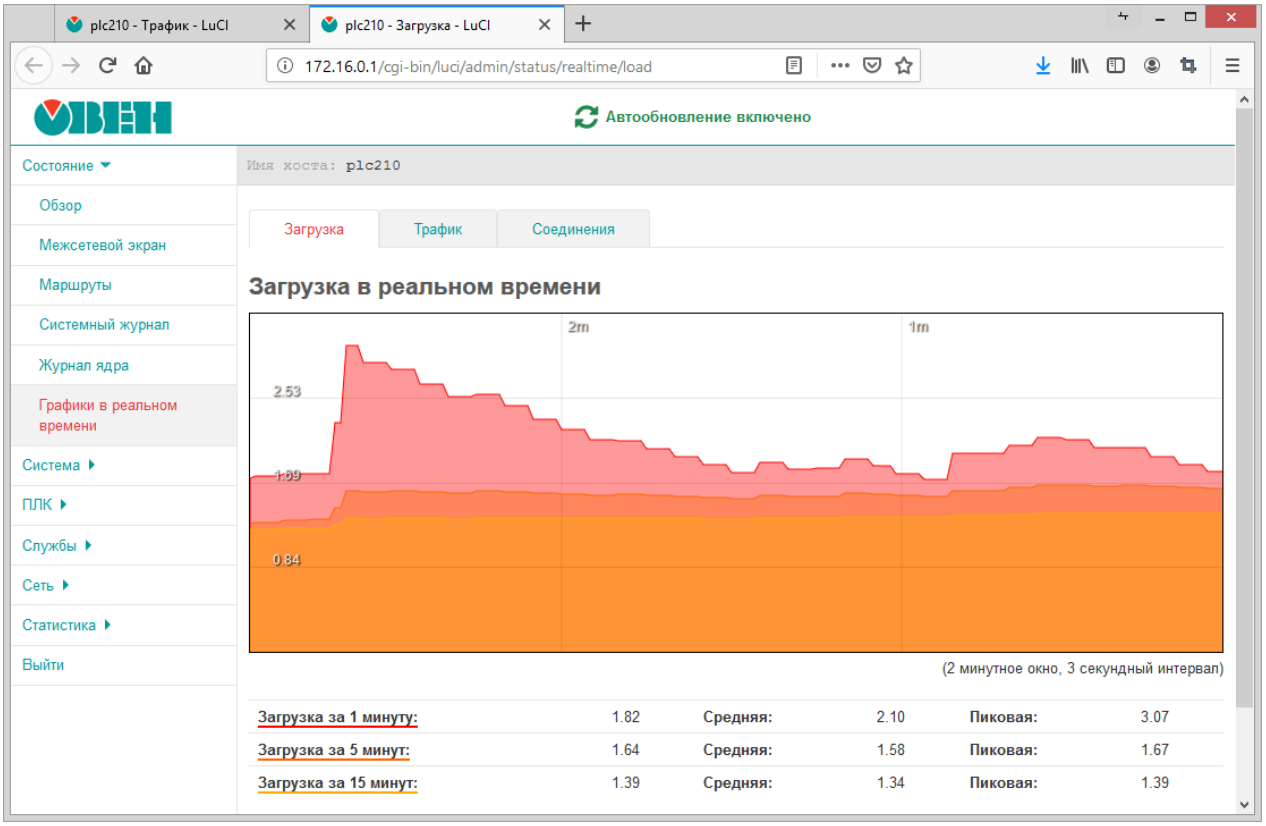


Рис. 3-16: Страница «Графики в реальном времени». График загрузки

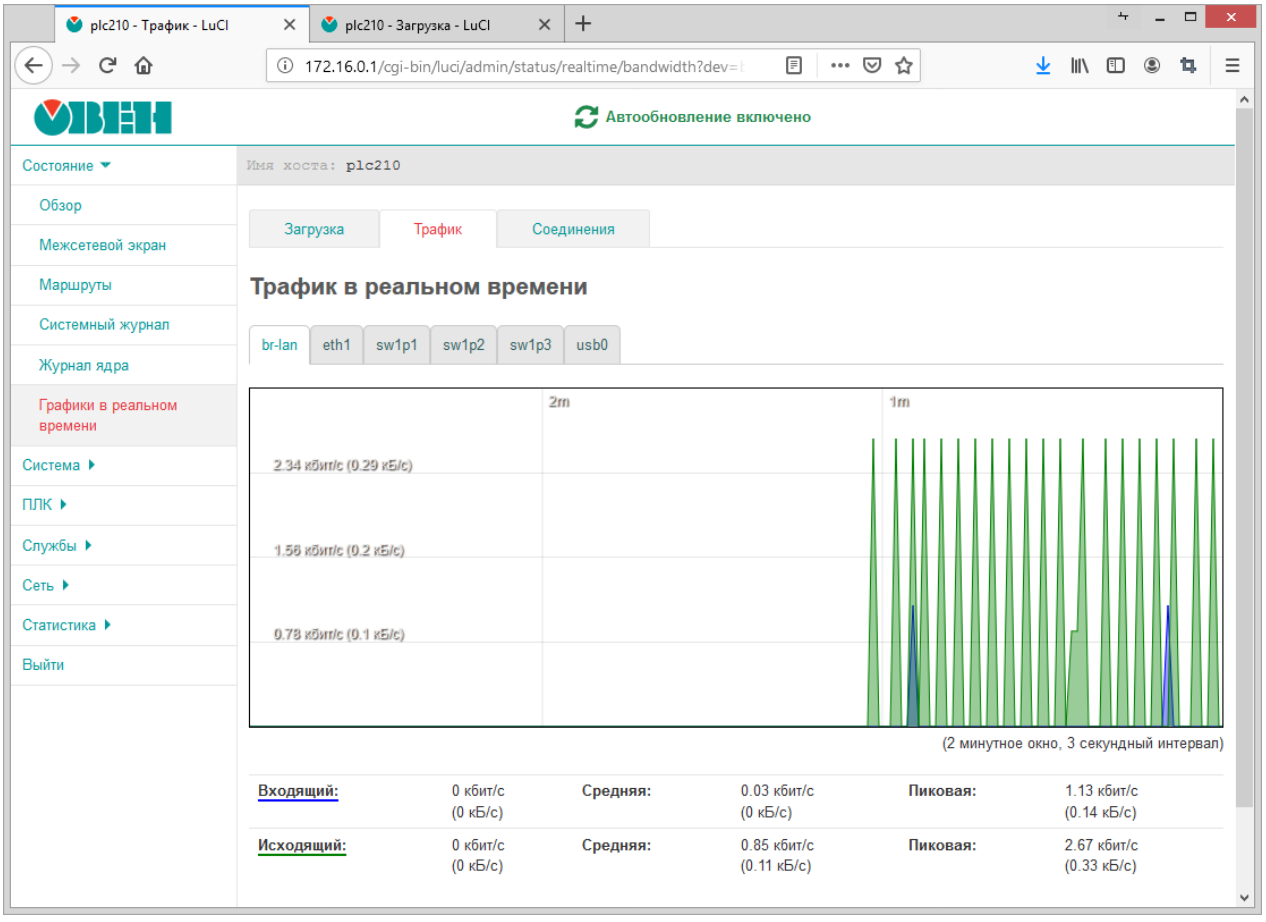


Рис. 3-17: Страница «Графики в реальном времени». График трафика моста «br-lan»

4 Система

4.1 Общие настройки

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

- «Хост» (см. раздел 4.1.1);
- «Журналирование» (см. раздел 4.1.2);
- «Язык» (см. раздел 4.1.3);
- «Дополнительные» (см. раздел 4.1.4).

Внешний вид страницы «Система» показан на рисунке 4-1.

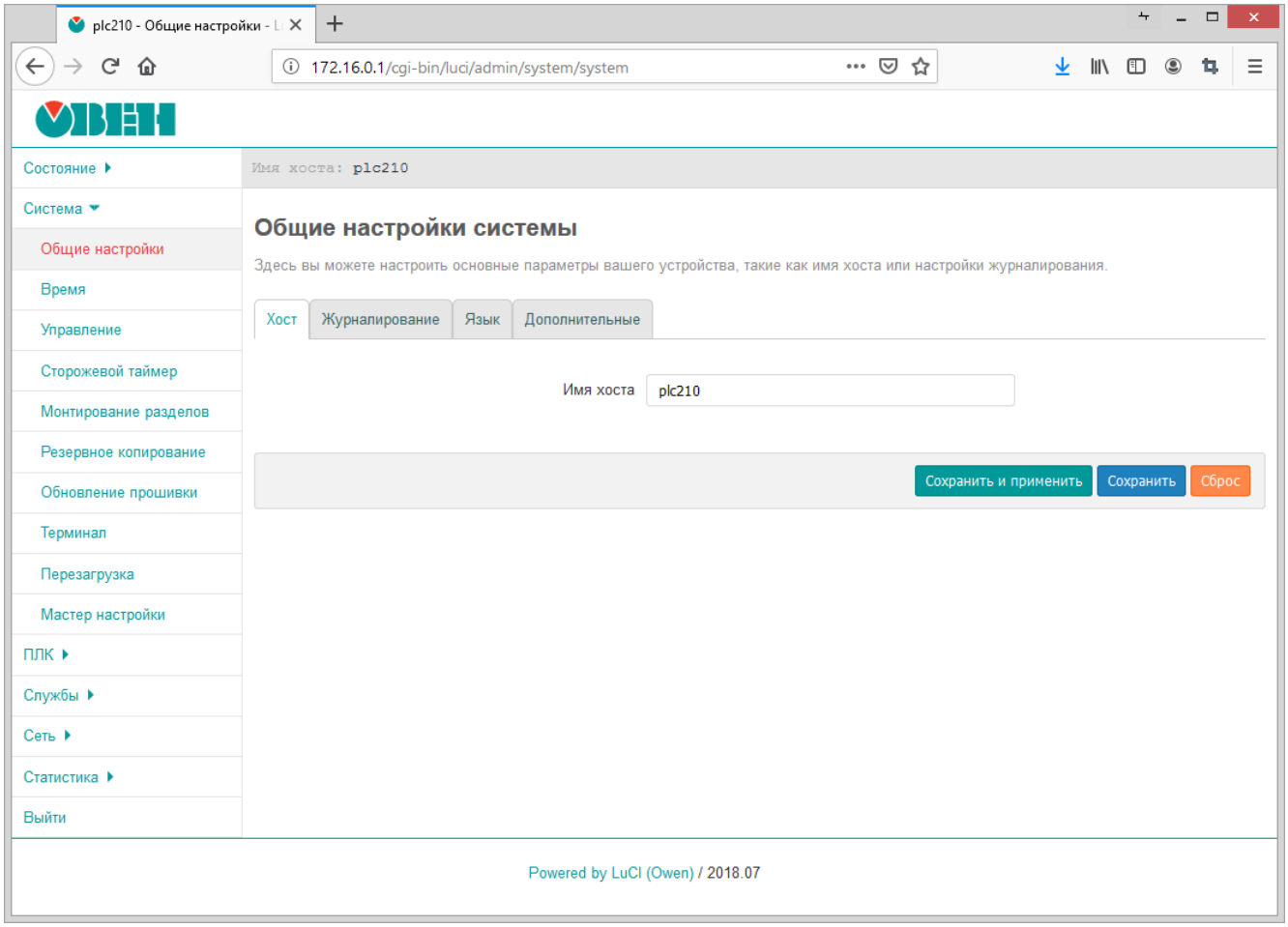


Рис. 4-1: Страница «Общие настройки»

4.1.1 Вкладка «Хост»

Вкладка «Хост» позволяет настроить имя хоста системы.

Внешний вид вкладки «Хост» показан на рисунке 4-2.

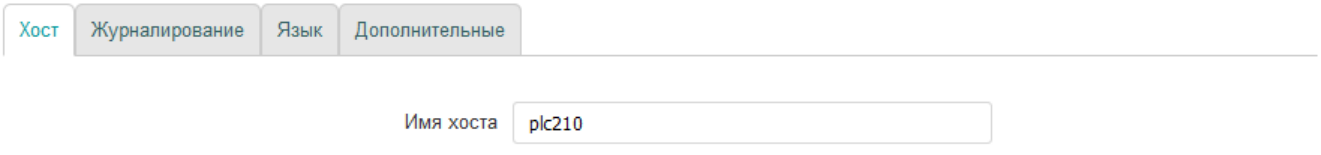


Рис. 4-2: Страница «Общие настройки». Вкладка «Хост»

4.1.2 Вкладка «Журналирование»

Во вкладке «Журналирование» выполняется настройка системной службы журналирования. Внешний вид вкладки «Журналирование» показан на рисунке 4-3.

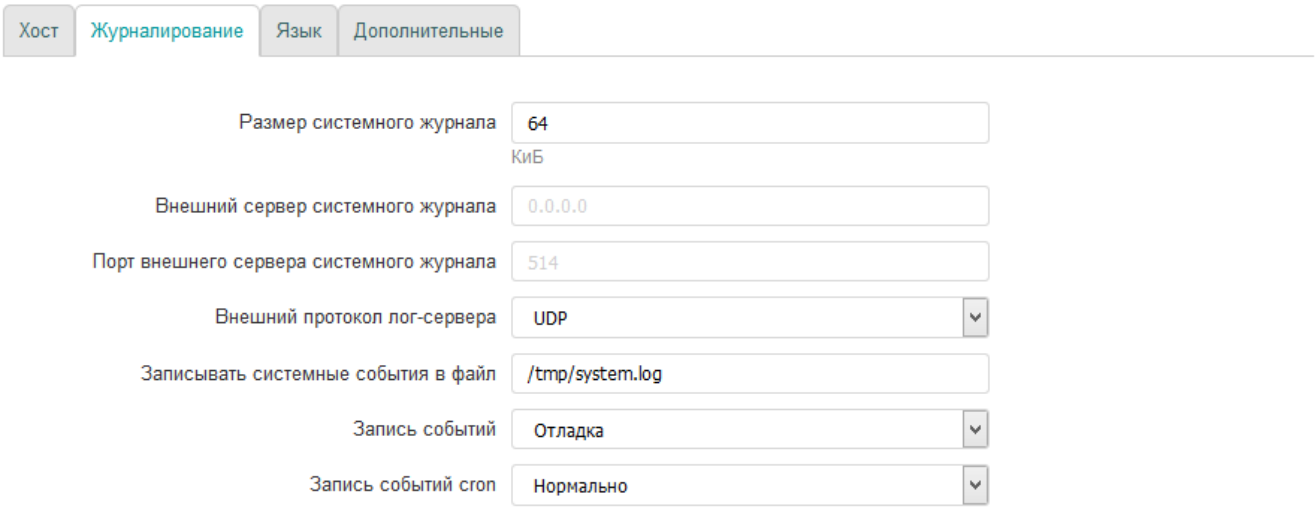


Рис. 4-3: Страница «Система». Вкладка «Журналирование»

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;
- «Внешний протокол лог-сервера» — выбор протокола внешнего сервера журналирования. Доступные протоколы:
  - UDP;
  - TCP;
- «Записывать системные события в файл» — локальный путь к файлу системного журнала;
- «Запись событий» — 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);
- «Запись событий Cron» — выбор уровня событий службы cron для журналирования. Для выбора доступны следующие уровни:
  - отладка (debug);
  - нормально (normal);
  - предупреждение (warning).

4.1.3 Вкладка «Язык»

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

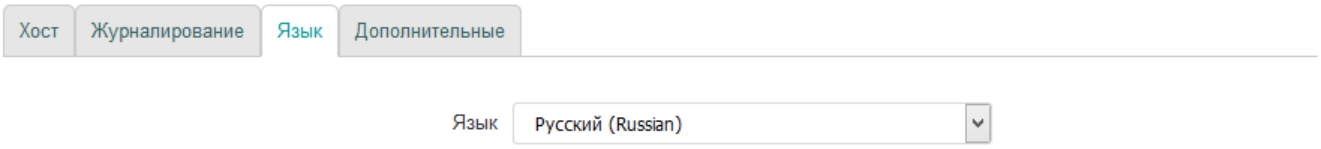


Рис. 4-4: Страница «Система». Вкладка «Язык»

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

4.1.4 Вкладка «Дополнительные»

Во вкладке «Дополнительные» предоставлены дополнительные настройки. Внешний вид вкладки «Дополнительные» показан на рисунке 4-5.

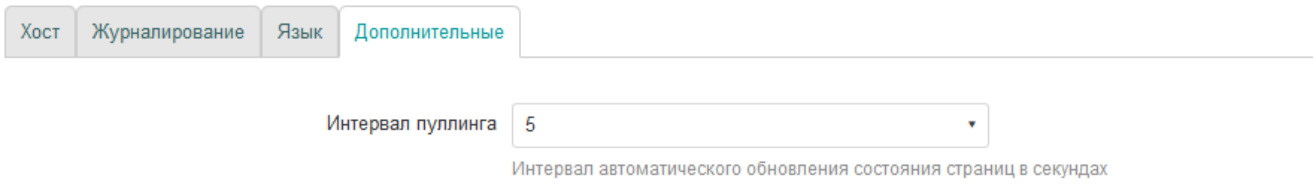


Рис. 4-5: Страница «Система». Вкладка «Дополнительные»

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

4.2 Время

На странице «Время» раздела «Система» размещены настройки локального времени устройства, а также настройки синхронизации времени при помощи службы NTP (см. рисунок 2-6). Внешний вид страницы «Время» показан на рисунке 4-6.

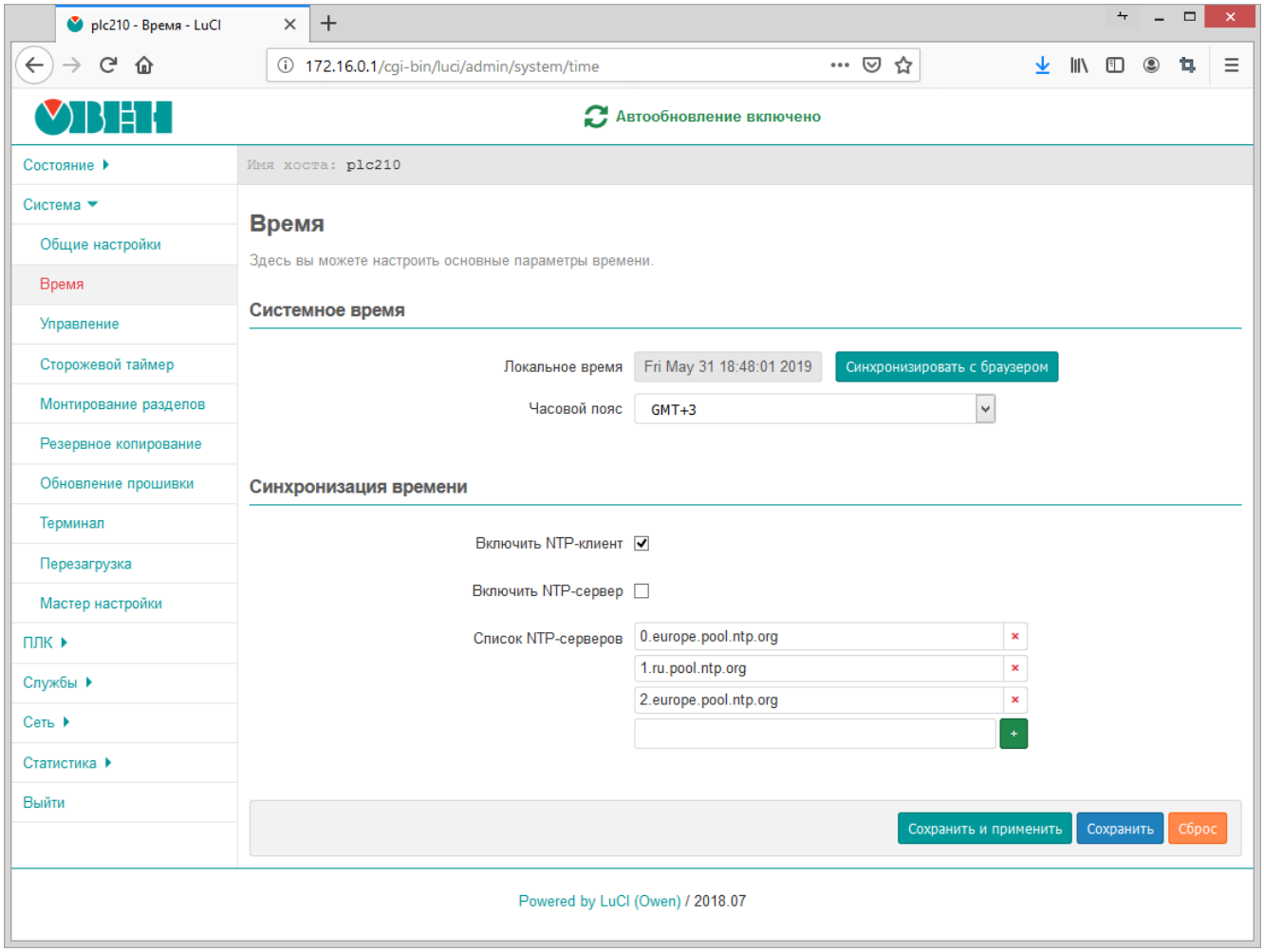


Рис. 4-6: Страница «Время»

В поле «Локальное 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.

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».

4.2.1 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.

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

4.3 Управление доступом

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

- «Пароль устройства» (см. раздел 4.3.1);
- «Доступ по SSH» (см. раздел 4.3.2);
- «SSH-ключи» (см. раздел 4.3.3);
- «RS232» (см. раздел 4.3.4).

4.3.1 Настройка пароля пользователя root

Во вкладке «Пароль устройства» страницы «Управление» (см. рисунок 4-7) 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).

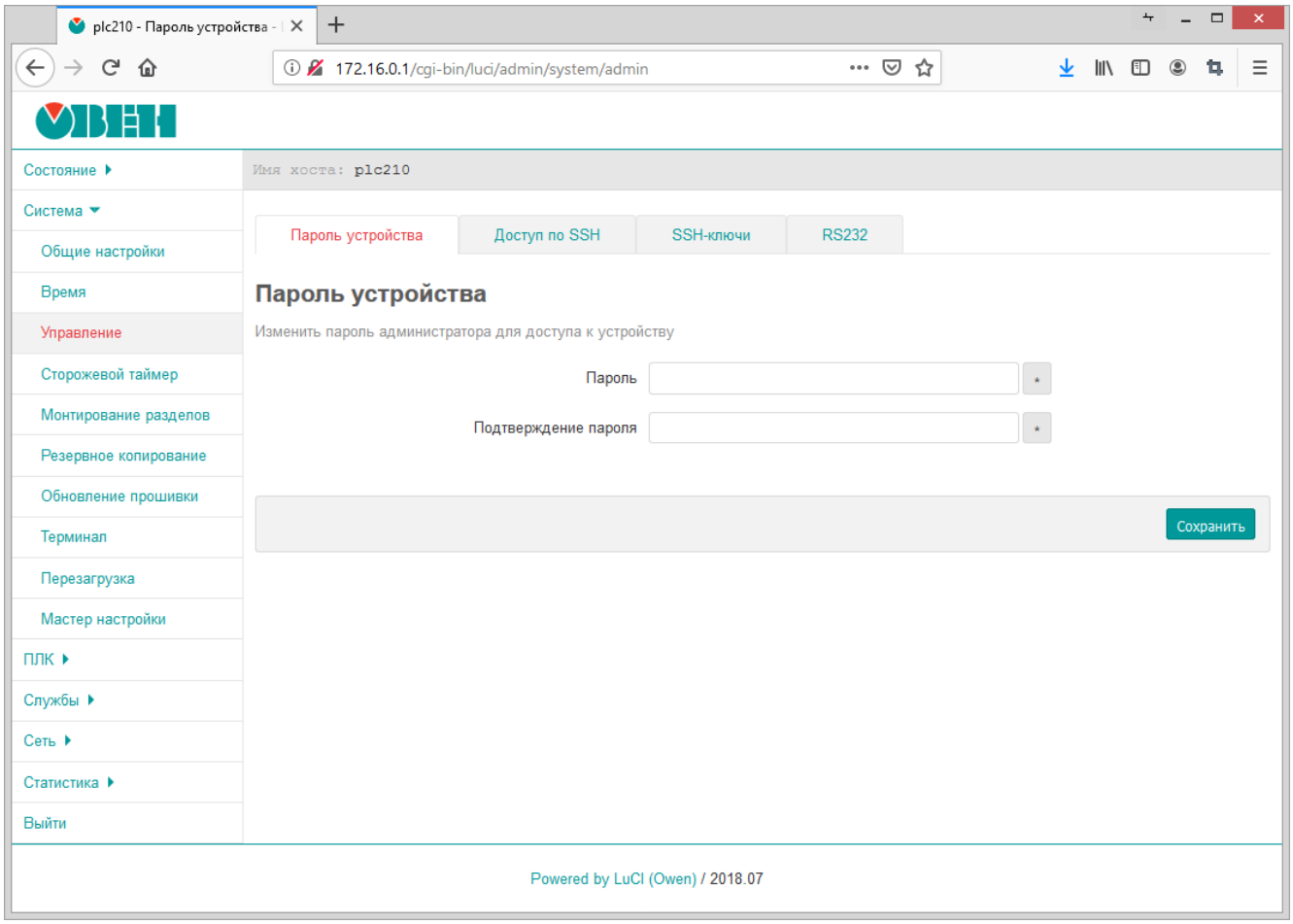


Рис. 4-7: Страница «Управление». Вкладка «Пароль маршрутизатора»

4.3.2 Настройка доступа по SSH

Во вкладке «Доступ по SSH» страницы «Управление» (см. рисунок 4-8) размещены настройки сервера Dropbear, который предоставляет доступ к устройствам по протоколам SSH и SFTP.

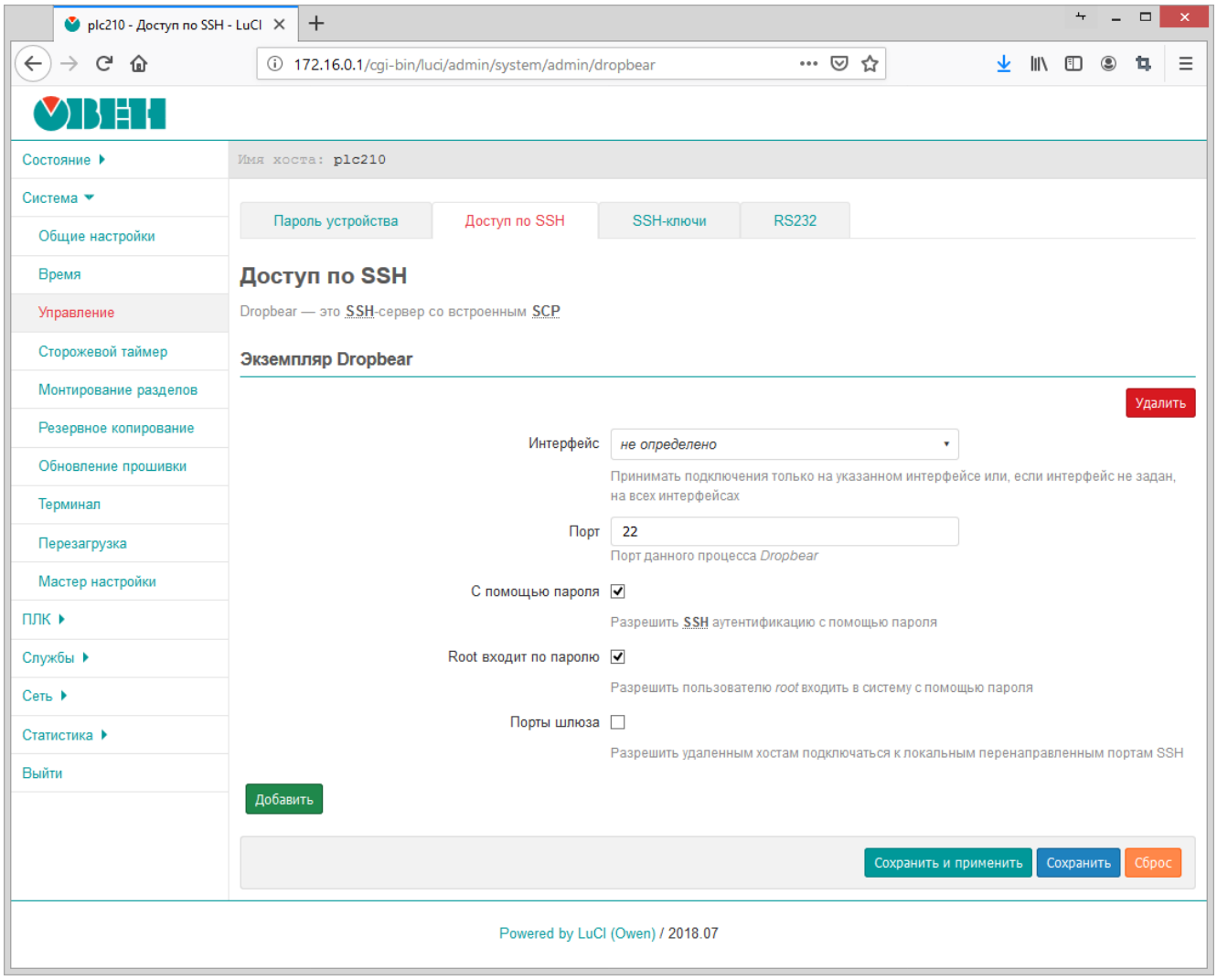


Рис. 4-8: Страница «Управление». Вкладка «Доступ по SSH»

Кнопки «Добавить» 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.

По умолчанию любые входящие подключения из зоны «WAN» запрещены правилами межсетевого экрана (см. раздел 7.5). В связи с этим, несмотря на то, что экземпляр Dropbear настроен на приём подключений на всех сетевых интерфейсах, на сетевых интерфейсах зоны «WAN» подключение к SSH будет невозможно.

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.

4.3.3 SSH-ключи

Во вкладке «SSH-ключи» страницы «Управление» (см. рисунок 4-9) реализована возможность добавления публичных OpenSSH ключей (.pub). Эти SSH ключи используются для выполнения авторизации.

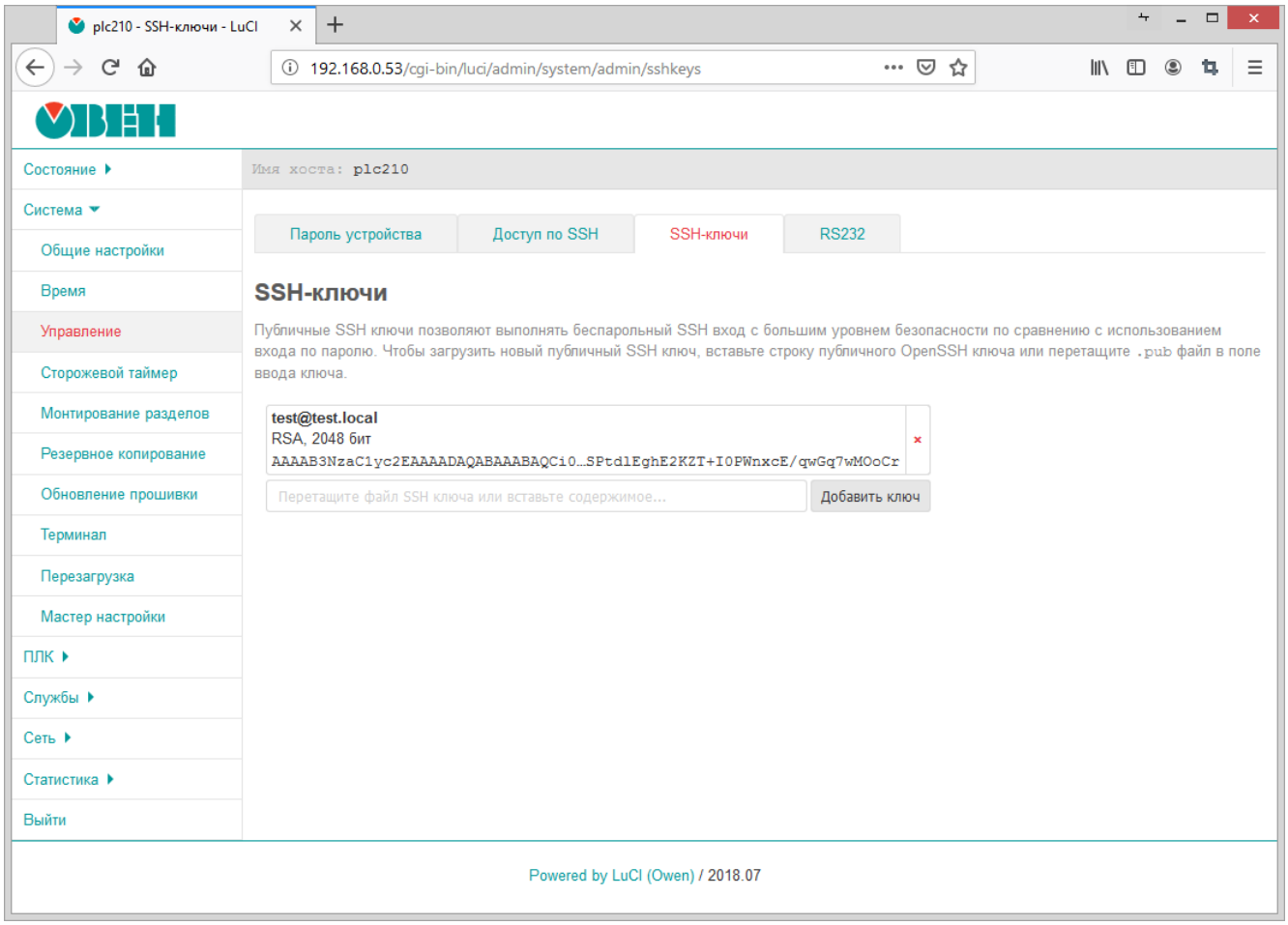


Рис. 4-9: Страница «Управление». Вкладка «SSH-ключи»

Для добавления нового публичного ключа необходимо вставить строку публичного SSH ключа или перетащить «.pub» файл в поле ввода ключа и нажать кнопку «Добавить». Успешно добавленный SSH ключ будет отображён на странице, как показано на рисунке 4-9.

Для удаления ранее добавленного ключа, необходимо нажать кнопку с красным крестиком справа от информации о ключе.

4.3.4 Настройка последовательного порта RS232

Во вкладке «RS232» страницы «Управление» (см. рисунок 4-10) размещены настройки последовательного порта RS232.

Данная вкладка отсутствует в Web-интерфейсе управления контроллеров ПЛК200.

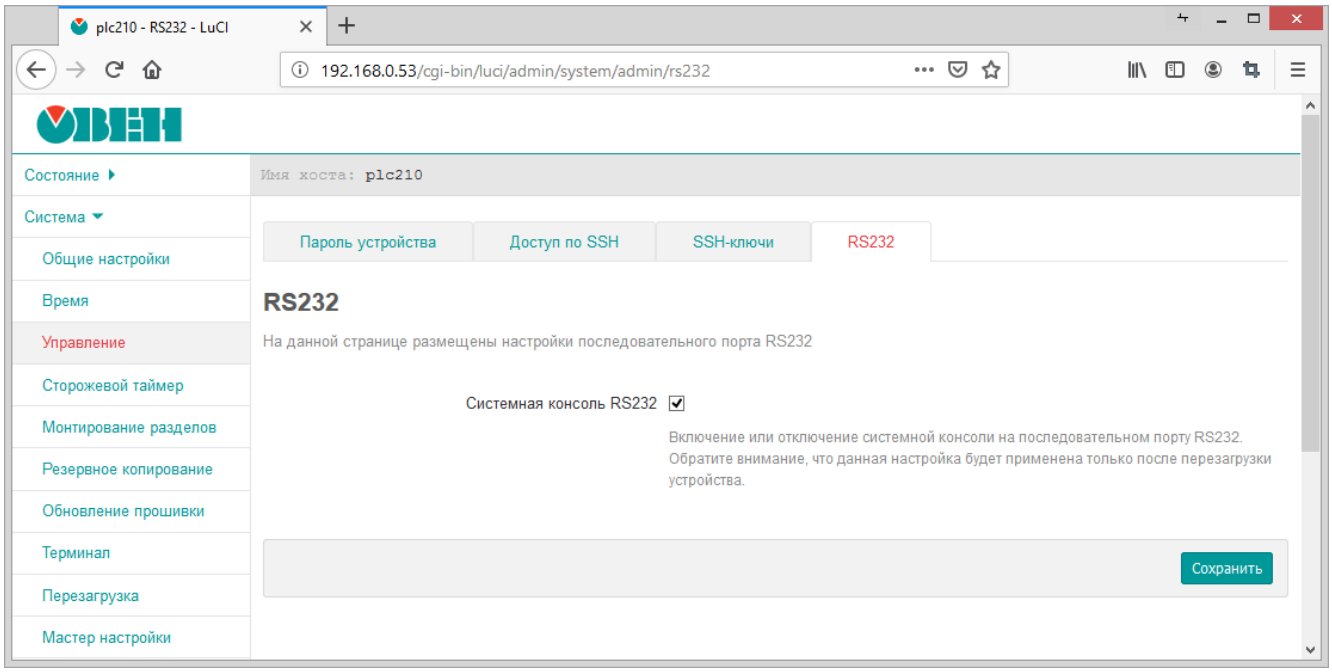


Рис. 4-10: Страница «Управление». Вкладка «RS232»

На вкладке размещена только одна настройка «Системная консоль RS232», которая управляет включением или отключением возможности доступа к системной консоли устройства через последовательный порт RS232.

Изменение настройки «Системная консоль RS232» применяется только после перезагрузки устройства.

Перезагрузка устройства может быть осуществлена на странице «Перезагрузка» раздела «Система» (см. раздел 4.9).

4.4 Сторожевой таймер

На странице «Сторожевой таймер» раздела «Система» расположены настройки службы сторожевого таймера (watchdog). Внешний вид страницы «Сторожевой таймер» показан на рисунке 4-11.

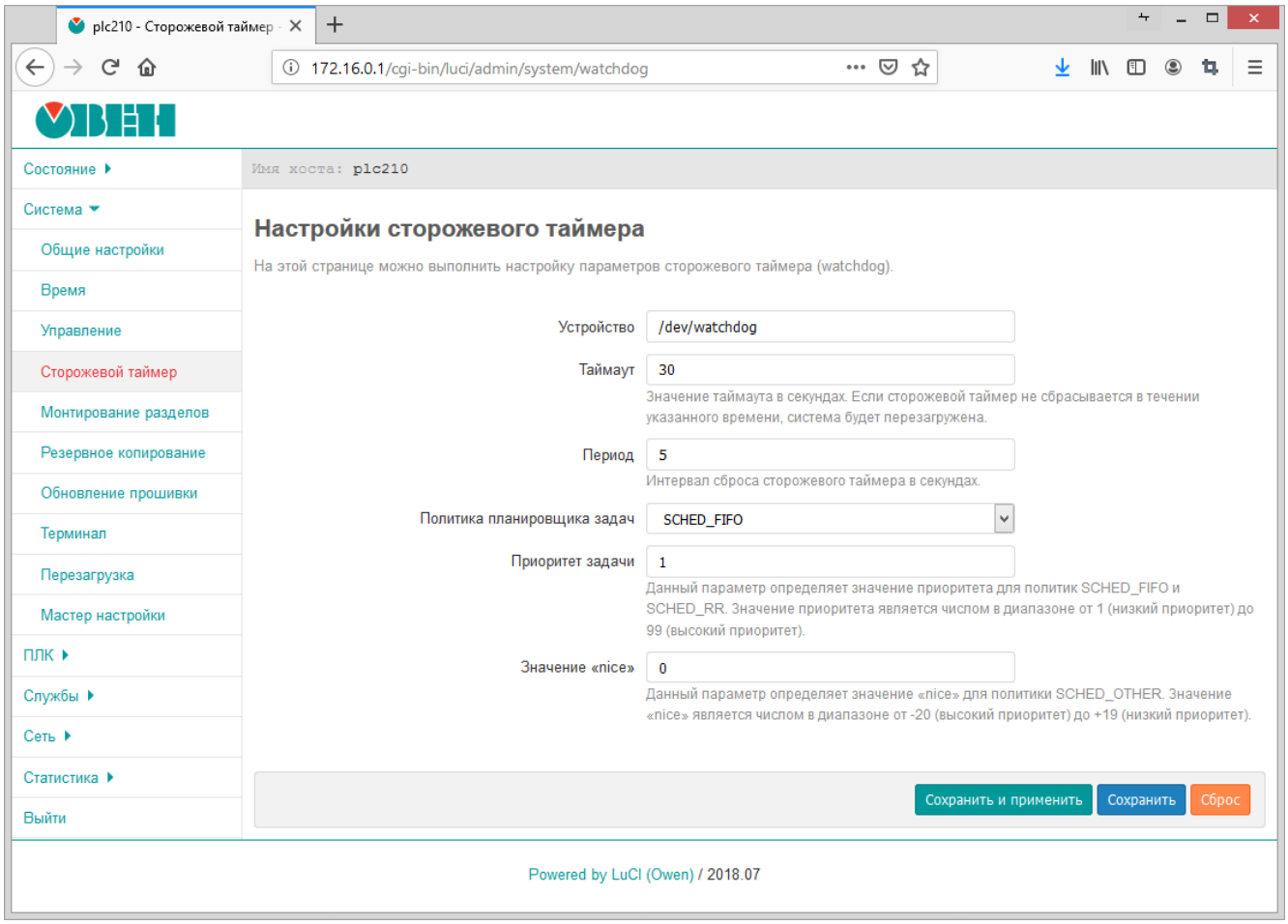


Рис. 4-11: Страница «Сторожевой таймер»

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). Если аппаратный сторожевой таймер не сбрасывается в течение указанного времени, система будет автоматически перезагружена.

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. Данный алгоритм является стандартным алгоритмом диспетчеризации Linux с разделением времени, предназначенным для процессов, не требующих специальных механизмов реального времени со статическими приоритетами;
- «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.

Более подробная информация об алгоритмах диспетчеризации задач Linux приведена в разделе «Scheduling policies» документа [6].

Настройки «Приоритет задачи» и «Значение „nice“» являются параметрами алгоритма диспетчеризации.

Настройка «Приоритет задачи» определяет значение приоритета для алгоритмов «SCHED_FIFO» и «SCHED_RR». Значение приоритета является числом в диапазоне от 1 (самый низкий приоритет) до 99 (самый высокий приоритет).

Настройка «Значение „nice“» определяет значение «nice» для алгоритма «SCHED_OTHER». Значение «nice» является числом в диапазоне от −20 (высокий приоритет) до +19 (низкий приоритет).

Более подробные разъяснения значений параметров приоритета и «nice» приведены в разделах «Scheduling policies» и «The nice value» документа [6].

4.5 Монтирование разделов

Управление монтированием разделов осуществляется на странице «Монтирование разделов» раздела «Система». Внешний вид страницы «Монтирование разделов» показан на рисунке 4-12.

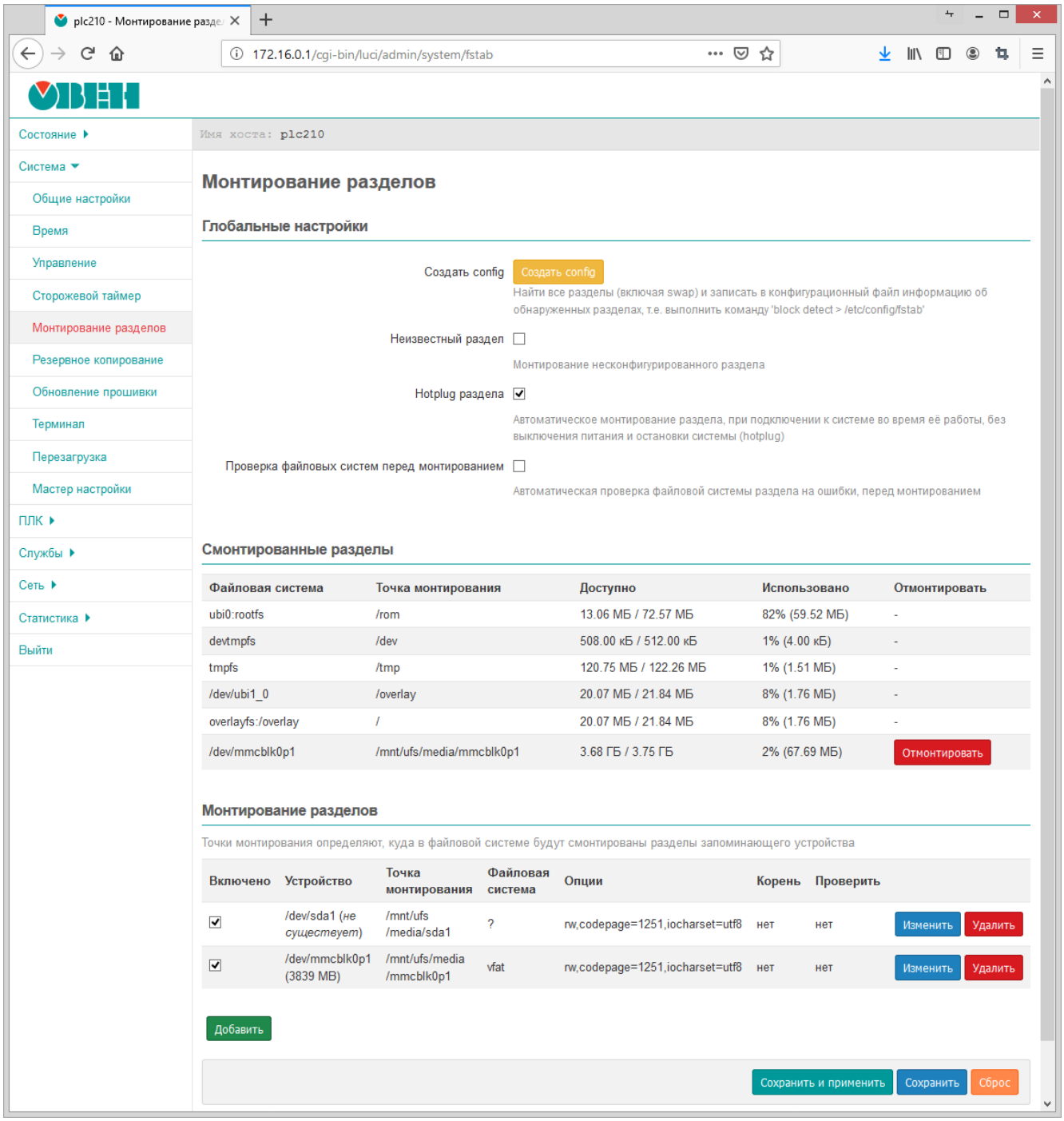


Рис. 4-12: Страница «Монтирование разделов»

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

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

1) «Глобальные настройки» (см. раздел 4.5.1);
2) «Смонтированные разделы» (см. раздел 4.5.2);
3) «Монтирование разделов» (см. раздел 4.5.3).

4.5.1 Подраздел «Глобальные настройки»

В разделе «Глобальные настройки» страницы «Монтирование разделов» (см. рисунок 4-12) представлены глобальные настройки монтирования:

- Кнопка «Создать config» — позволяет создать (переписать) конфигурационный файл «/etc/config/fstab» на основе обнаруженных в системе разделов. Нажатие кнопки «Создать config» равнозначно выполнению в консоли команды:

  ```
  block detect > /etc/config/fstab
  ```

- «Неизвестный раздел» — автоматическое монтирование разделов, даже если эти разделы явно не указаны в конфигурации подраздела «Монтирование разделов» (см. раздел 4.5.3).

  Если опция включена, то неизвестные разделы будут автоматически смонтированы в папку «/mnt/<имя_устройства>».

- «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 раздела «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.

4.5.2 Подраздел «Смонтированные разделы»

В подразделе «Смонтированные разделы» страницы «Монтирование разделов» приведена текущая таблица монтирования (см. рисунок 4-13).

Смонтированные разделы

Файловая система	Точка монтирования	Доступно	Использовано	Отмонтировать
ubi0:rootfs	/rom	13.06 МБ / 72.57 МБ	82% (59.52 МБ)	-
devtmpfs	/dev	508.00 кБ / 512.00 кБ	1% (4.00 кБ)	-
tmpfs	/tmp	120.75 МБ / 122.26 МБ	1% (1.51 МБ)	-
/dev/ubi1_0	/overlay	20.07 МБ / 21.84 МБ	8% (1.76 МБ)	-
overlayfs:/overlay	/	20.07 МБ / 21.84 МБ	8% (1.76 МБ)	-
/dev/mmcblk0p1	/mnt/ufs/media/mmcblk0p1	3.68 ГБ / 3.75 ГБ	2% (67.69 МБ)	Отмонтировать

Рис. 4-13: 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».

4.5.3 Подраздел «Монтирование разделов»

Управление точками монтирования осуществляется в разделе «Монтирование разделов» страницы «Монтирование разделов» (см. рисунок 4-14). В данном разделе можно добавить точки монтирования для пользовательских разделов (например, для USB-накопителей).

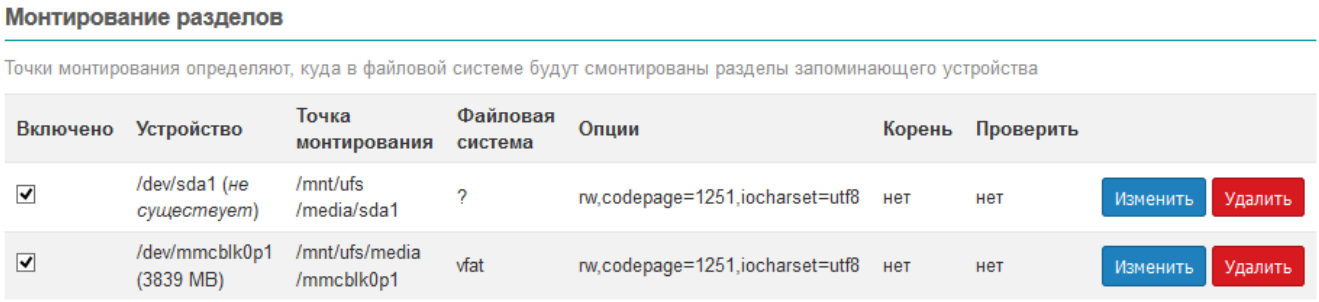


Рис. 4-14: Страница «Монтирование разделов». Управление монтированием пользовательских разделов

В разделе приведена таблица уже созданных точек монтирования пользовательских разделов с их параметрами (см. рисунок 4-14). 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).

  По умолчанию добавлены два устройства, которые при появлении устройства будут автоматически смонтированы:

  - «/dev/sda1» — первый раздел USB-накопителя;
  - «/dev/mmcblc0p1» —- первый раздел MMC-карты памяти.
- «Точка монтирования» — точка монтирования раздела.
- «Файловая система» — файловая система смонтированного раздела.
- «Опции» — дополнительные опции, передаваемые утилите mount [7] при монтировании.
- «Корень» — признак корневой файловой системы. Может принимать значения:
  - «нет» — раздел не является корневым;
  - «да» — раздел является корневым (монтируется в «/»);
  - «overlay» — раздел используется как внешний overlay (монтируется в «/overlay»).
- «Проверить» — признак проверки файловой системы перед монтированием.

4.5.3.1 Редактирование точки монтирования

Для редактирования точки монтирования пользовательского раздела необходимо нажать кнопку «Изменить», расположенную в строке соответствующего раздела таблицы точек монтирования (см. рисунок 4-14). При этом откроется страница редактирования параметров точки монтирования раздела, как показано на рисунке 4-15.

Страница редактирования параметров точки монтирования раздела разделена на вкладки «Общие настройки» (см. рисунок 4-15) и «Дополнительные настройки» (см. рисунок 4-16).

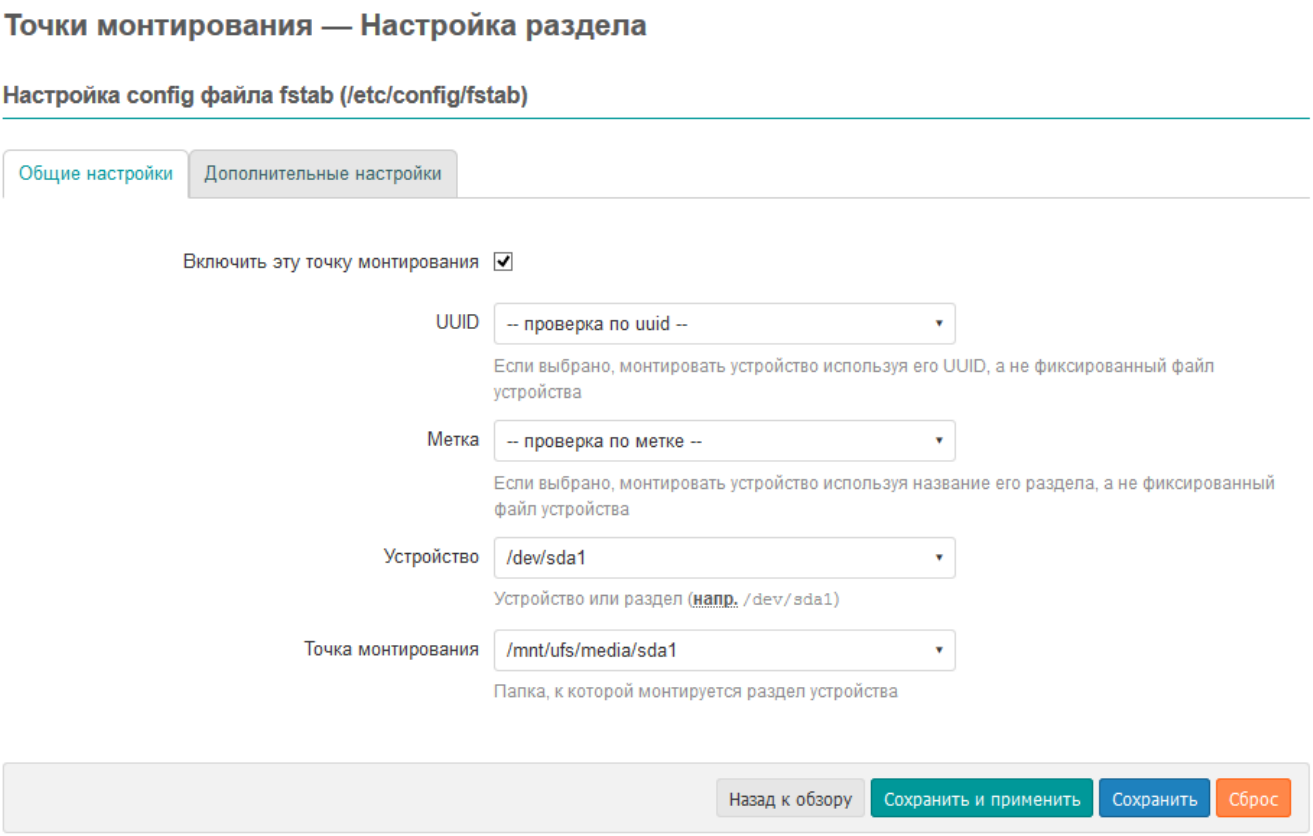


Рис. 4-15: Общие настройки точки монтирования раздела

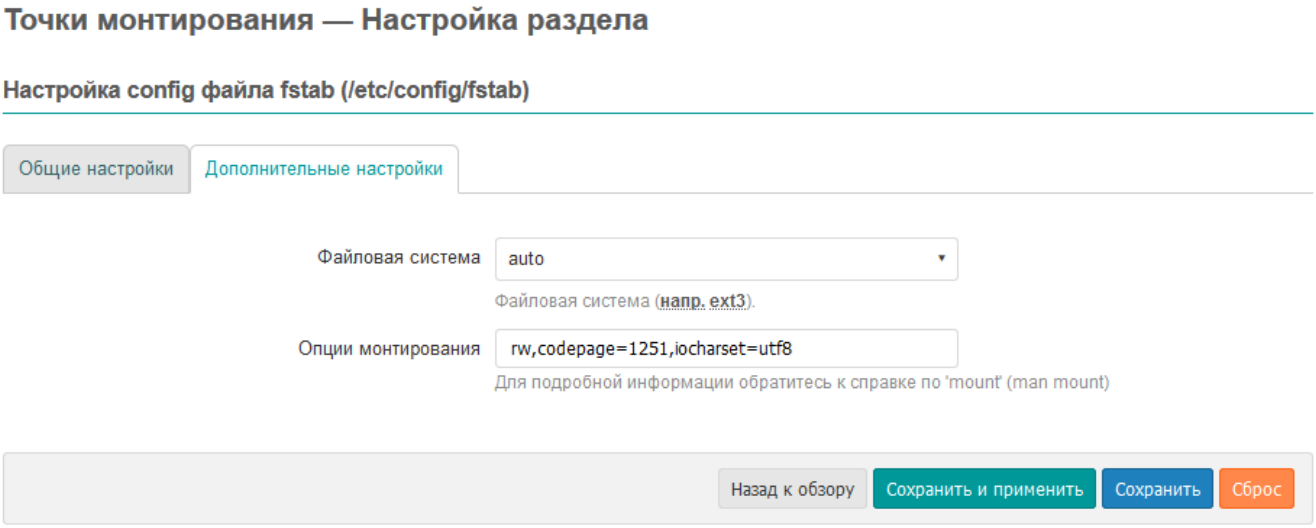


Рис. 4-16: Дополнительные настройки точки монтирования раздела

Во вкладке «Общие настройки» размещены следующие настройки:

- «Включить данную точку монтирования» — 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.
- «Метка» — если выбрана данная опция, то монтируемый раздел будет идентифицироваться по выбранной метке.

  Возможен ручной ввод имени метки или выбор из списка меток всех подключённых разделов на момент загрузки страницы.

- «Устройство» — если выбрана данная опция, то монтируемый раздел будет идентифицироваться по имени устройства.

  Возможен ручной ввод имени устройства или выбор из списка устройств всех подключённых разделов на момент загрузки страницы.

- «Точка монтирования» — определяет точку монтирования раздела.

  Возможен ручной ввод точки монтирования раздела или выбор из следующих вариантов:

  - «Использовать как корень (/)» — использовать раздел как корневой раздел.

    В случае выбора данной опции будет выдано сообщение с рекомендациями, в виде набора команд по подготовке раздела для использования в качестве корневого на основе существующего. Данные команды выглядят следующим образом:

    ```
    mkdir -p /tmp/introot
    mkdir -p /tmp/extroot
    mount --bind / /tmp/introot
    mount имя_устройства_раздела /tmp/extroot
    tar -C /tmp/introot -cvf - . | tar -C /tmp/extroot -xf -
    umount /tmp/introot
    umount /tmp/extroot
    ```

    При вводе данных команд, имя_устройства_раздела следует заменить на реальное имя устройства раздела (например, /dev/sda1).

Во вкладке «Дополнительные настройки» расположены следующие настройки:

- «Файловая система» — выбор файловой системы монтируемого раздела. Доступны следующие варианты:
  - «auto» — автоматическое определение файловой системы раздела (значение по умолчанию);
  - «ext2» — файловая система ext2;
  - «ext3» — файловая система ext3;
  - «ext4» — файловая система ext4;
  - «vfat» — файловая система VFAT;
  - «msdos» — файловая система FAT32;
  - «ntfs» — файловая система NTFS;
  - «пользовательский» — ручной ввод названия файловой системы, которое будет передано утилите mount [7] при монтировании.
- «Опции монтирования» — дополнительные опции, передаваемые утилите mount [7] при монтировании раздела.

Для корректного отображения имён файлов и каталогов с использованием символов кириллицы, необходимо указать следующие опции монтирования:

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

4.5.3.2 Добавление точки монтирования

Для добавления новой точки монтирования пользовательского раздела необходимо нажать кнопку «Добавить», расположенную под таблицей точек монтирования (см. рисунок 4-14).

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 4.5.3.1 данного руководства.

4.5.3.3 Удаление точки монтирования

Для удаления точки монтирования пользовательского раздела необходимо нажать кнопку «Удалить», расположенную в строке соответствующего раздела таблицы точек монтирования (см. рисунок 4-14).

4.6 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 4.6.1. Кроме того, на данной странице можно выполнить сброс устройства к заводским настройкам (factory reset).

Внешний вид страницы «Резервное копирование» показан на рисунке 4-17.

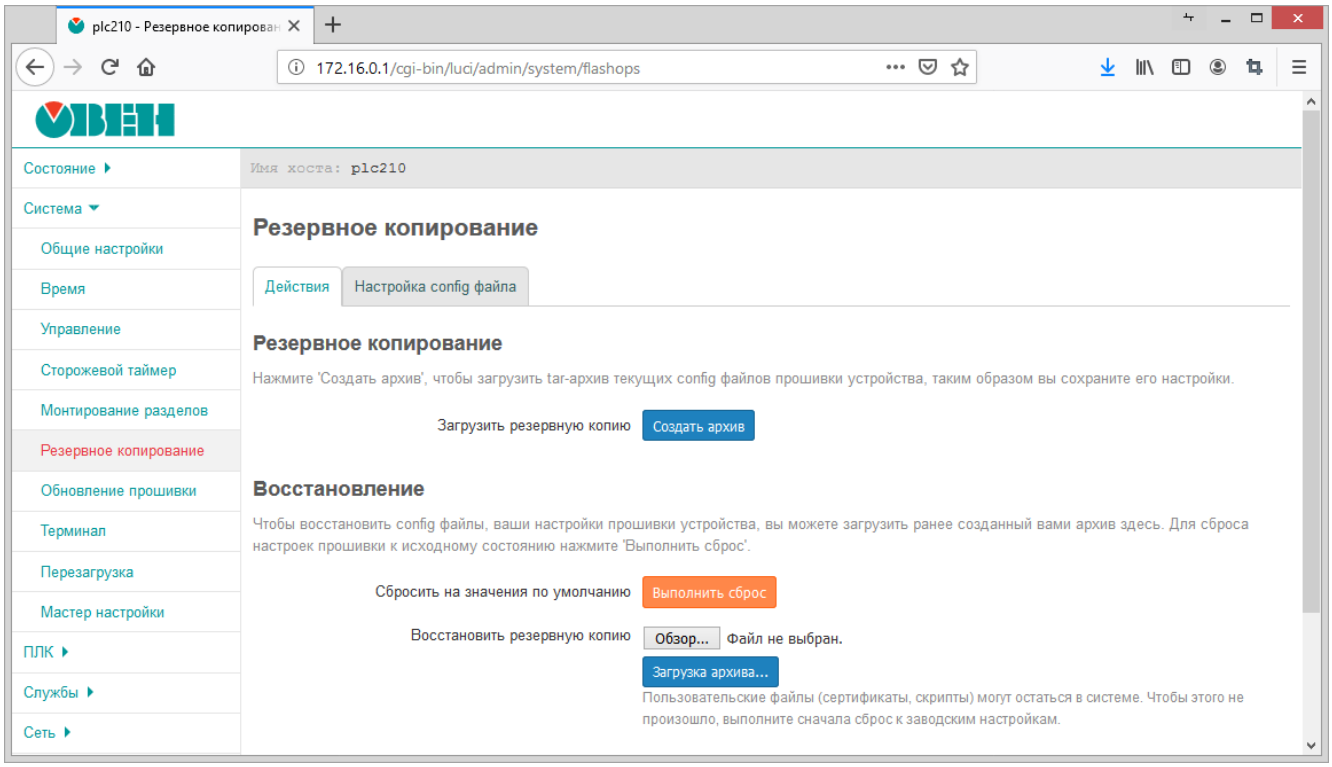


Рис. 4-17: Страница «Резервное копирование»

На странице «Резервное копирование» во вкладке «Действия» (см. рисунок 4-17) представлены следующие элементы управления:

- Кнопка «Создать архив» — позволяет создать (скачать) tar-архив текущих конфигурационных файлов прошивки устройства;
- Кнопка «Обзор...» (в некоторых браузерах может называться «Выберите файл») — позволяет выбрать на локальном компьютере tar-архив резервной копии для последующего восстановления;
- Кнопка «Выполнить сброс» — выполняет сброс устройства к заводским настройкам (factory reset);

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

При выполнении сброса к заводским настройкам будет выполнена перезагрузка устройства.

- Кнопка «Загрузка архива...» — выполняет восстановление настроек из tar-архива, выбранного при помощи кнопки «Обзор...».

При выполнении восстановления резервной копии настроек будет выполнена перезагрузка устройства.

При выполнении восстановления резервной копии некоторые пользовательские файлы (например сертификаты, скрипты) могут остаться в системе. Чтобы этого не произошло, выполните перед восстановлением резервной копии сброс к заводским настройкам.

4.6.1 Настройка списка файлов резервной копии

На вкладке «Настройка config файла» страницы «Резервное копирование» можно выполнить настройку списка файлов, которые будут сохраняться в резервной копии. Внешний вид вкладки «Настройка config файла» показан на рисунке 4-18.

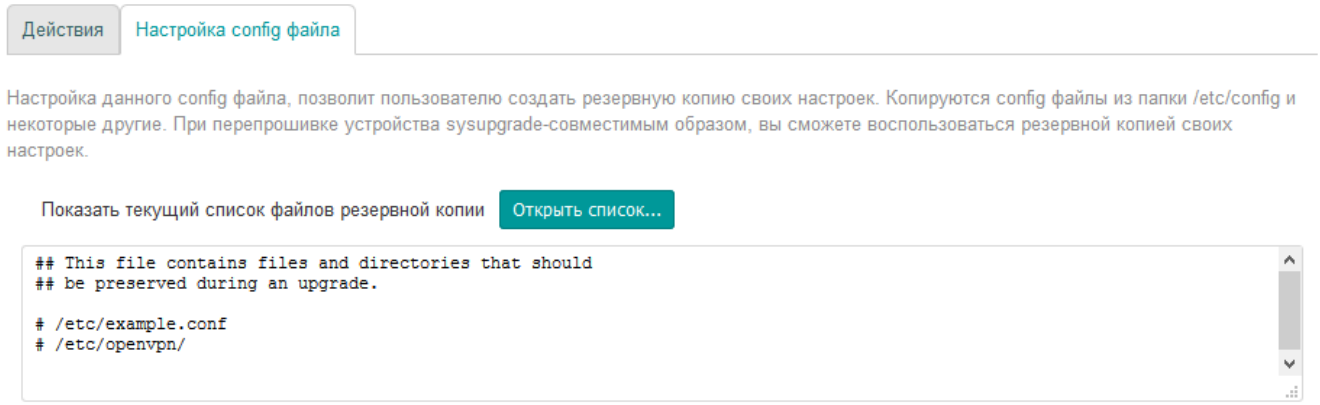


Рис. 4-18: Страница «Резервное копирование». Вкладка «Настройка config файла»

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 «Открыть список...» будет отображён полный список файлов, которые будут сохранены в резервную копию с учётом конфигурационного файла «/etc/sysupgrade.conf» (см. рисунок 4-19).

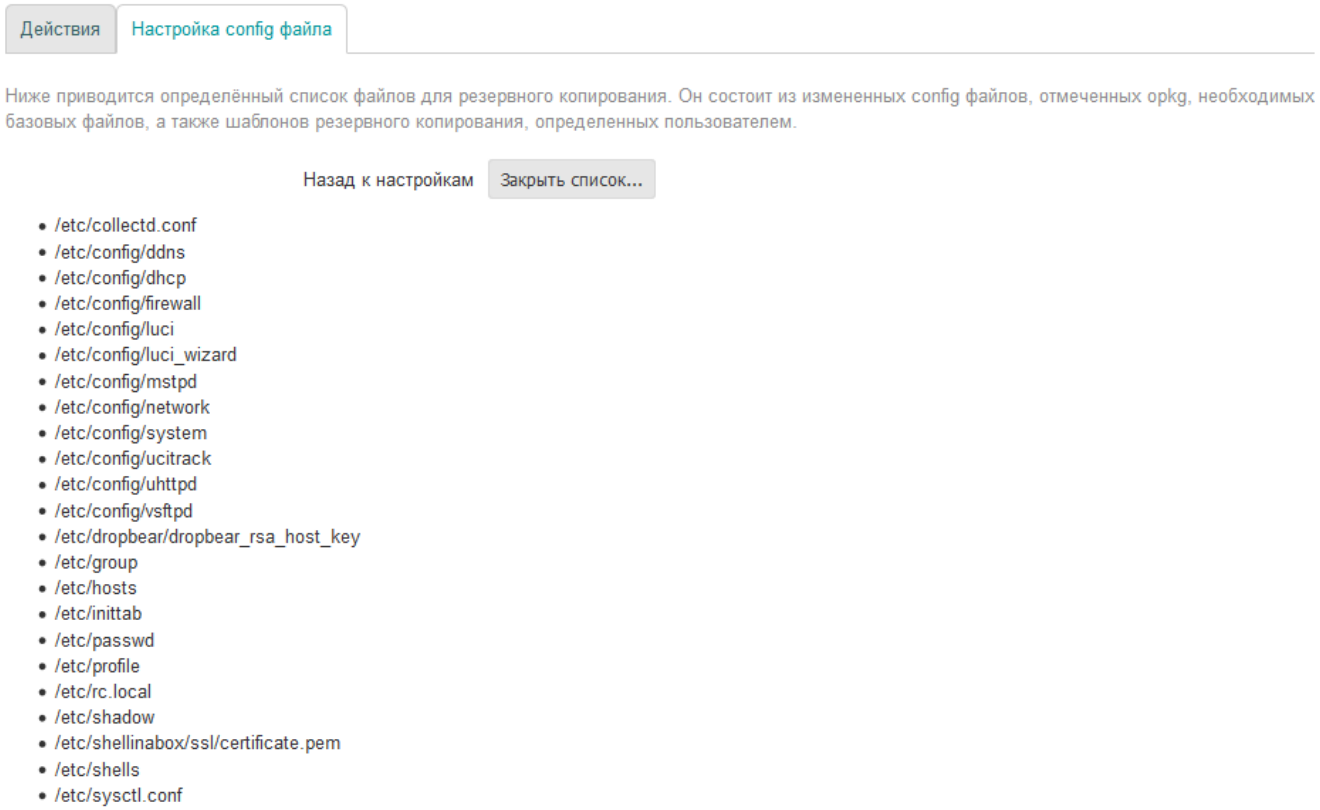


Рис. 4-19: Страница «Резервное копирование». Вкладка «Настройка config файла». Список файлов

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

4.7 Обновление прошивки

На странице «Обновление прошивки» раздела «Система» расположен функционал обновления прошивки устройства. Внешний вид страницы «Обновление прошивки» показан на рисунке 4-20.

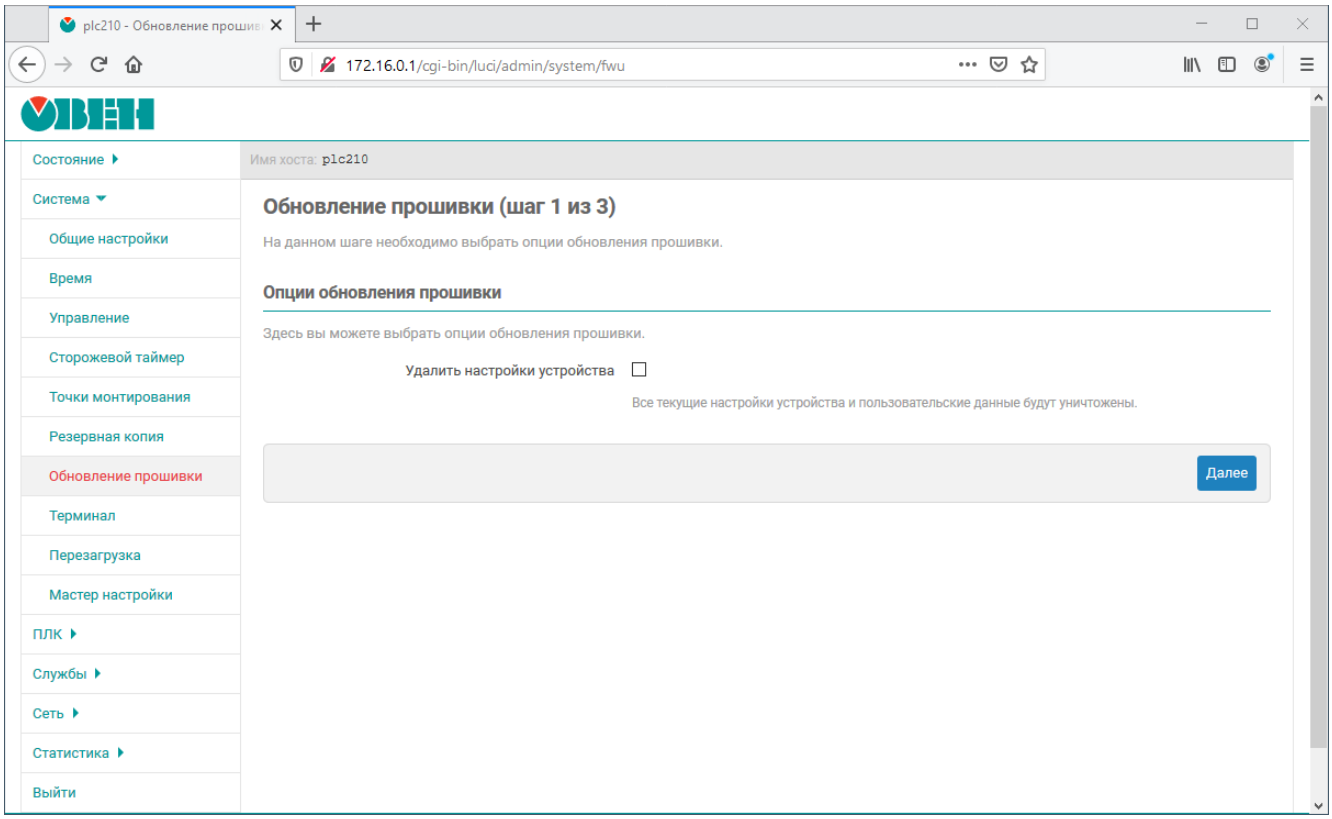


Рис. 4-20: Страница «Обновление прошивки»

Вся процедура обновления прошивки устройства состоит из 3-х шагов:

1) Выбор опций обновления прошивки;
2) Загрузка образа прошивки на устройство;
3) Выполнение обновления прошивки устройства и перезагрузки.

4.7.1 Выбор опций обновления прошивки

При выполнении обновления прошивки устройства можно выполнить автоматический сброс всех настроек к заводскому состоянию. Для выполнения сброса предназначена настройка «Удалить настройки устройства» (см. рисунок 4-20). Если данная настройка включена, то при выполнении обновления прошивки все пользовательские настройки и данные на устройстве будут уничтожены. Если же настройка не включена

Процедуры ручного создания и восстановления резервной копии подробно рассматриваются в разделе 4.6 данного документа. При обновлении прошивки устройства, для создания и восстановления резервной копии используются те же возможности.

4.7.2 Загрузка образа прошивки

Внешний вид страницы второго шага, на котором выполняется загрузка файла образа прошивки, показан на рисунке 4-21.

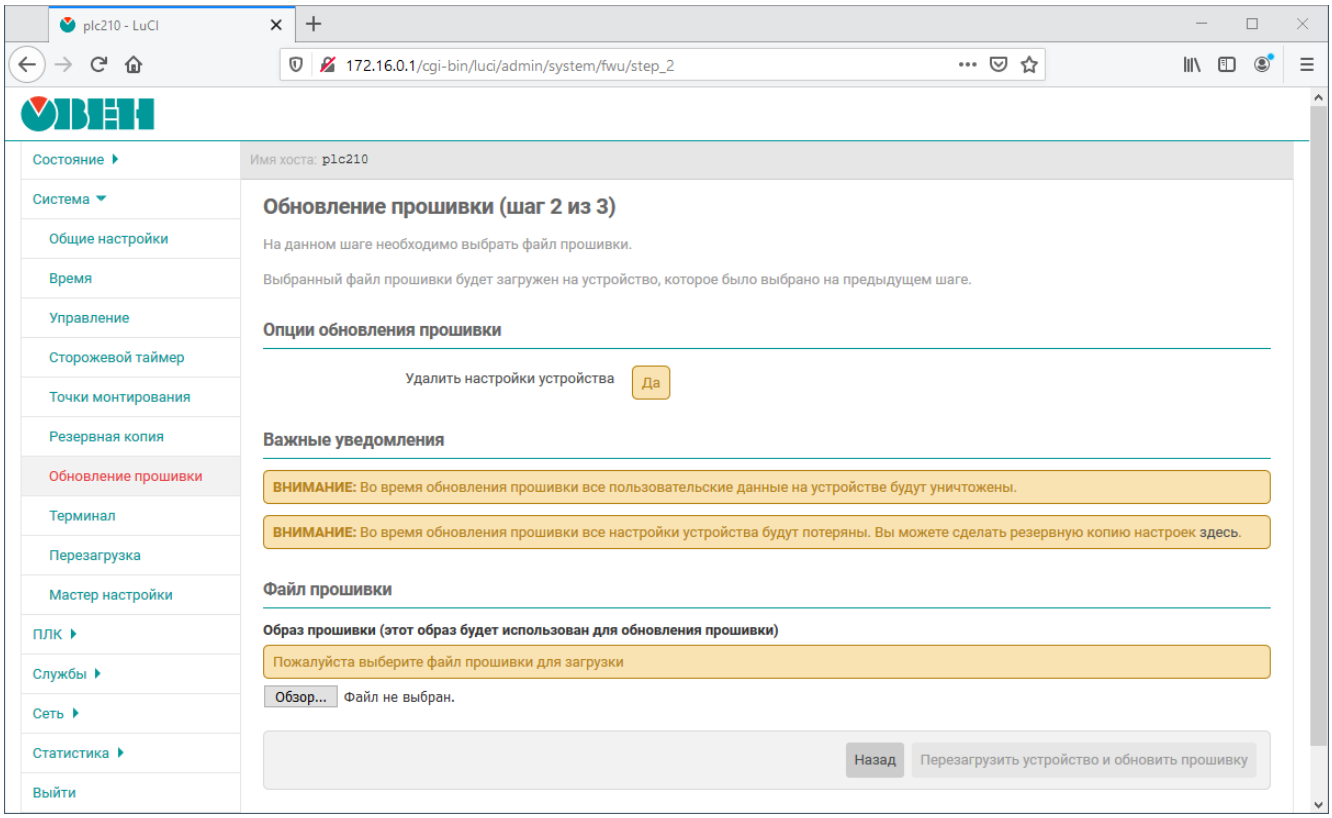


Рис. 4-21: Страница «Обновление прошивки». Загрузка файла прошивки

В подразделе «Опции обновления прошивки» отображаются значения выбранных опций на предыдущем шаге.

В подразделе «Важные уведомления» отображаются различные важные сообщения, которые могут зависеть от выбранных дополнительных опций и т.п. Например, в случае включённой опции «Удалить настройки устройства» данный подраздел будет выглядеть так, как показано на рисунке 4-22.

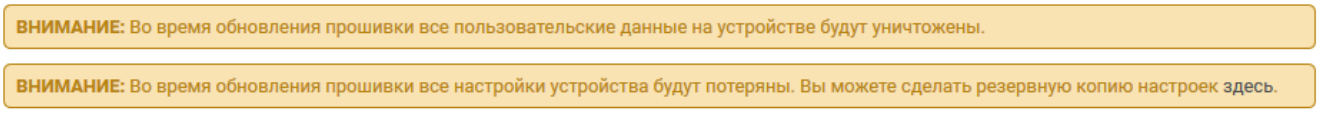


Рис. 4-22: Страница «Обновление прошивки». Область важных уведомлений

При отсутствии уведомлений подраздел «Важные уведомления» не отображается.

В подразделе «Файл прошивки» отображается информация о загруженном файле образа прошивки. Если на текущий момент нет загруженного файла образа прошивки, то подраздел «Файл прошивки» будет выглядеть, как показано на рисунке 4-23.

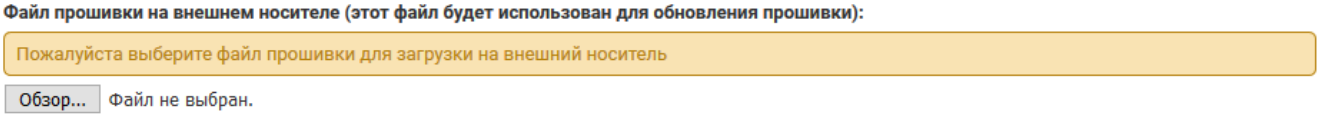


Рис. 4-23: Страница «Обновление прошивки». Отсутствие файла прошивки на внешнем устройстве

В этом случае необходимо выбрать файл образа прошивки для загрузки при помощи кнопки «Обзор...». Во время выполнения загрузки файла образа прошивки на внешнее устройство, подраздел «Файл прошивки» будет выглядеть так, как показано на рисунке 4-24.

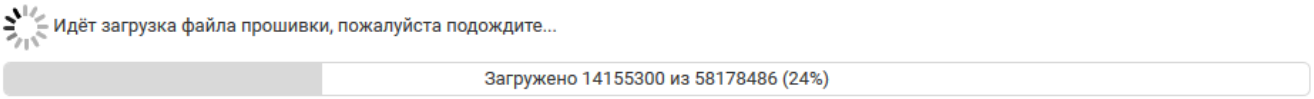


Рис. 4-24: Страница «Обновление прошивки». Процесс загрузки файла прошивки

Если загружен файл образа прошивки, который не предназначен для прошивки на устройстве ПЛК210, то подраздел «Файл прошивки» будет выглядеть так, как показано на рисунке 4-25. В этом случае необходимо выбрать новый файл образа прошивки для загрузки на внешнее устройство при помощи кнопки «Обзор...».

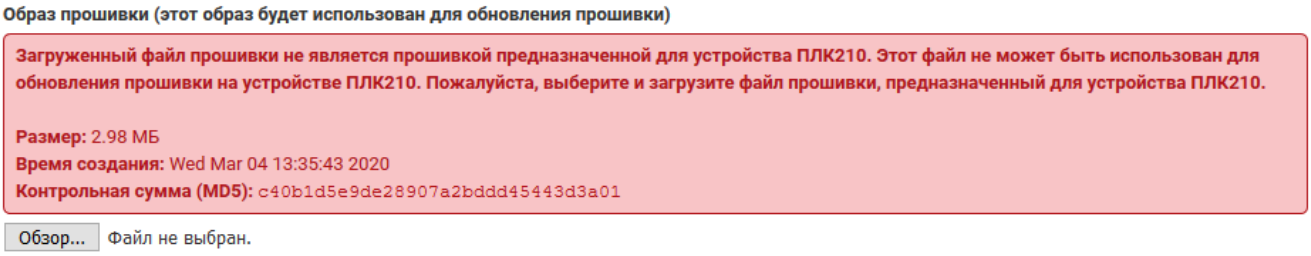


Рис. 4-25: Страница «Обновление прошивки». Некорректный файл прошивки на внешнем устройстве

Если же загружен файл образа прошивки, который предназначен для прошивки на устройстве ПЛК210, то подраздел «Файл прошивки» будет выглядеть так, как показано на рисунке 4-26.

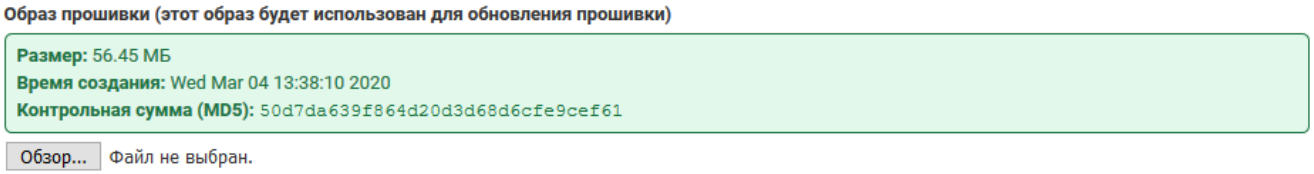


Рис. 4-26: Страница «Обновление прошивки». Корректный файл прошивки на внешнем устройстве

В подразделе «Файл прошивки» для загруженного файла образа прошивки на внешнее устройство выводится следующая дополнительная информация:

- «Размер» — размер файла образа прошивки на внешнем устройстве;

  «Время создания» — дата и время создания файла образа прошивки на внешнем устройстве;

  «Контрольная сумма (MD5)» — контрольная сумма файла образа прошивки на внешнем устройстве, рассчитанная алгоритмом MD5.

4.7.3 Перезагрузка и обновление прошивки

При наличии на внешнем устройстве корректного файла образа прошивки, предназначенного для прошивки на устройстве ПЛК210, кнопка «Перезагрузить устройство и обновить прошивку» становится активна.

Нажатие этой кнопки начинает процедуру обновления прошивки устройства. При этом страница «Обновление прошивки» будет выглядеть, как показано на рисунке 4-27.

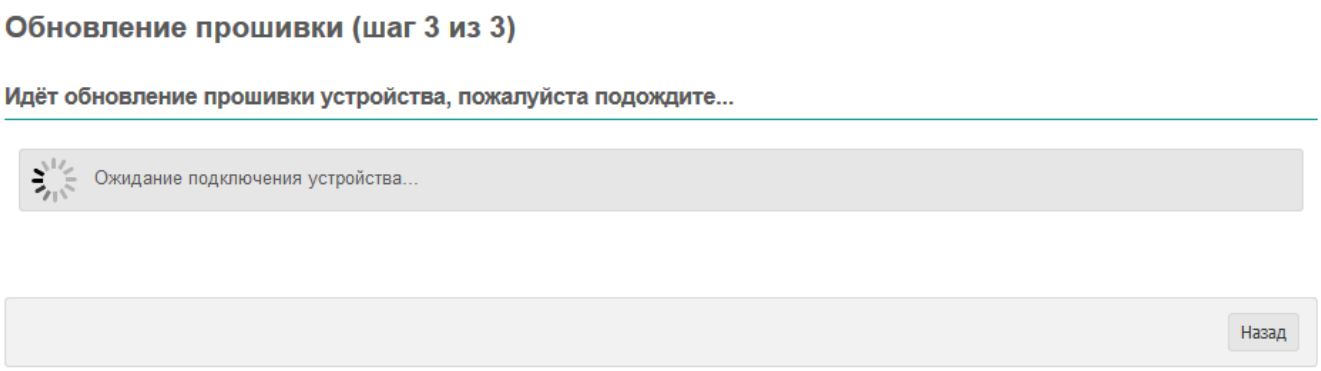


Рис. 4-27: Страница «Обновление прошивки». Обновление прошивки устройства

В том случае, если обновление прошивки выполняется с выключенной настройкой «Удалить настройки устройства», то после обновления прошивки и успешной загрузки устройства произойдёт автоматический переход на страницу аутентификации (см. раздел 1.1). Если дополнительная настройка «Удалить настройки устройства» включена, то возможно потребуется подключение к устройству в ручном режиме, так как IP-адрес устройства после обновления прошивки может быть изменён.

Процедура обновления прошивки устройства может занимать до 10 минут;

Запрещается отключать внешнее устройство, используемое для временного сохранения файла образа прошивки, до полного окончания процедуры обновления прошивки;

Запрещается отключать питание устройства до полного окончания процедуры обновления прошивки.

4.8 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 4-28.

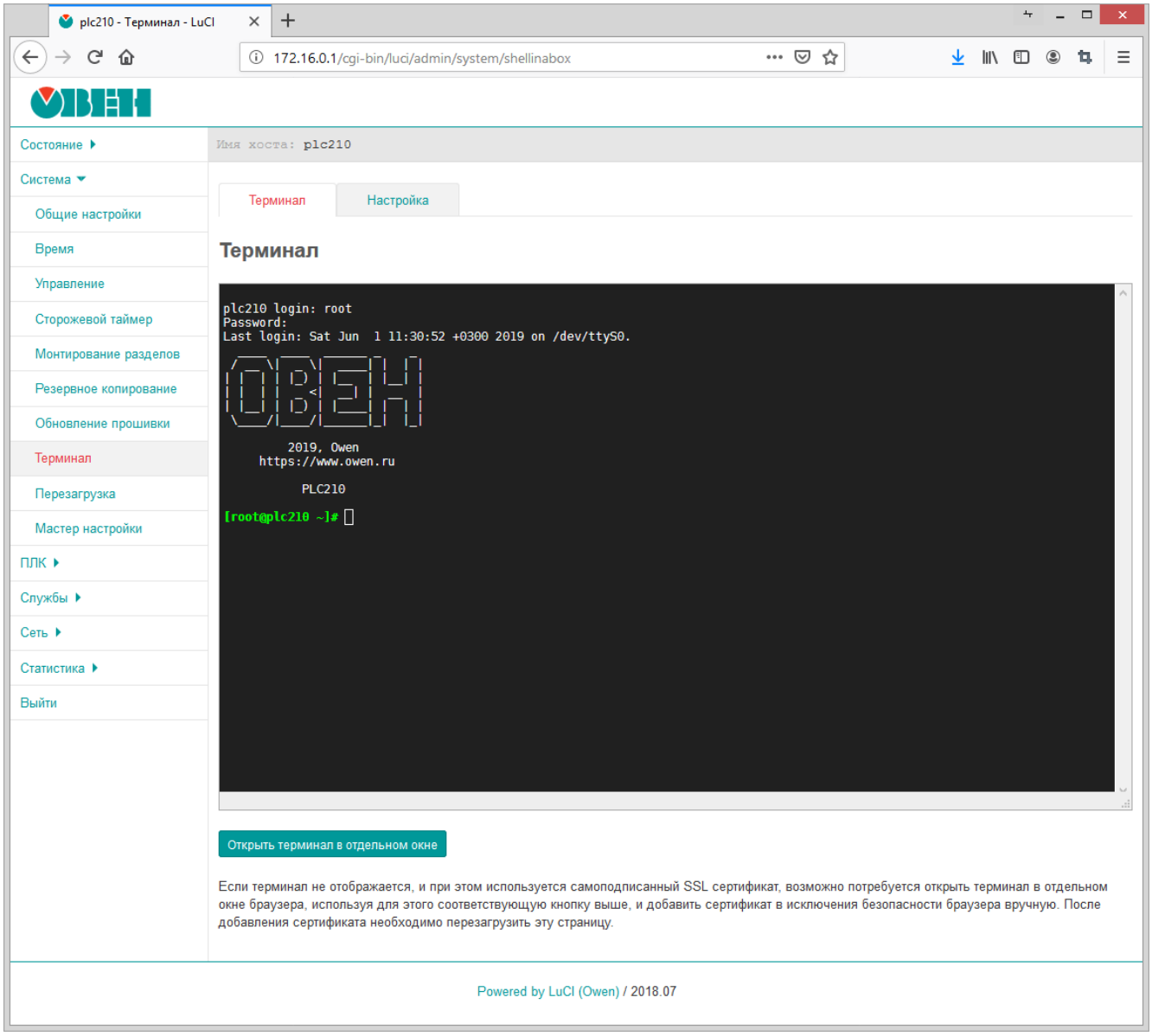


Рис. 4-28: Страница «Терминал»

При использовании самоподписанного SSL сертификата область терминала на странице «Терминал» может выглядеть так, как показано на рисунке 4-29.

В заводской прошивке устройства самоподписанный сертификат генерируется автоматически при первом включении устройства.

Данное сообщение свидетельствует о том, что браузеру не удалось выполнить проверку сертификата. В целях безопасности практически все современные браузеры по умолчанию не открывают страницы, на которых используются самоподписанные сертификаты.

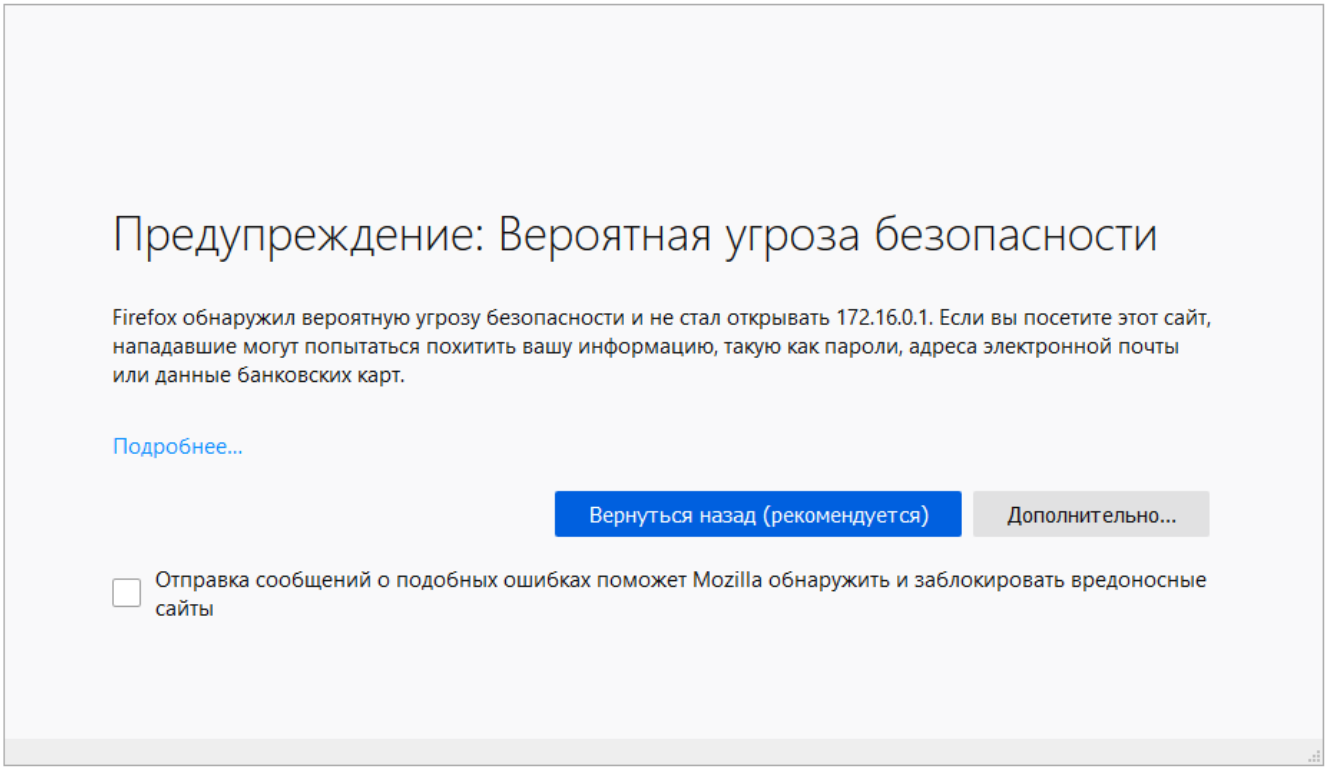


Рис. 4-29: Страница «Терминал». Ошибка проверки сертификата в браузере Mozilla Firefox

На рисунке 4-29 показано содержимое области терминала для браузера Mozilla Firefox. В других браузерах внешний вид и содержание данного сообщения может отличаться.

Для разрешения работы терминала с самоподписанным сертификатом, необходимо выполнить следующие действия (на примере браузера Mozilla Firefox[1]):

1) Открыть терминал в отдельном окне браузера, нажав кнопку «Открыть терминал в отдельном окне», расположенную в нижней части страницы «Терминал» (см. рисунок 4-28).
2) В открывшемся окне будет отображено сообщение, аналогичное показанному на рисунке 4-29. Необходимо нажать кнопку «Дополнительно...».
3) В открывшейся области дополнительной информации (см. рисунок 4-30) необходимо нажать кнопку «Принять риск и продолжить».

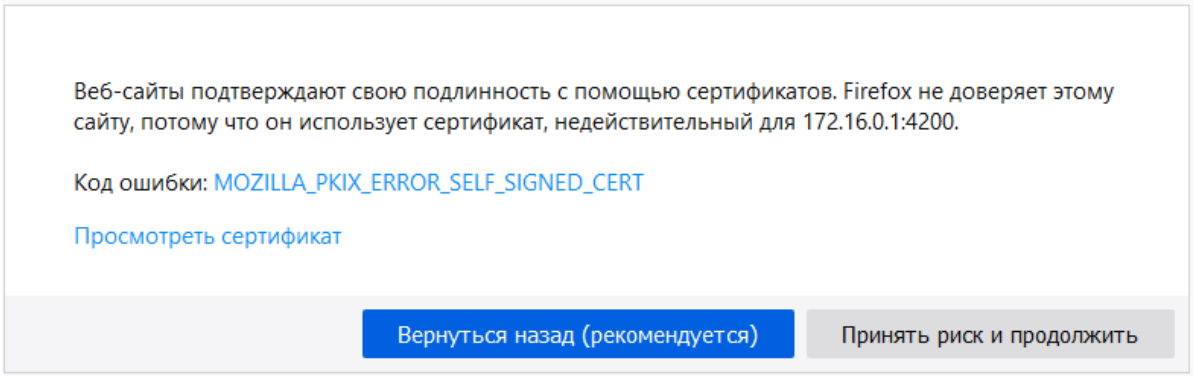


Рис. 4-30: Страница «Терминал». Дополнительная информация об ошибке проверки сертификата на примере браузера Mozilla Firefox

[1] в других браузерах (Google Chrome, Opera, Microsoft Internet Explorer и т.п.) приведённая последовательность действий может несущественно отличаться.

4) Будет открыт терминал с приглашением к вводу имени пользователя, как показано на рисунке 4-31.

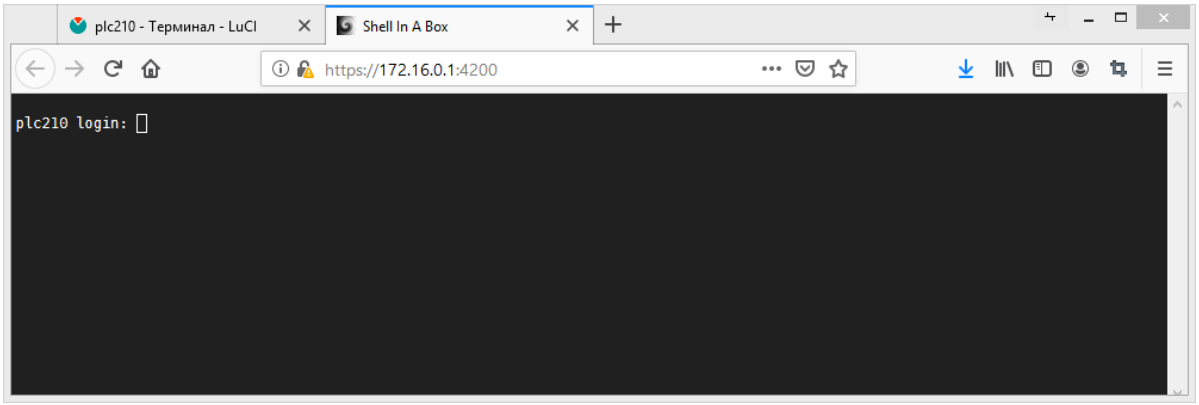


Рис. 4-31: Страница «Терминал». Открытие терминала после подтверждения самоподписанного сертификата

5) Отдельное окно браузера можно закрыть. После обновления основного окна, в котором была открыта страница «Терминал», область терминала должна выглядеть, как показано на рисунке 4-28.

4.8.1 Настройки терминала

Страница настроек терминала показана на рисунке 4-32.

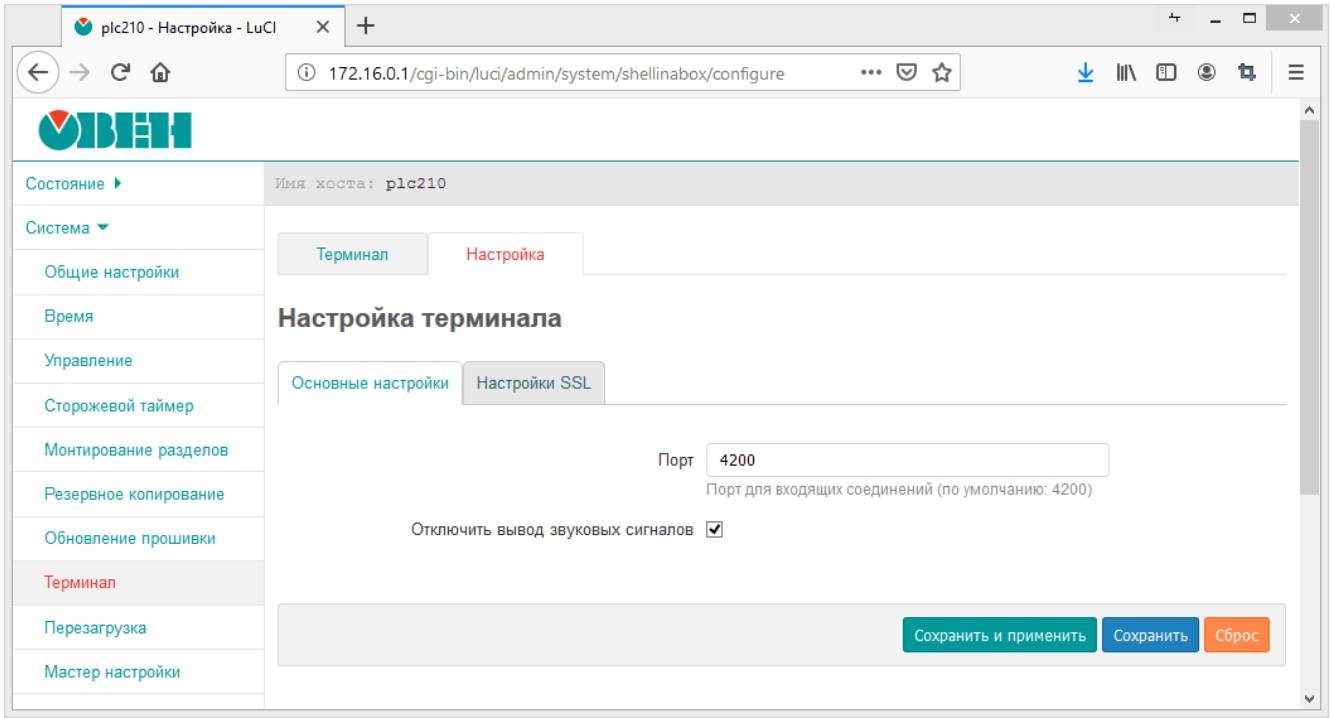


Рис. 4-32: Страница основных настроек терминала

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) [8].

На вкладке «Настройки SSL» расположены настройки шифрования SSL. Внешний вид вкладки «Настройки SSL» показан на рисунке 4-33

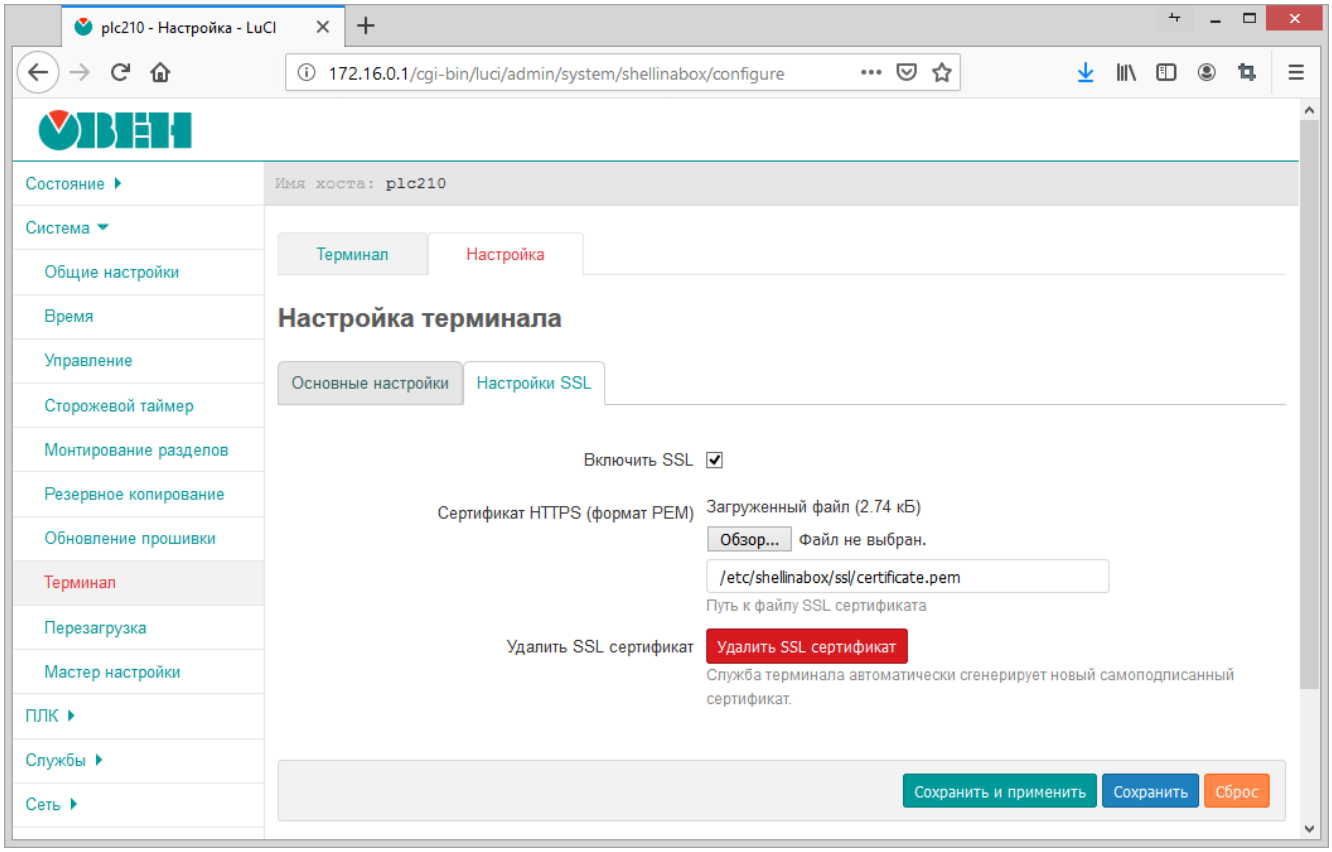


Рис. 4-33: Страница SSL настроек терминала

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 «Обзор...».

При нажатии кнопки «Удалить SSL сертификат» происходит удаление текущего SSL сертификата. При этом, если включена опция «Включить SSL», автоматически будет выполнена генерация нового самоподписанного сертификата.

4.9 Перезагрузка

Страница «Перезагрузка» раздела «Система» предназначена для выполнения программной перезагрузки устройства. Данная функция аналогична выполнению в консоли команды reboot. Внешний вид страницы «Перезагрузка» раздела «Система» показан на рисунке 4-34.

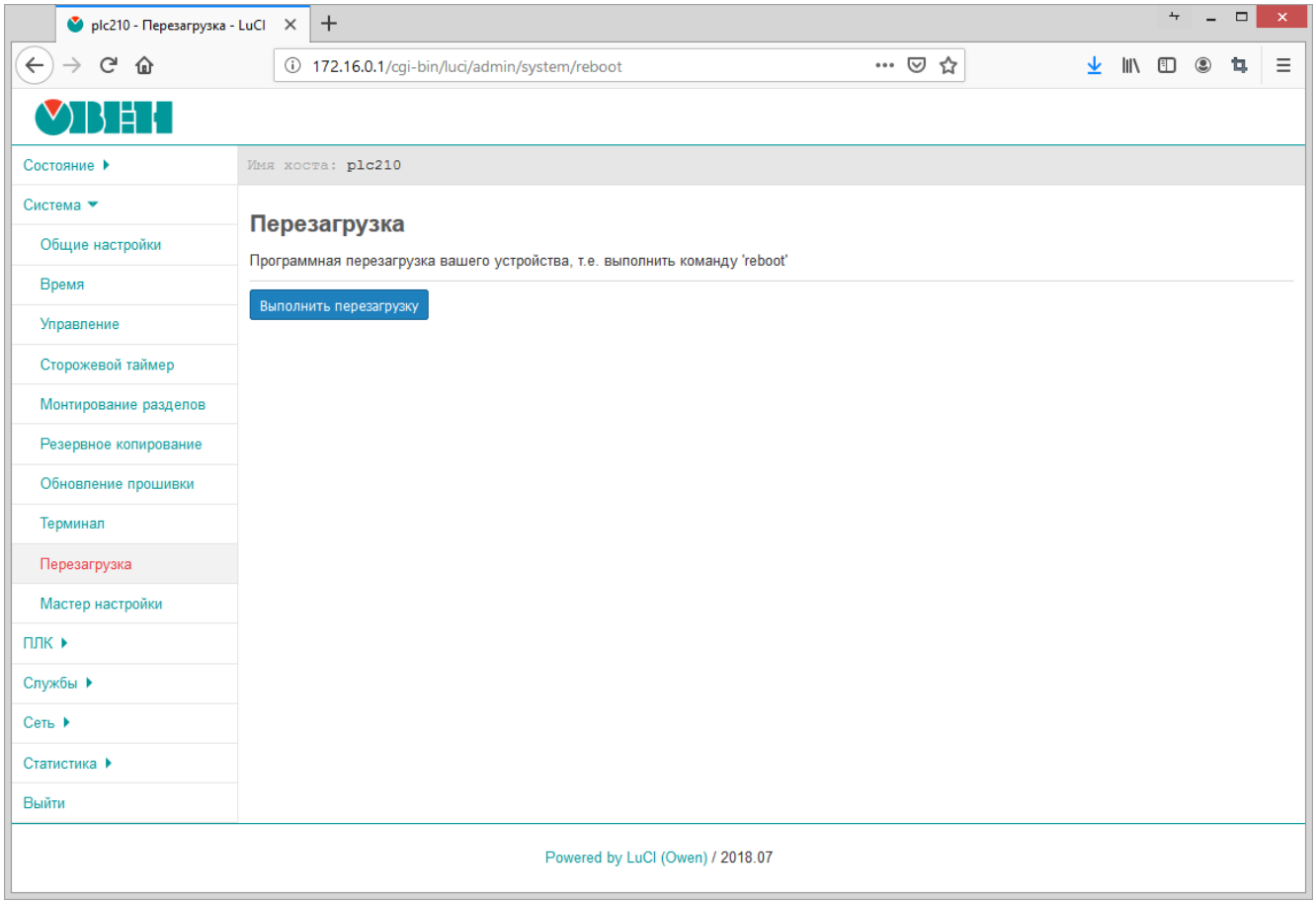


Рис. 4-34: Страница «Перезагрузка»

Перезагрузка устройства выполняется при нажатии кнопки «Выполнить перезагрузку».

4.10 Мастер настройки

Данный раздел отсутствует в Web-интерфейсе управления контроллеров СПК.

На странице «Мастер настройки» раздела «Система» можно выполнить запуск мастера настройки, который подробно описан в разделе 2 данного документа.

Внешний вид страницы «Мастер настройки» раздела «Система» показан на рисунке 4-35.

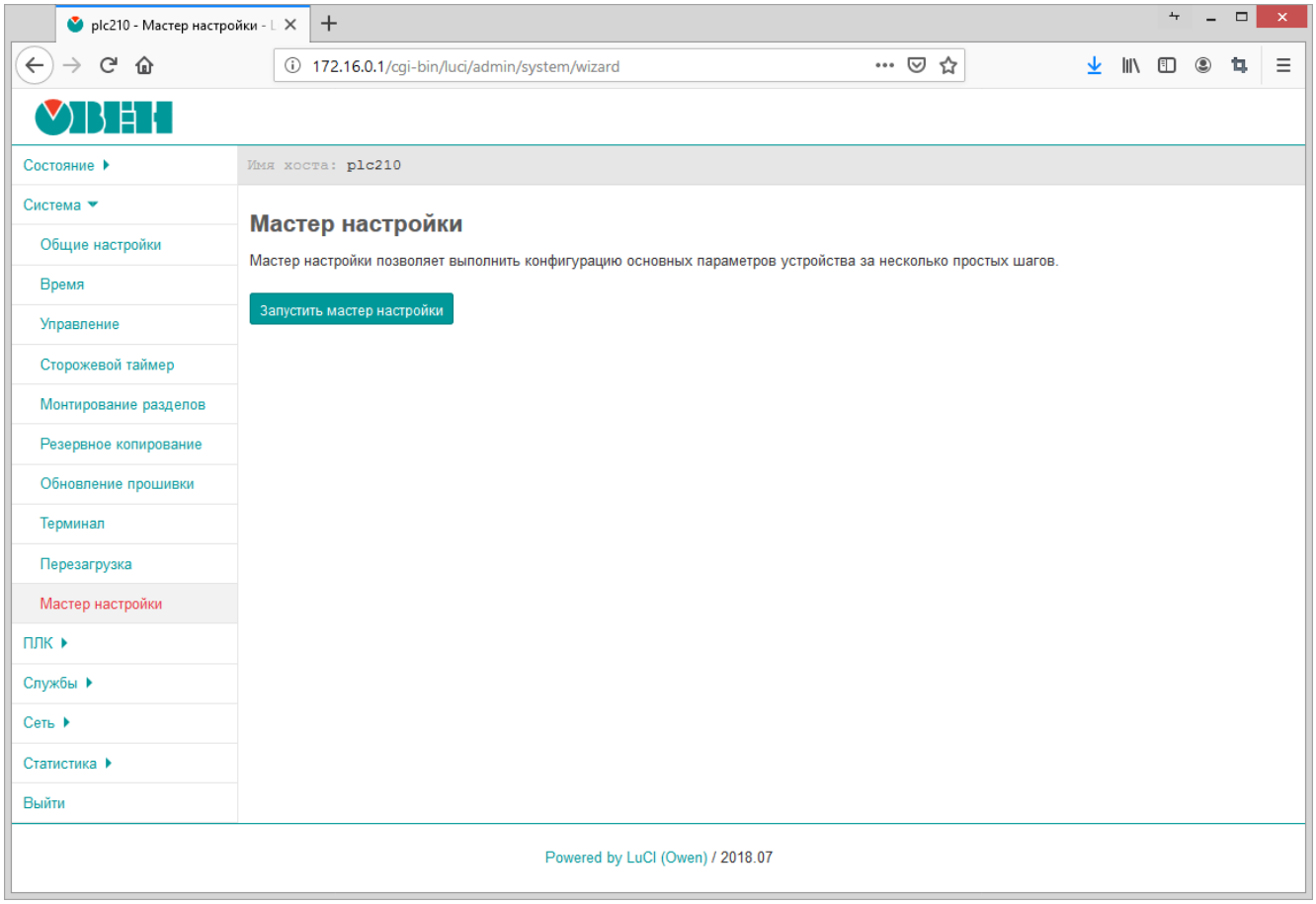


Рис. 4-35: Страница «Мастер настройки»

Запуск мастера настройки осуществляется при нажатии кнопки «Запустить мастер настройки».

5 ПЛК

В данном разделе содержится описание страниц для управления, настройки и мониторинга функций ПЛК устройства, которые обеспечиваются средой исполнения CODESYS.

5.1 Веб визуализация

На странице «Веб визуализация» раздела «ПЛК» отображается визуализация пользовательского приложения CODESYS.

Внешний вид страницы «Веб визуализация» раздела «ПЛК», при запущенном пользовательском приложении, показан на рисунке 5-1.

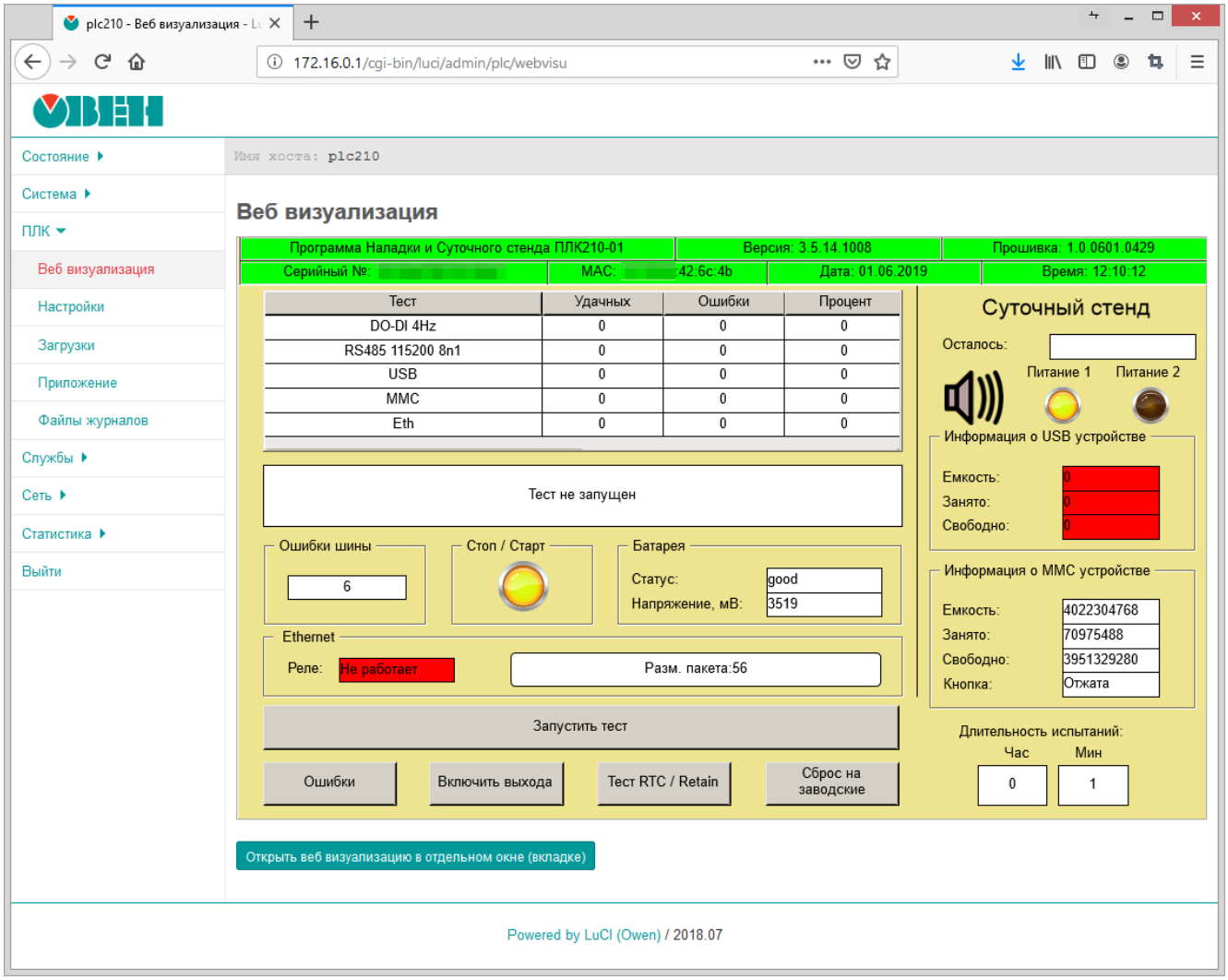


Рис. 5-1: Страница «Веб визуализация»

В нижней части страницы расположена кнопка «Открыть веб визуализацию в отдельном окне (вкладке)», которая позволяет открыть веб визуализацию в отдельном окне (или вкладке) браузера, что может быть удобно при необходимости ручного масштабирования окна веб визуализации.

Если пользовательское приложение CODESYS не запущено, то на странице «Веб визуализация» будет отображено соответствующее сообщение (см. рисунок 5-2).

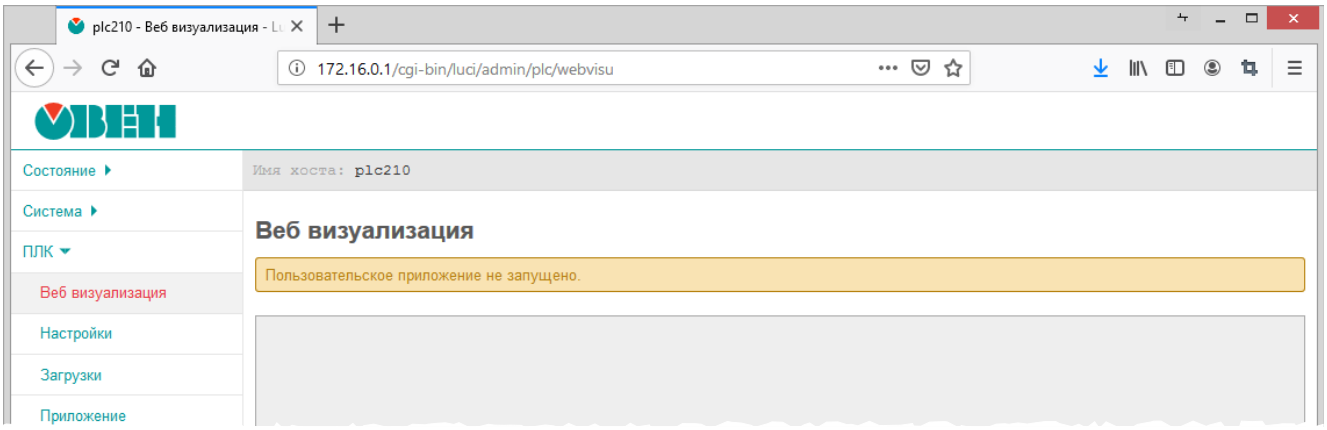


Рис. 5-2: Страница «Веб визуализация». Пользовательское приложение не запущено

5.2 Настройки

Страница «Настройки» раздела «ПЛК» содержит основные настройки среды исполнения CODESYS, включая функцию веб визуализации. Внешний вид страницы «Настройки» показан на рисунке 5-3.

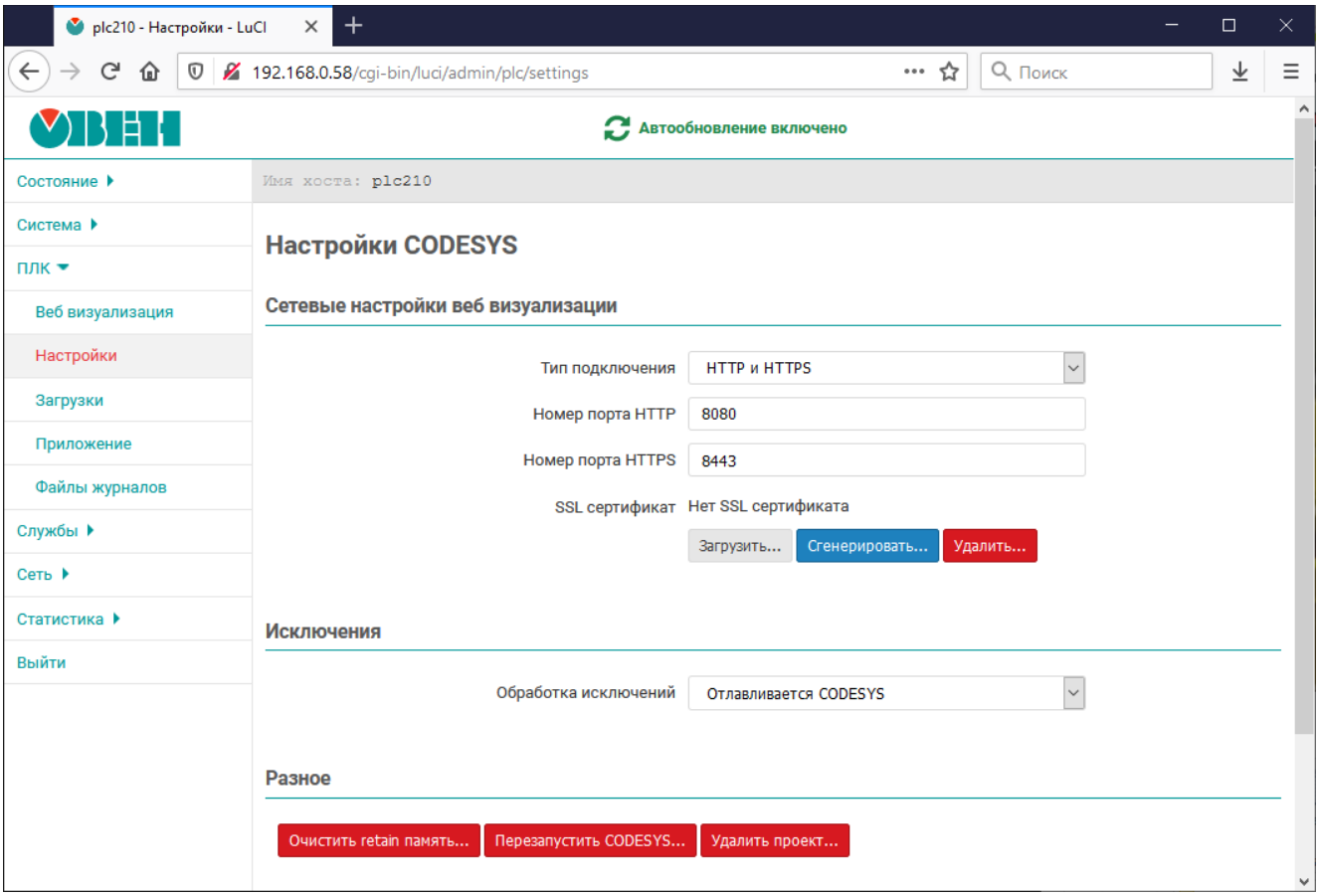


Рис. 5-3: Страница «Настройки»

На странице «Настройки» раздела «ПЛК» доступны следующие настройки:

- «Тип подключения» — выбор поддерживаемых протоколов подключения веб визуализации CODESYS (по умолчанию «HTTP и HTTPS»);
- «Номер порта HTTP» — номер порта TCP, используемый веб визуализацией CODESYS, при использовании протокола HTTP (по умолчанию 8080);
- «Номер порта HTTPS» — номер порта TCP, используемый веб визуализацией CODESYS, при использовании протокола HTTPS (по умолчанию 8443);

- «SSL сертификат» — информация и настройки SSL сертификата, используемого для HTTPS подключения к веб-визуализации.

  Если сертификат отсутствует, то отображается сообщение «Нет SSL сертификата». Для имеющегося сертификата отображается дата его создания и дата истечения его срока действия (см. рисунок 5-4).

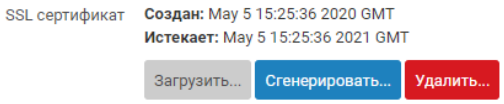


Рис. 5-4: Информация о текущем SSL сертификате веб визуализации CODESYS

  Кнопки «Сгенерировать...» и «Удалить...» предназначены для генерации нового SSL сертификата и удаления текущего сертификата соответственно. Генерация и удаление SSL сертификата веб визуализации CODESYS рассмотрены в разделах 5.2.1 и 5.2.2;

  Кнопка «Загрузить...» предназначена для выбора и загрузки SSL сертификата с закрытым ключом. Процесс загрузки SSL сертификата рассмотрен в разделе 5.2.3.

- «Обработка исключений» — метод обработки исключений. Доступны следующие варианты:
  - «Отлавливается CODESYS» — исключения обрабатываются средой исполнения CODESYS;
  - «Перезагрузка» — при возникновении исключения выполняется перезагрузка.
- «Очистить retain память...» — очистка энергонезависимой retain памяти (см. раздел 5.2.4).
- «Перезапустить CODESYS» — выполняется полная перезагрузка всех служб CODESYS (интерфейсов, приложений и др.) (см. раздел 5.2.5).
- «Удалить проект» — позволяет удалить загруженный проект (см. раздел 5.2.5).

5.2.1 Генерация SSL сертификата

Кнопка «Сгенерировать...» (см. рисунок 5-3) позволяет выполнить генерацию нового SSL сертификата. При нажатии данной кнопки будет отображено модальное окно с запросом подтверждения генерации нового SSL сертификата, показанное на рисунке 5-5.

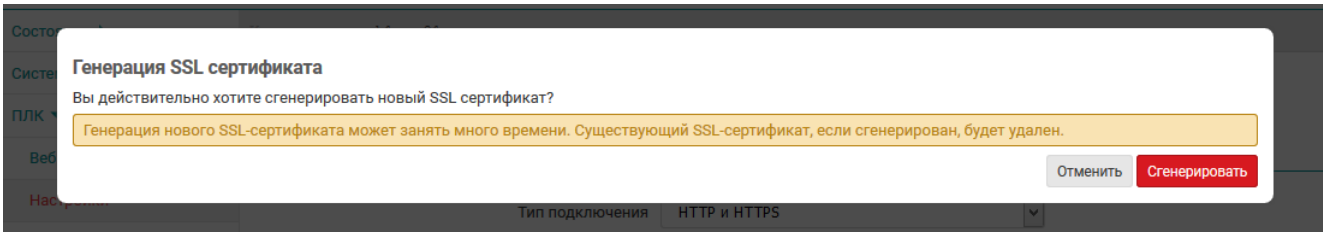


Рис. 5-5: Подтверждение генерации нового SSL сертификата

При нажатии кнопки «Сгенерировать» будет запущен процесс генерации нового SSL сертификата. Во время выполнения генерации будет отображаться окно, показанное на рисунке 5-6.

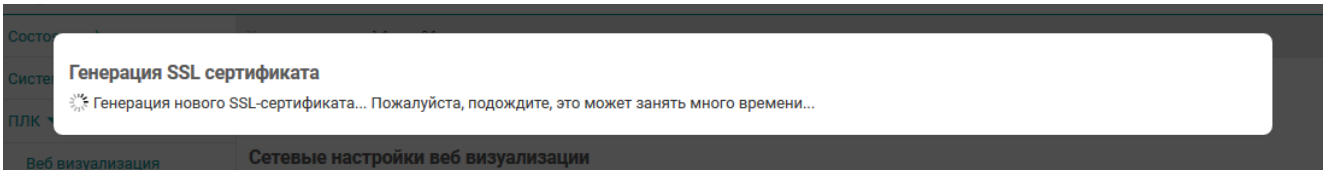


Рис. 5-6: Генерация нового SSL сертификата

При успешном завершении генерации нового SSL сертификата будет отображено окно с сообщением, как показано на рисунке 5-7. В поле информации о текущем сертификате (см. рисунок 5-4) будут отображены данные нового сертификата.

Рис. 5-7: Успешная генерация нового SSL сертификата

5.2.2 Удаление SSL сертификата

Кнопка «Удалить...» (см. рисунок 5-3) позволяет удалить текущий SSL сертификат. При нажатии этой кнопки будет отображено модальное окно подтверждения удаления сертификата, показанное на рисунке 5-8.

Рис. 5-8: Подтверждение удаления сертификата

Нажатие кнопки «Удалить» приведёт к запуску процесса удаления текущего SSL сертификата. В случае успешного удаления будет отображено окно с сообщением, как показано на рисунке 5-9.

Рис. 5-9: Успешное удаление сертификата

5.2.3 Загрузка SSL сертификата

Кнопка «Загрузить...» (см. рисунок 5-3) предназначена для загрузки файлов SSL сертификата веб-визуализации CODESYS. При нажатии данной кнопки будет отображено модальное окно с запросом требуемых файлов (см. рисунок 5-10):

- Файл сертификата (.cer файл) — файл сертификата безопасности, который используется для обеспечения безопасности серверов, транзакций, логинов. Сертификат безопасности выдается специальным Центром сертификации.
- Файл приватного ключа (.key файл) — файл закрытого (приватного) ключа, который обеспечивает защищенное HTTPS соединение между сервером и клиентом.
- DH (Diffie Hellman) ключ (.pem файл) — файл DH ключа, закодированный в Base64, применяемый для безопасной верификации пользователей.

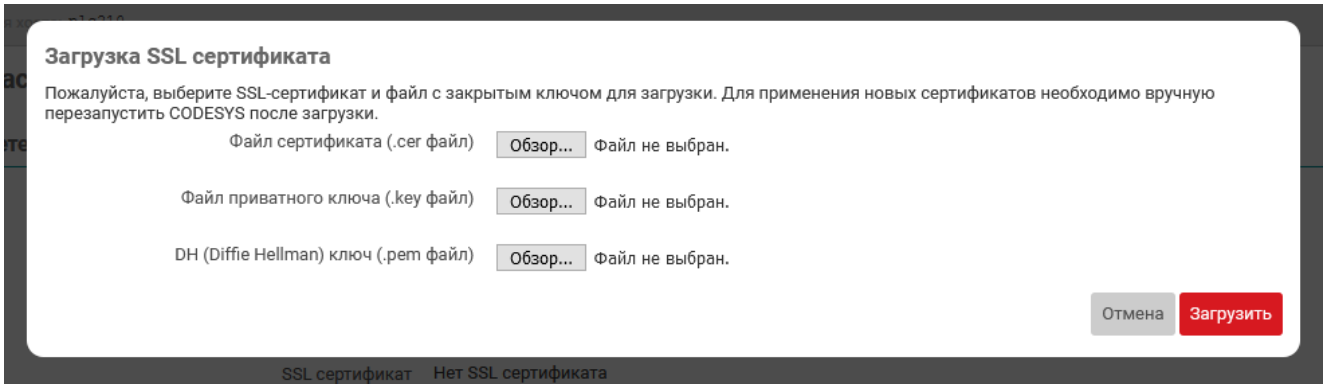


Рис. 5-10: Модальное окно загрузки SSL сертификата веб-визуализации CODESYS

После загрузки всех трёх файлов и нажатии кнопки «Загрузить» (см. рисунок 5-10) будет выполнена загрузка файлов SSL сертификата веб-визуализации CODESYS на устройство. Во время выполнения загрузки будет отображаться окно, показанное на рисунке 5-11.

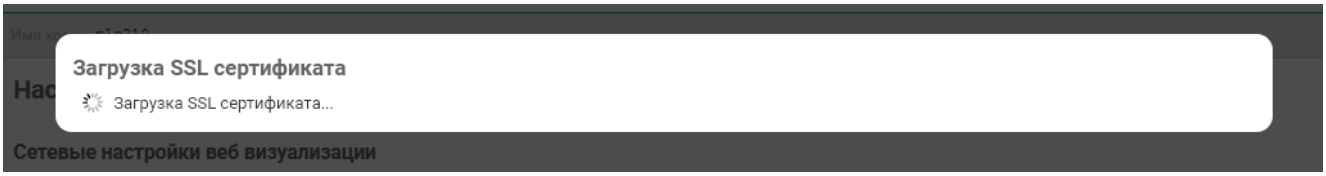


Рис. 5-11: Загрузка SSL сертификата

При успешном завершении загрузки файлов SSL сертификата будет отображено окно с сообщением, как показано на рисунке 5-12. В поле информации о текущем сертификате (см. рисунок 5-4) будут отображены данные нового сертификата.

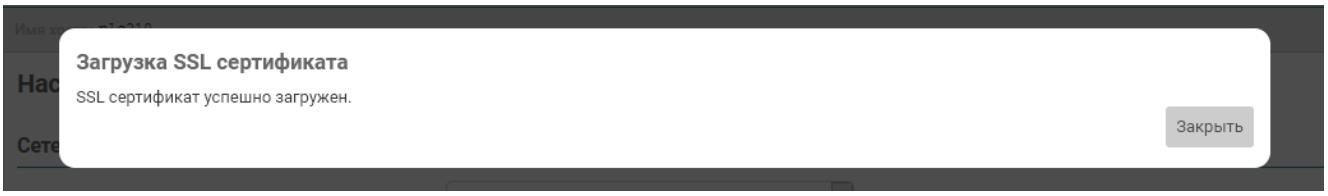


Рис. 5-12: Успешная загрузка SSL сертификата

Для применения загруженного SSL сертификата необходимо выполнить перезапуск CODESYS при помощи кнопки «Перезапустить CODESYS...» (см. раздел 5.2.5).

5.2.4 Очистка retain памяти

Кнопка «Очистка retain памяти...» (см. рисунок 5-3) позволяет выполнить очистку retain памяти (энергонезависимой). При нажатии данной кнопки будет отображено модальное окно с запросом подтверждения очистки retain памяти, показанное на рисунке 5-13.

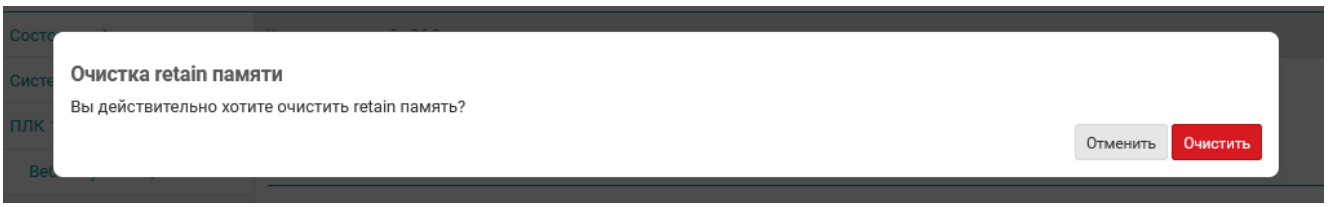


Рис. 5-13: Подтверждение очистки retain памяти

При нажатии кнопки «Очистка retain памяти...» будет запущен процесс очистки retain памяти. Во время выполнения очистки будет отображаться окно, показанное на рисунке 5-14.

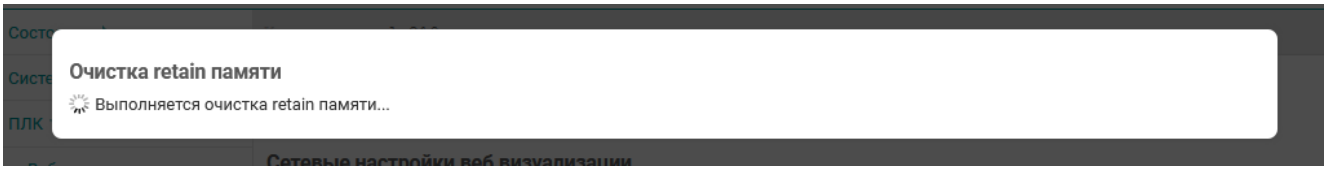


Рис. 5-14: Очистка retain памяти

При успешном завершении очистки retain памяти будет отображено окно с сообщением, как показано на рисунке 5-15.

Рис. 5-15: Успешная очистка retain памяти

5.2.5 Перезапуск CODESYS

Кнопка «Перезапустить CODESYS...» (см. рисунок 5-3) позволяет перезапустить CODESYS. При нажатии данной кнопки будет отображено модальное окно с запросом подтверждения перезагрузки CODESYS, показанное на рисунке 5-16.

Рис. 5-16: Подтверждение перезагрузки CODESYS

При нажатии кнопки «Перезапустить CODESYS...» будет запущен процесс перезагрузки CODESYS. Во время выполнения перезагрузки будет отображаться окно, показанное на рисунке 5-17.

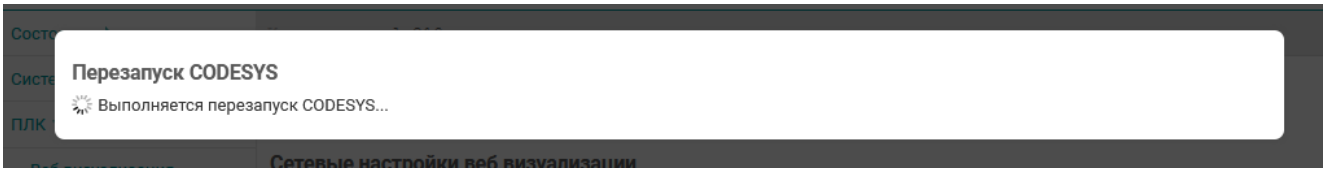


Рис. 5-17: Перезагрузка CODESYS

При успешном завершении процесса перезагрузки CODESYS будет отображено окно с сообщением, как показано на рисунке 5-18.

Рис. 5-18: Успешная перезагрузка CODESYS

5.2.6 Удаление проекта

Кнопка «Удалить проект...» (см. рисунок 5-3) позволяет удалить проект CODESYS. При нажатии данной кнопки будет отображено модальное окно с запросом подтверждения удаления проекта, показанное на рисунке 5-19.

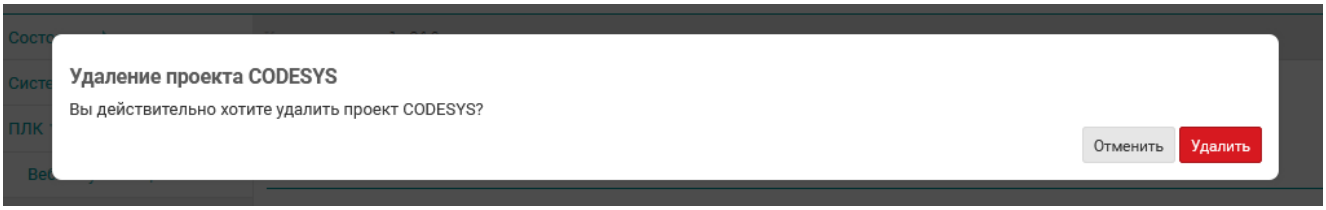


Рис. 5-19: Подтверждение удаление проекта

При нажатии кнопки «Удалить проект...» будет запущен процесс удаления проекта CODESYS. Во время выполнения удаления будет отображаться окно, показанное на рисунке 5-14.

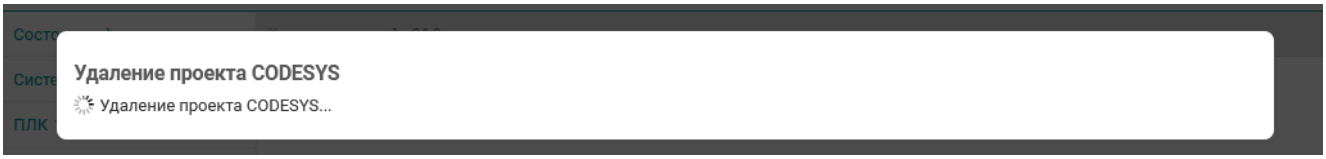


Рис. 5-20: Удаление проекта

При успешном завершении удаления проекта будет отображено окно с сообщением, как показано на рисунке 5-21.

Рис. 5-21: Успешное удаление проекта

5.3 Загрузки

На странице «Загрузки» раздела «ПЛК» представлены ссылки для загрузки различных полезных файлов и ссылки на информационные материалы по работе устройства. Внешний вид страницы «Загрузки» раздела «ПЛК» показан на рисунке 5-22.

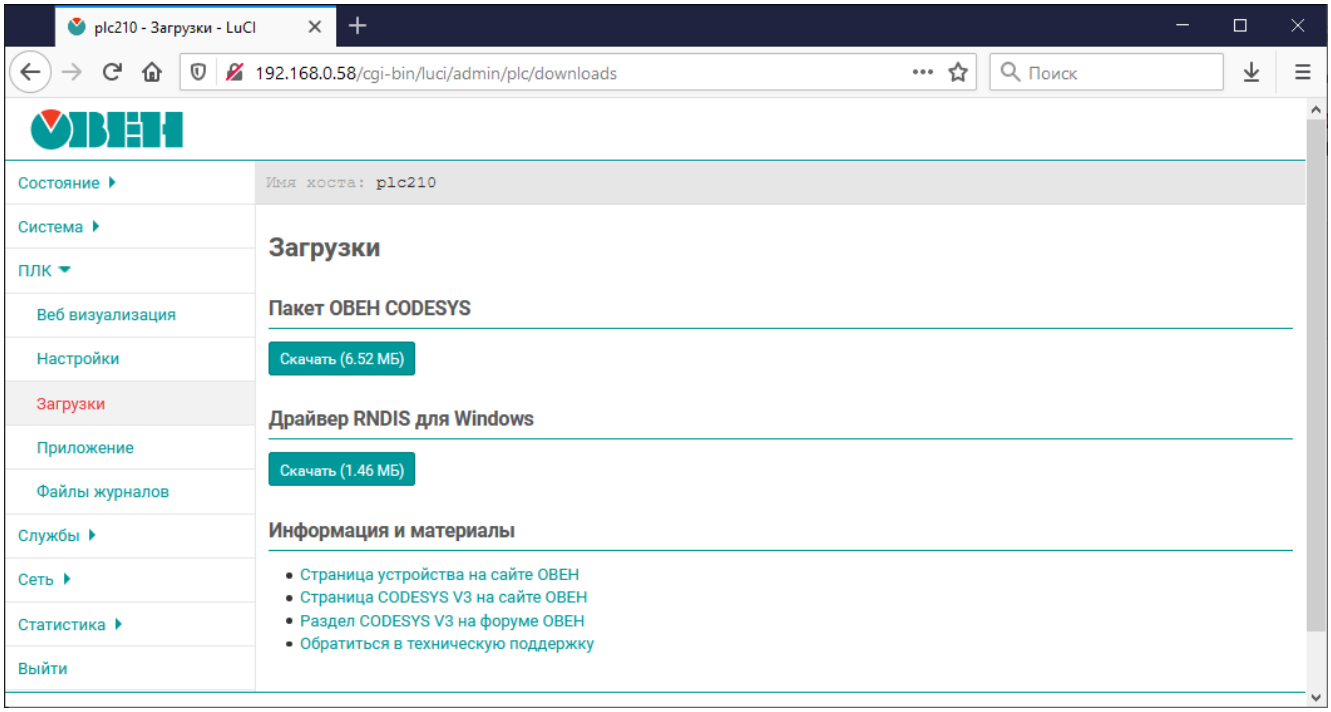


Рис. 5-22: Страница «Загрузки»

Для загрузки доступны следующие файлы:

- «Пакет ОВЕН CODESYS» — пакет для среды разработки CODESYS;
- «Драйвер RNDIS для Windows» — пакет драйверов для USB RNDIS подключения для операционной системы Windows.
- «Информация и материалы» — ссылки на страницы поддержки устройства, CODESYS и технической поддержки.

5.4 Приложение

На странице «Приложение» раздела «ПЛК» отображается информация о запущенном пользовательском приложении CODESYS. Внешний вид страницы «Приложение», при запущенном пользовательском приложении, показан на рисунке 5-23.

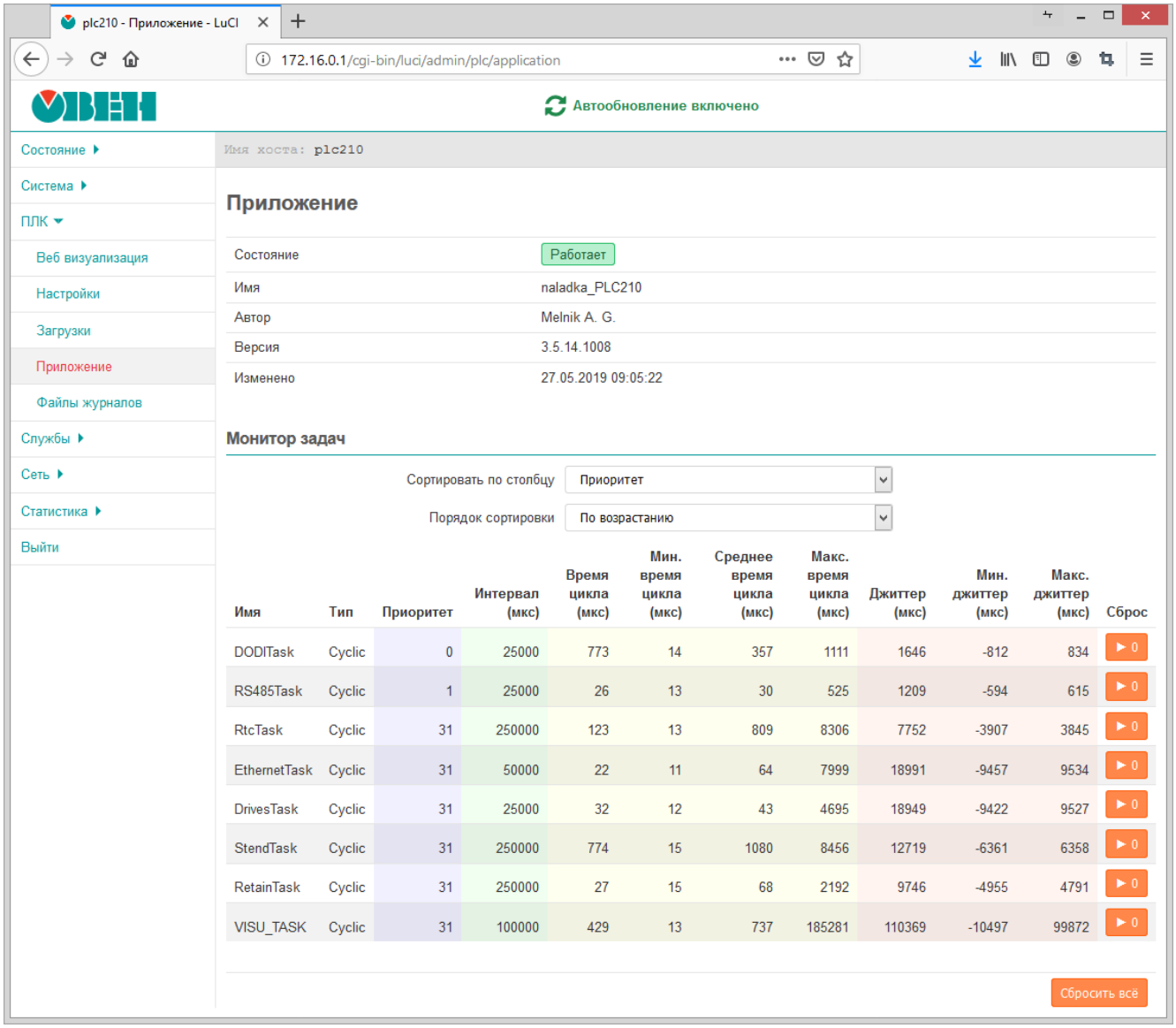


Рис. 5-23: Страница «Приложение»

В верхней части страницы отображается краткая информация о запущенном приложении в виде таблицы:

- «Состояние» — состояние пользовательского приложения. Может принимать одно из следующих значений:
  - «Работает» — пользовательское приложение запущено и работает;
  - «Не запущено» — пользовательское приложение не запущено;
  - «Остановлено» — пользовательское приложение остановлено;
  - «Исключение» — работа пользовательского приложения была прервана из-за произошедшего исключения;
- «Имя» — название (имя) приложения;
- «Автор» — автор приложения;
- «Версия» — версия приложения;
- «Изменено» — дата и время последнего изменения приложения.
- «Target» — версия целевого рантайма.

Например, если пользовательское приложение CODESYS не запущено, то таблица с информацией о приложении будет выглядеть, как показано на рисунке 5-24.

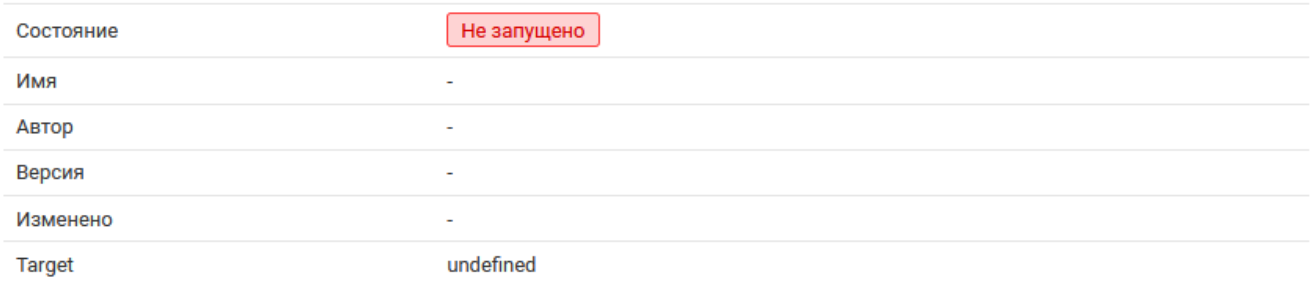
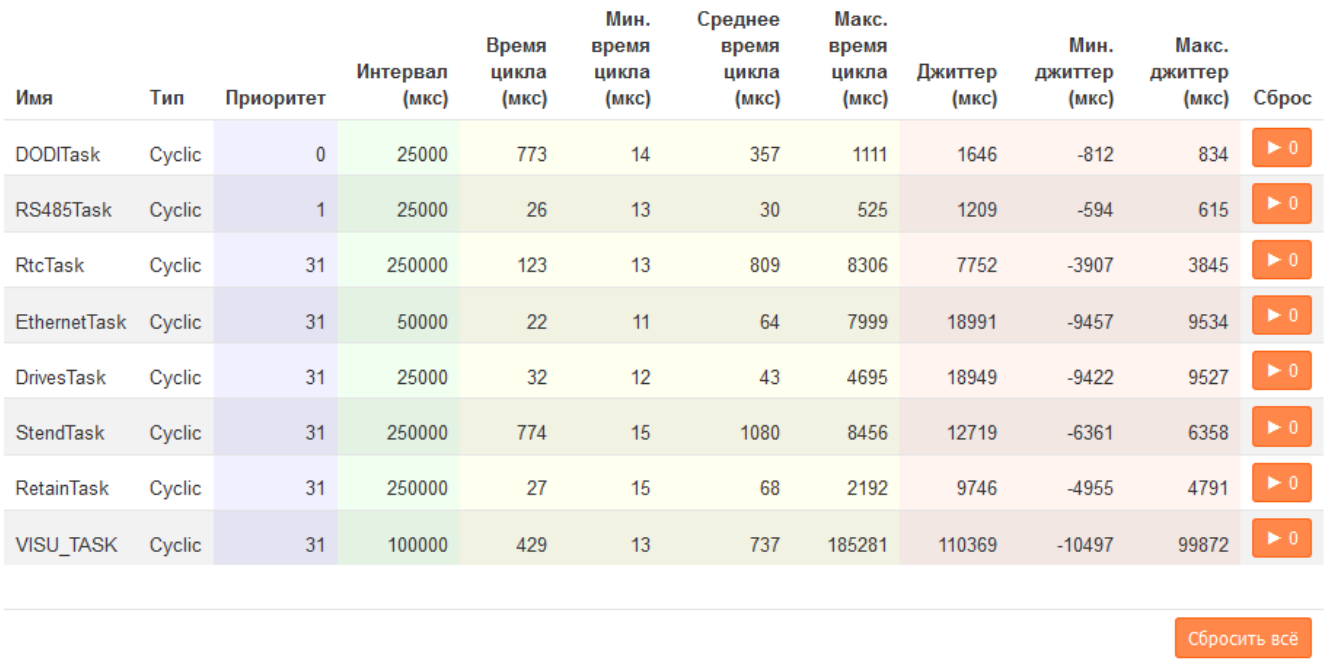


Рис. 5-24: Страница «Приложение». Пользовательское приложение не запущено

5.4.1 Монитор задач

В подразделе «Монитор задач» страницы «Приложение» отображается таблица задач (task) текущего запущенного пользовательского приложения CODESYS (см. рисунок 5-25).



Имя	Тип	Приоритет	Интервал (мкс)	Время цикла (мкс)	Мин. время цикла (мкс)	Среднее время цикла (мкс)	Макс. время цикла (мкс)	Джиттер (мкс)	Мин. джиттер (мкс)	Макс. джиттер (мкс)	Сброс
DODITask	Cyclic	0	25000	773	14	357	1111	1646	-812	834	▶ 0
RS485Task	Cyclic	1	25000	26	13	30	525	1209	-594	615	▶ 0
RtcTask	Cyclic	31	250000	123	13	809	8306	7752	-3907	3845	▶ 0
EthernetTask	Cyclic	31	50000	22	11	64	7999	18991	-9457	9534	▶ 0
DrivesTask	Cyclic	31	25000	32	12	43	4695	18949	-9422	9527	▶ 0
StendTask	Cyclic	31	250000	774	15	1080	8456	12719	-6361	6358	▶ 0
RetainTask	Cyclic	31	250000	27	15	68	2192	9746	-4955	4791	▶ 0
VISU_TASK	Cyclic	31	100000	429	13	737	185281	110369	-10497	99872	▶ 0

Рис. 5-25: Страница «Приложение». Таблица монитора задач

Каждая строка таблицы соответствует одной задаче, для которой отображаются следующие параметры в соответствующих столбцах таблицы:

- «Имя» — имя задачи;
- «Тип» — тип задачи. Может принимать следующие значения:
  - «Cyclic»;
  - «Event»;
  - «Status»;
  - «Freewheeling»;
- «Приоритет» — приоритет задачи. Может принимать значения от 0 (наивысший приоритет) до 31 (наименьший приоритет);
- «Интервал (мкс)» — интервал запуска задачи в микросекундах;
- «Время цикла (мкс)» — время цикла задачи в микросекундах;

- «Мин. время цикла (мкс)» — минимальное время цикла задачи в микросекундах;
- «Макс. время цикла (мкс)» — максимальное время цикла задачи в микросекундах;
- «Джиттер (мкс)» — джиттер задачи в микросекундах;
- «Мин. джиттер (мкс)» — минимальный джиттер задачи в микросекундах;
- «Макс. джиттер (мкс)» — максимальный джиттер задачи в микросекундах;
- «Сброс» — кнопка сброса счётчиков для данной задачи. Сбрасываются счётчики времени цикла и джиттера в значение «0».

Кнопка «Сбросить всё» выполняет сброс счётчиков времени цикла и джиттера в значение «0» для всех задач, перечисленных в таблице. Сброс счётчиков только для конкретной задачи выполняется при помощи кнопки, расположенной в столбце «Сброс» строки соответствующей задачи таблицы монитора задач.

Сверху таблицы монитора задач расположены элементы управления (см. рисунок 5-26), позволяющие выполнить сортировку строк таблицы по заданному столбцу с заданным порядком (по возрастанию или убыванию значений).

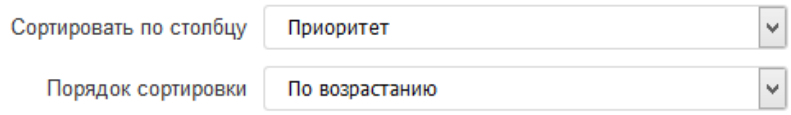


Рис. 5-26: Страница «Приложение». Управление сортировкой таблицы монитора задач

5.5 Файлы журналов

На странице «Файлы журналов» раздела «ПЛК» отображаются данные журналов сообщений среды исполнения CODESYS. Внешний вид страницы «Файлы журналов» показан на рисунке 5-27.

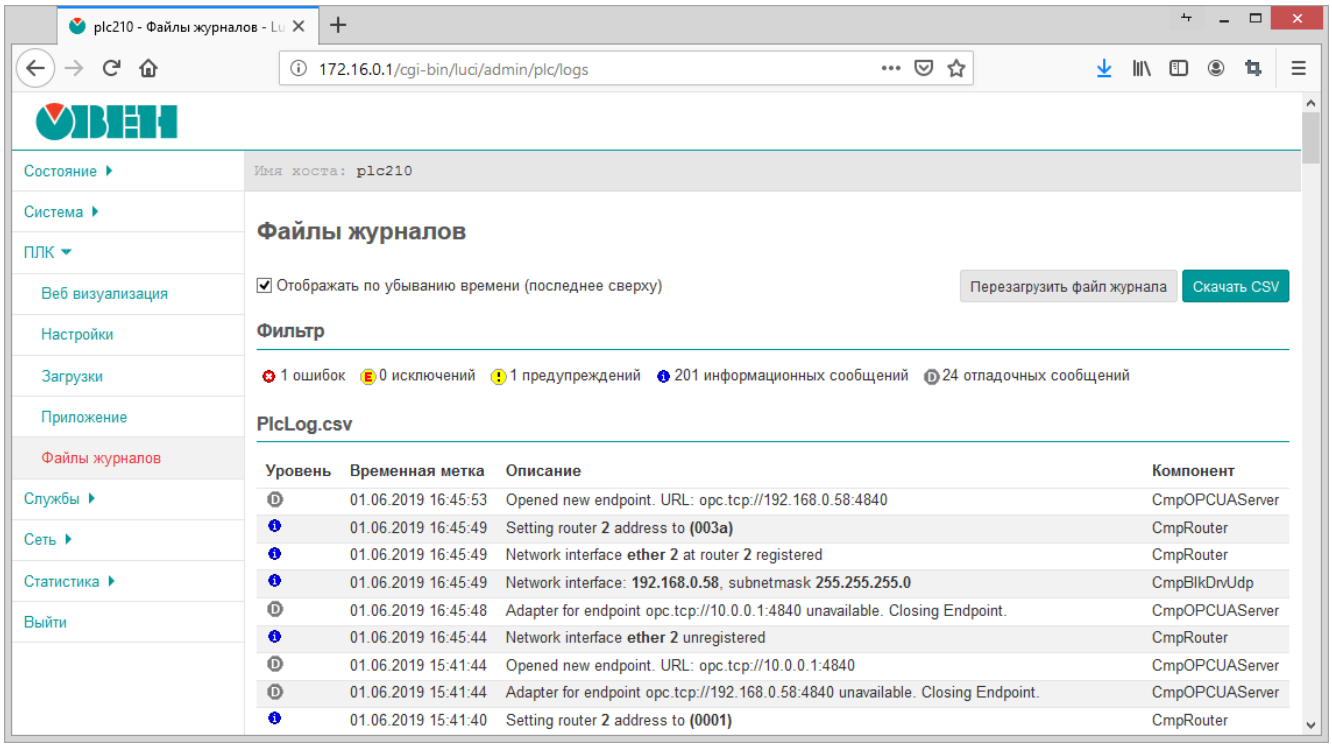


Рис. 5-27: Страница «Файлы журналов»

5.5.1 Основные элементы управления

Все элементы управления расположены в верхней части страницы.

На рисунке 5-27 показана страница «Файлы журналов» для случая, когда в системе имеется только один файл журнала. Если в системе будет несколько файлов журналов, то в верхней части страницы будут отображены вкладки для выбора файла журнала, как показано на рисунке 5-28.

Рис. 5-28: Страница «Файлы журналов». Вкладки выбора файла журнала

Опция «Отображать по убыванию времени (последнее сверху)» управляет порядком отображения записей журнала. Возможно отображение записей как по возрастанию времени, так и по убыванию (режим по умолчанию).

Записи из файла журнала считываются только один раз при загрузке страницы (записи на странице не обновляются автоматически). Кнопка «Перезагрузить файл журнала» позволяет выполнить повторное считывание данных из файла журнала и обновить данные на странице.

Исходные файлы журналов содержат записи в формате CSV [9]. Кнопка «Скачать CSV» позволяет скачать (загрузить) оригинальный файл журнала в формате CSV.

5.5.2 Фильтр записей

В подразделе «Фильтр» расположены элементы управления фильтра отображаемых записей журнала (см. рисунок 5-29).

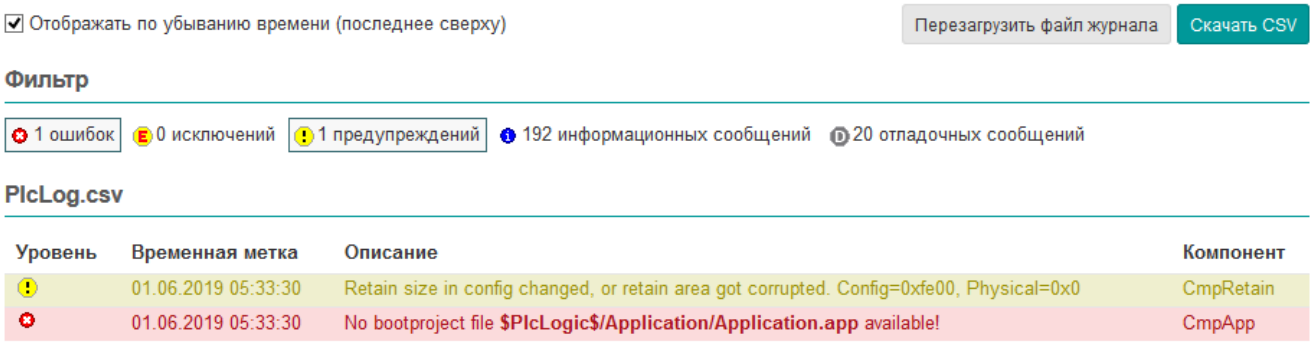


Рис. 5-29: Страница «Файлы журналов». Фильтр записей журнала

Каждая запись журнала соответствует определённому уровню сообщений. В свою очередь, каждому уровню сообщений соответствует своя графическая иконка. Возможные уровни сообщений и соответствующие им графические иконки представлены в следующем списке:

- — ошибка;
- — исключение;
- — предупреждение;
- — информационное сообщение;
- — отладочное сообщение.

Фильтр представляет собой кнопки-переключатели для каждого уровня сообщений. Когда фильтр выключен (все кнопки-переключатели отжаты), отображаются сообщения всех уровней. При включении фильтра (нажата одна или несколько кнопок-переключателей) в таблице отображаются лишь сообщения тех уровней, для которых кнопки фильтра находятся в нажатом состоянии. Например, на рисунке 5-29, включено отображение только сообщений с уровнями «ошибка» и «исключение».

Дополнительно для каждого уровня сообщений, на кнопках-переключателях отображается количество записей в журнале, соответствующих данному уровню сообщений.

5.5.3 Сообщения журнала

В подразделе с именем файла журнала (например, «PlcLog.csv») отображаются записи журнала в виде таблицы (см. рисунок 5-30).

PlcLog.csv

Уровень	Временная метка	Описание	Компонент
D	02.06.2019 04:05:23	BIO_new_sysfile: Failed to open file = $.pki$/own/tls/dhparams.pem	CmpOpenSSL
i	02.06.2019 04:05:23	CODESYS Control ready	CmpMgr
D	02.06.2019 04:05:23	Segment[0]: Tag=TAG_RETAIN_FREE, Size=65000, Guid={00000000-00000000-00000000-00000000}	CmpRetain
D	02.06.2019 04:05:23	--- SRAM layout: Address=0xb596b000	CmpRetain
D	02.06.2019 04:05:23	Component CmpOpenSSL opened the certificate store!	CmpOpenSSL
D	02.06.2019 04:05:23	Segment[0]: Tag=TAG_RETAIN_FREE, Size=65000, Guid={00000000-00000000-00000000-00000000}	CmpRetain
D	02.06.2019 04:05:23	--- SRAM layout: Address=0xb596b000	CmpRetain
D	02.06.2019 04:05:23	Segment[0]: Tag=TAG_RETAIN_FREE, Size=65000, Guid={00000000-00000000-00000000-00000000}	CmpRetain
D	02.06.2019 04:05:23	--- SRAM layout: Address=0xb596b000	CmpRetain
✖	02.06.2019 04:05:23	No bootproject file **$PlcLogic$/Application/Application.app** available!	CmpApp
D	02.06.2019 04:05:23	Component CmpApp opened the certificate store!	CmpOpenSSL
i	02.06.2019 04:05:23	Setting router **2** address to **(2ddc:c0a8:003a)**	CmpRouter
i	02.06.2019 04:05:23	Setting router **1** address to **(0000:0001)**	CmpRouter
i	02.06.2019 04:05:23	Setting router **0** address to **(003a)**	CmpRouter
D	02.06.2019 04:05:23	Component CmpSecureChannel opened the certificate store!	CmpOpenSSL
D	02.06.2019 04:05:23	Component CmpWebServer opened the certificate store!	CmpOpenSSL
i	02.06.2019 04:05:23	Network interface **BlkDrvTcp** at router **2** registered	CmpRouter
i	02.06.2019 04:05:23	Local network address: **192.168.0.58**	CmpBlkDrvTcp
i	02.06.2019 04:05:23	Provider CmpOPCUAProviderIecVarAccess with Version 0x3050e00 registerd at the OPC UA server.	CmpOPCUAServer
i	02.06.2019 04:05:22	Provider CODESYS_DefaultProvider with Version 0x3050e00 registerd at the OPC UA server.	CmpOPCUAServer
i	02.06.2019 04:05:22	**********	CmpOPCUAServer
i	02.06.2019 04:05:22	All available networkadapters are used.	CmpOPCUAServer
i	02.06.2019 04:05:22	Loopbackadapter activated.	CmpOPCUAServer
i	02.06.2019 04:05:22	URL: opc.tcp://plc210:4840	CmpOPCUAServer
i	02.06.2019 04:05:22	Hostname: plc210, Port: 4840	CmpOPCUAServer
i	02.06.2019 04:05:22	OPC UA Server Started:	CmpOPCUAServer
i	02.06.2019 04:05:22	**********	CmpOPCUAServer
D	02.06.2019 04:05:22	Opened new endpoint. URL: opc.tcp://127.0.0.1:4840	CmpOPCUAServer

Рис. 5-30: Страница «Файлы журналов». Таблица записей журнала

Таблица записей журнала имеет следующие столбцы:

- «Уровень» — уровень сообщения, представленный в виде графической иконки (соответствие графических иконок уровням сообщений описано в разделе 5.5.2);
- «Временная метка» — дата и время регистрации данной записи в журнале;
- «Описание» — текст сообщения записи в журнале;
- «Компонент» — имя компонента CODESYS, который выполнил журналирование данной записи. Может быть представлено в текстовом виде (например, «CmpBlkDrvUdp») или в виде шестнадцатеричного кода компонента (например, «0x16289ca5»).

6 Службы

6.1 Динамический DNS (DDNS)

На странице «DDNS» раздела «Службы» расположены настройки службы динамического DNS.

Динамический DNS — технология, позволяющая информации на DNS-сервере обновляться в реальном времени и (по желанию) в автоматическом режиме. Она применяется для назначения постоянного доменного имени устройству с динамическим IP-адресом.

Внешний вид страницы «DDNS» раздела «Службы» показан на рисунке 6-1.

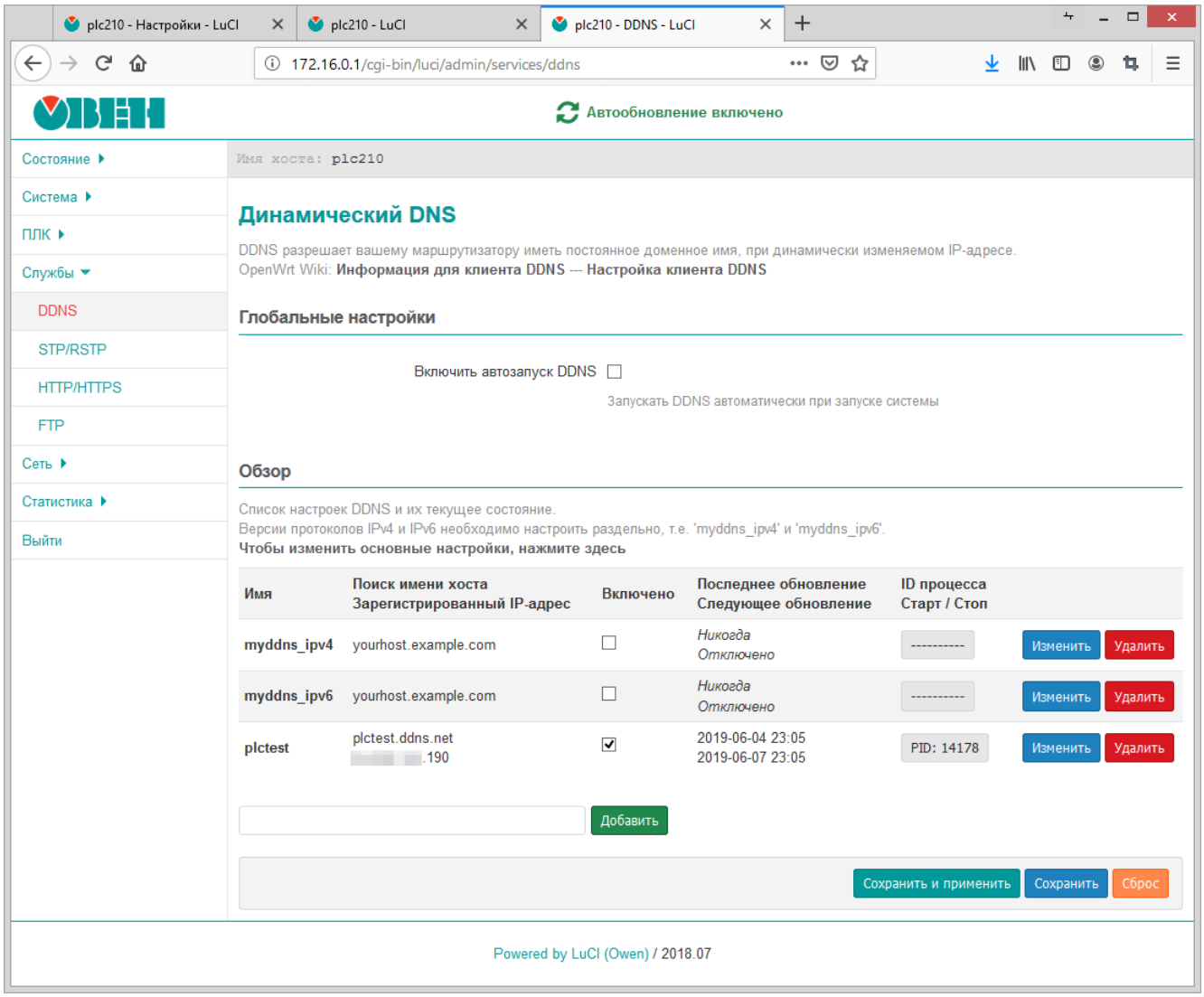


Рис. 6-1: Страница «DDNS»

В приложении B данного руководства приведены инструкции для настройки службы DDNS на примере провайдера no-ip.com.

В подразделе «Глобальные настройки» расположена опция «Включить автозапуск DDNS», которая управляет автоматическим запуском скриптов обновления DDNS записей при запуске системы. По умолчанию, автоматический запуск DDNS отключён.

В подразделе «Обзор» в виде таблицы перечислены текущие настроенные DDNS записи. Таблица имеет следующие столбцы:

- «Имя» — произвольное имя данной DDNS записи;
- «Поиск имени хоста / Зарегистрированный IP-адрес» — отображает доменное имя данной DDNS записи и определённый для него IP-адрес при последней проверке;
- «Включено» — признак включения текущей DDNS записи. Если данная опция отключена, для данной записи скрипт обновления не запускается;
- «Последнее обновление / Последующее обновление» — дата и время последнего и следующего планового обновления DDNS записи;
- «ID процесса / Старт / Стоп» — ручной запуск и остановка скрипта обновления DDNS записи.

  Если скрипт обновления в данный момент запущен и работает, то в данном столбце будет отображаться кнопка с текущим идентификатором процесса скрипта обновления DDNS записи, как показано на рисунке 6-2. Нажатие этой кнопки выполняет ручную остановку скрипта.

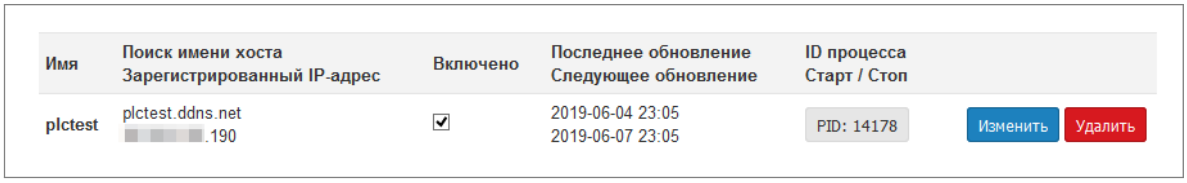


Рис. 6-2: Страница «DDNS». Скрипт обновления DDNS записи работает

Если скрипт в данный момент остановлен, то в данном столбце будет отображаться кнопка с надписью «Старт», как показано на рисунке 6-3. Нажатие кнопки «Старт» выполняет запуск скрипта обновления для данной DDNS записи.

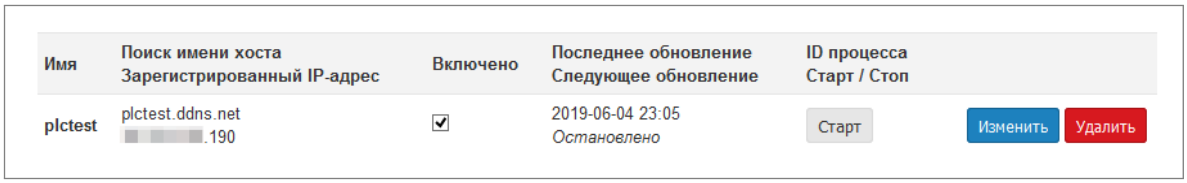


Рис. 6-3: Страница «DDNS». Скрипт обновления DDNS записи остановлен

- В последнем столбце расположены кнопки управления «Изменить» и «Удалить».

  Кнопка «Изменить» предназначена для редактирования соответствующей DDNS записи (см. раздел 6.1.1).

  Кнопка «Удалить» предназначена для удаления соответствующей DDNS записи (см. раздел 6.1.3).

6.1.1 Редактирование DDNS записи

Для редактирования DDNS записи необходимо нажать кнопку «Изменить» для соответствующей записи в таблице на странице «DDNS» (см. рисунок 6-4).

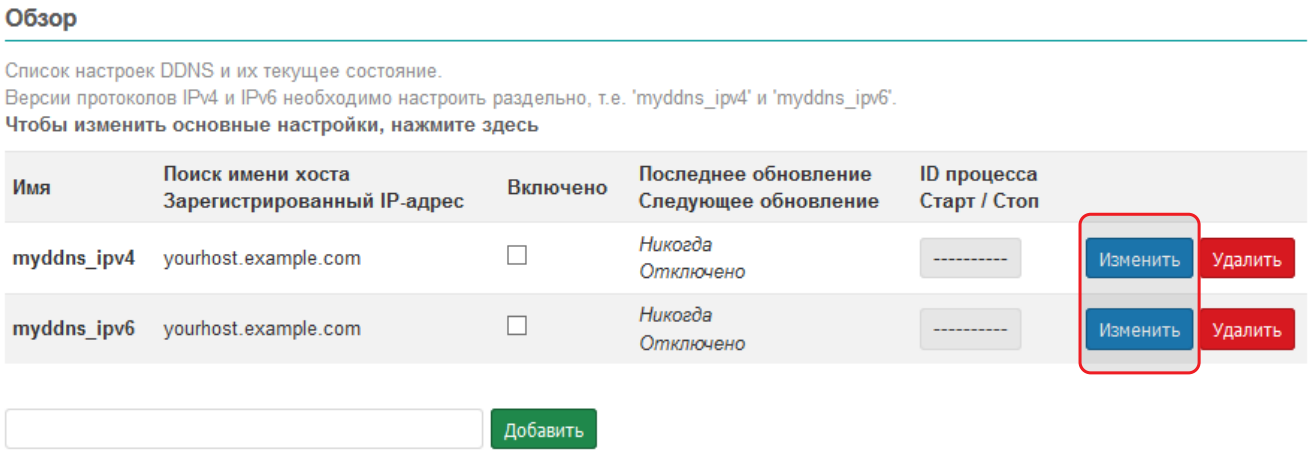


Рис. 6-4: Страница «DDNS». Кнопки изменения записи

При этом будет открыта страница редактирования DDNS записи, как показано на рисунке 6-5.

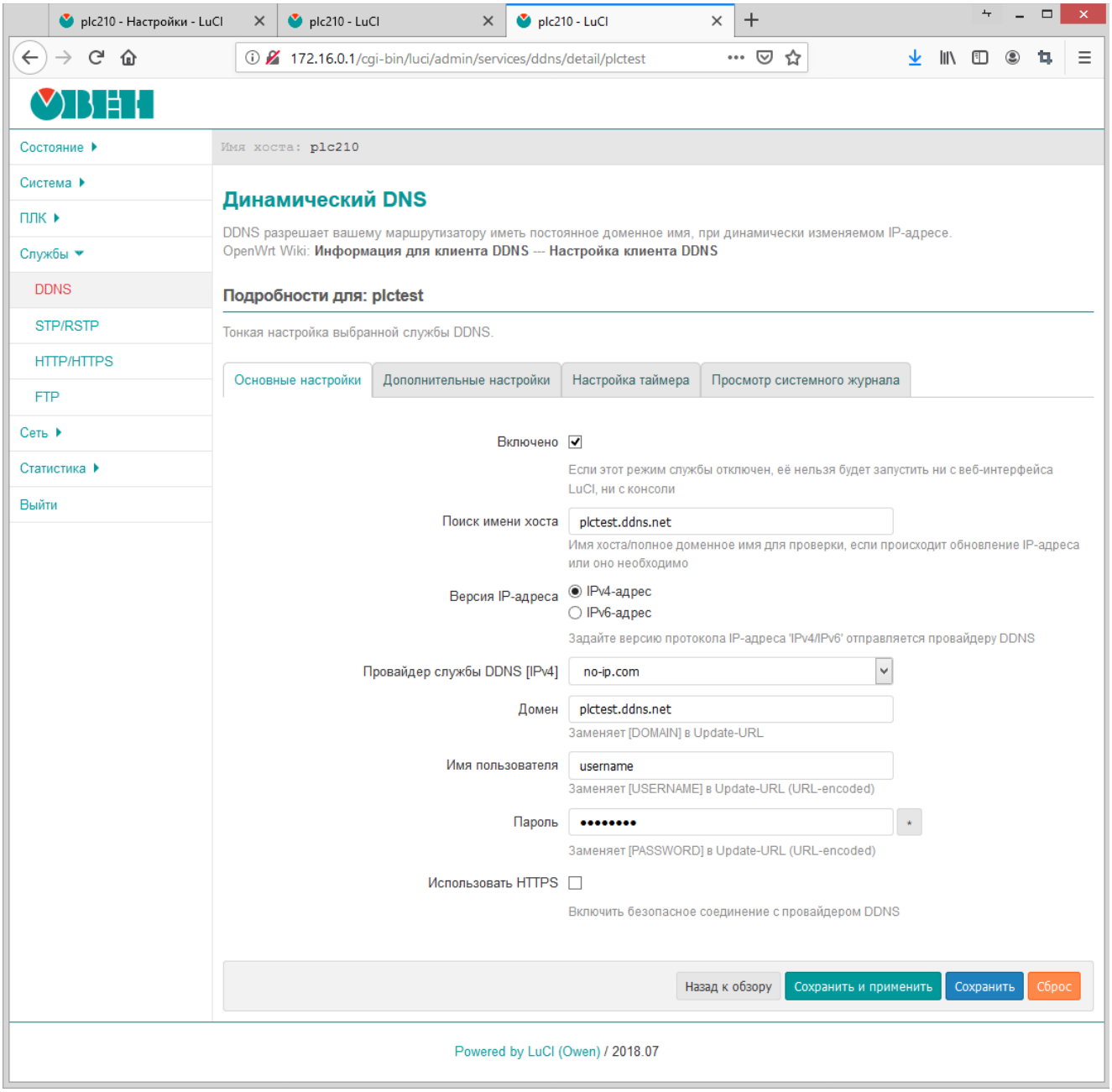


Рис. 6-5: Страница редактирования DDNS записи

Настройки DDNS записи распределены по четырём вкладкам:

- «Основные настройки» (см. раздел 6.1.1.1);
- «Дополнительные настройки» (см. раздел 6.1.1.2);
- «Настройка таймера» (см. раздел 6.1.1.3);
- «Просмотр системного журнала» (см. раздел 6.1.1.4).

6.1.1.1 Вкладка «Основные настройки»

Внешний вид вкладки «Основные настройки» показан на рисунке 6-5.

На вкладке размещены основные настройки DDNS записи:

- «Включено» — глобальный флаг активации редактируемой записи DDNS. Если эта опция отключена, то скрипт обновления для данной DDNS записи нельзя будет запустить ни с web-интерфейса LuCI, ни с консоли;

- «Поиск имени хоста» — полное доменное имя, используемое для проверки необходимости обновления IP-адреса данной DDNS записи;
- «Версия IP-адреса» — выбор версии IP протокола DDNS записи;
- «Провайдер службы DDNS» — выбор провайдера службы DDNS.

  При выборе провайдера отличного от установленного в данный момент, будет отображена кнопка «Сменить провайдера», как показано на рисунке 6-6. Для подтверждения смены DDNS провайдера, необходимо нажать кнопку «Сменить провайдера».

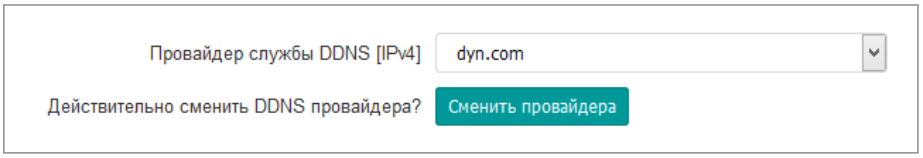


Рис. 6-6: Смена провайдера DDNS записи

Для пользовательского провайдера (элемент «-- пользовательский --» в списке) доступны две дополнительные настройки — «Пользовательский URL обновления» и «Пользовательский скрипт обновления» (см. рисунок 6-7).

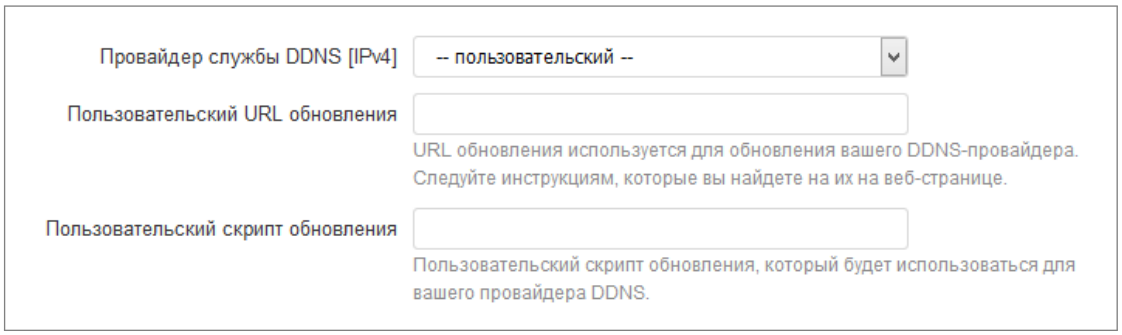


Рис. 6-7: Настройки пользовательского DDNS провайдера

В поле «Пользовательский URL обновления» указывается URL адрес обновления DDNS записи, где могут использоваться специальные значения, вместо которых будут подставляться определённые значения:

- `[DOMAIN]` — значение настройки «Домен»;
- `[USERNAME]` — значение настройки «Имя пользователя»;
- `[PASSWORD]` — значение настройки «Пароль»;
- `[IP]` — текущий определённый IP-адрес;

В поле «Пользовательский скрипт обновления» указывается путь пользовательского скрипта обновления DDNS записи;

- «Домен» — полное доменное имя, зарегистрированное у провайдера службы DDNS. Данное доменное имя будет отправлено провайдеру службы DDNS при обновлении IP-адреса. Данная настройка может отсутствовать для некоторых DDNS провайдеров.

  Значение данной настройки подставляется вместо `[DOMAIN]` в URL обновления;
- «Имя пользователя» — имя пользователя учётной записи провайдера службы DDNS.

  Значение данной настройки подставляется вместо `[USERNAME]` в URL обновления;
- «Пароль» — пароль учётной записи провайдера службы DDNS.

  Значение данной настройки подставляется вместо `[PASSWORD]` в URL обновления;
- «Использовать HTTPS» — включение безопасного HTTPS соединения с провайдером службы DDNS.

  При включении данной настройки становится доступна дополнительная настройка «Путь к CA-сертификату» (см. рисунок 6-8), в которой указывается путь к папке или файлу CA-сертификата.

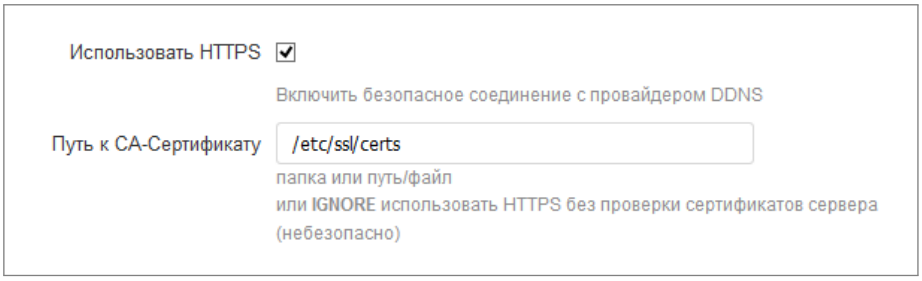


Рис. 6-8: Настройка «Путь к CA-сертификату» DDNS записи

Для использования HTTPS без проверки сертификатов сервера (небезопасно) необходимо указать значение «IGNORE».

6.1.1.2 Вкладка «Дополнительные настройки»

Внешний вид вкладки «Дополнительные настройки» показан на рисунке 6-9.

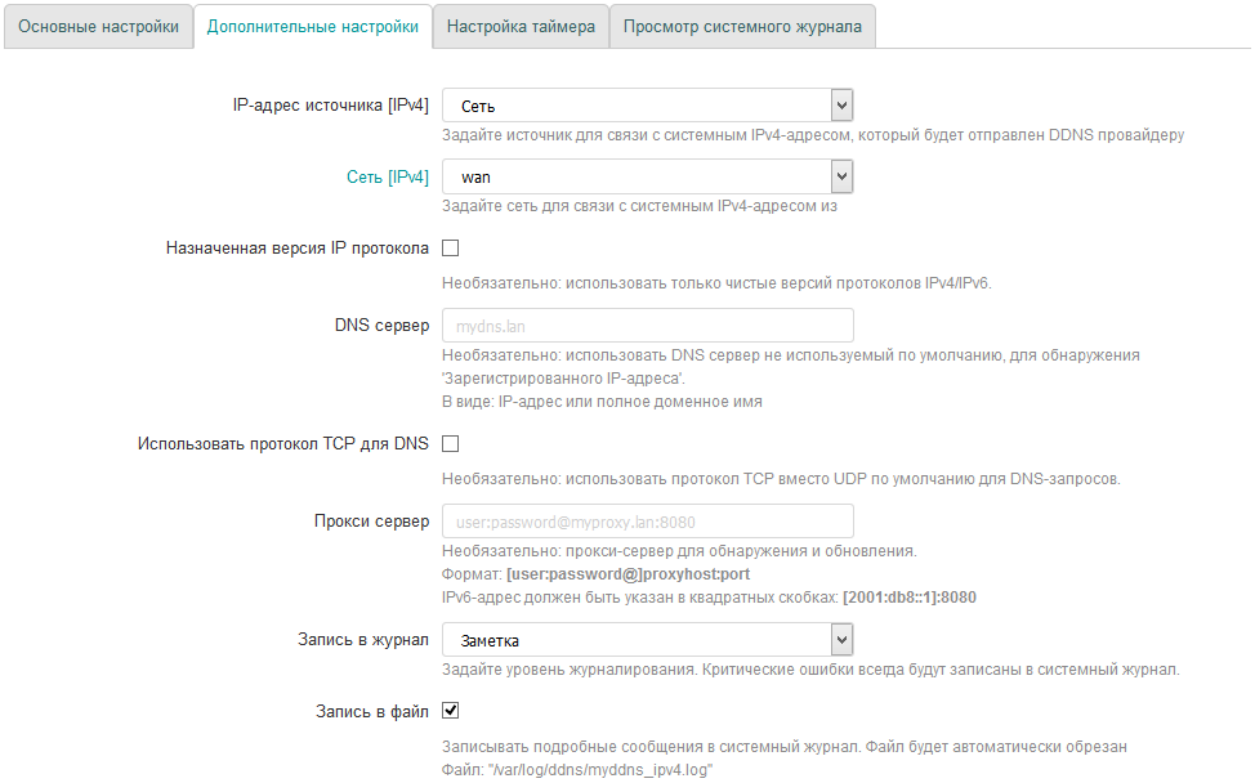


Рис. 6-9: Вкладка «Дополнительные настройки» страницы редактирования DDNS записи

На вкладке «Дополнительные настройки» расположены следующие настройки DDNS записи:

- «IP-адрес источника» — выбор источника для определения IP-адреса домена данной DDNS записи.

  Возможен выбор одного из следующих источников:

  - «Сеть» — источником IP-адреса выступает сеть, выбранная в выпадающем списке «Сеть» (см. рисунок 6-10).

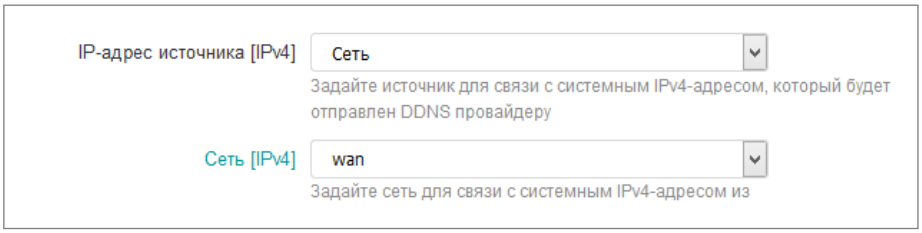


Рис. 6-10: Настройки DDNS записи для источника IP-адреса «Сеть»

- «URL» — источником IP-адреса выступает ответ запроса по указанному адресу (URL) в поле «URL для обнаружения» (см. рисунок 6-11).

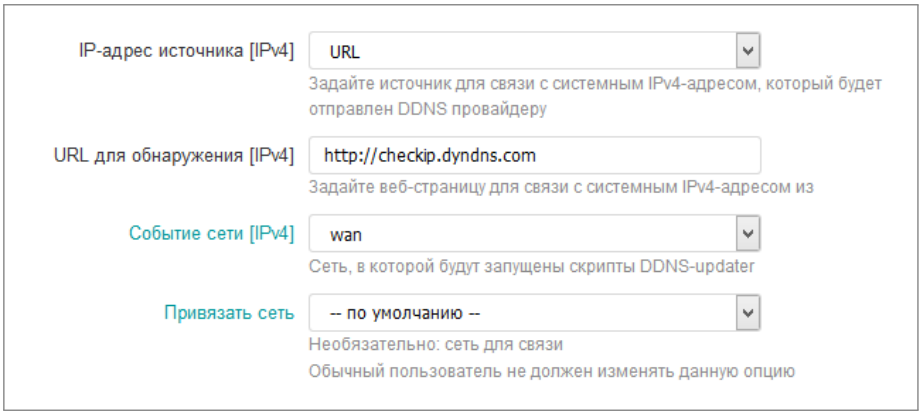


Рис. 6-11: Настройки DDNS записи для источника IP-адреса «URL»

Дополнительно в выпадающем списке «Событие сети» (см. рисунок 6-11) выбирается сеть, для которой будет запускаться скрипт обновления DDNS записи.

В выпадающем списке «Привязать сеть» (см. рисунок 6-11) выбирается сеть, через которую необходимо выполнять запрос указанного URL. В большинстве случаев рекомендуется выбрать значение «по умолчанию»;

- «Интерфейс» — источником IP-адреса выступает IP-адрес сетевого интерфейса, выбранного в выпадающем списке «Интерфейс» (см. рисунок 6-12);

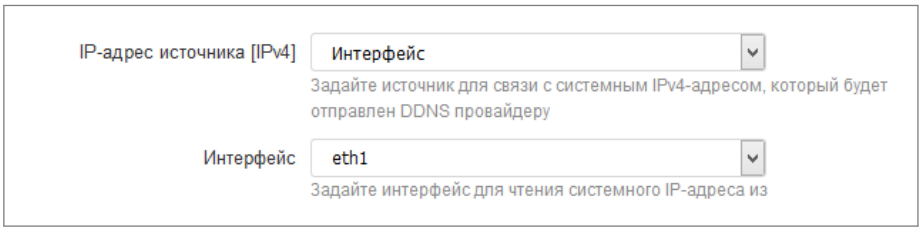


Рис. 6-12: Настройки DDNS записи для источника IP-адреса «Интерфейс»

- «Скрипт» — источником IP-адреса выступает результат выполнения скрипта, путь к которому указан в поле «Скрипт» (см. рисунок 6-13).

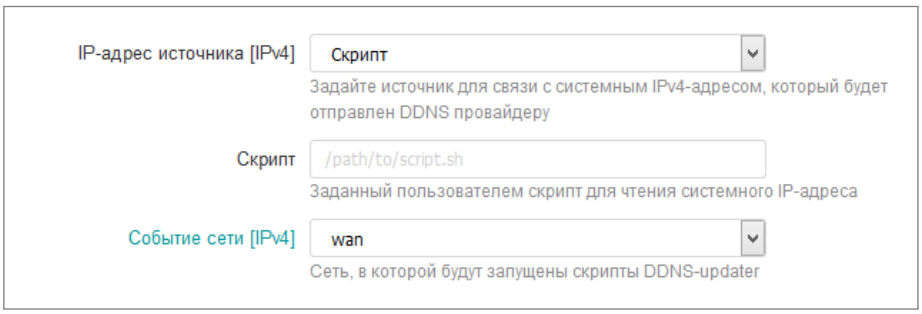


Рис. 6-13: Настройки DDNS записи для источника IP-адреса «Скрипт»

Дополнительно в выпадающем списке «Событие сети» (см. рисунок 6-13) выбирается сеть, для которой будет запускаться скрипт обновления DDNS записи.

- «Назначенная версия IP протокола» — настройка указывает на необходимость использования конкретной версии IP (IPv4 или IPv6) протокола в работе таких утилит, как wget, curl и host. Версия используемого IP протокола соответствует выбранной версии IP-адреса в настройке «Версия IP-адреса» на вкладке «Основные настройки» (см. раздел 6.1.1.1);

- «DNS сервер» — адрес DNS-сервера для определения зарегистрированного IP адреса для данной DDNS записи. Если не задано, то будет использован DNS сервер по умолчанию;
- «Выбрать протокол TCP для DNS» — установка данной опции включает использование TCP вместо UDP для DNS запросов;
- «Прокси сервер» — адрес прокси сервера для обнаружения и обновления DDNS записи. Указывается в формате:

  ```
  [user:password@]proxyhost:port
  ```

  где
  - `[user:password@]` — имя пользователя (`user`) и пароль (`password`) для выполнения авторизации на прокси сервере, если требуется;
  - `proxyhost` — адрес прокси сервера;

    Если адресом прокси сервера является IPv6-адрес, он должен быть указан в квадратных скобках (например, `[2001:db8::1]:8080`).

  - `port` — номер порта сервера;
- «Запись в журнал» — выбирается уровень сообщений для журналирования. Критические ошибки журналируются всегда, вне зависимости от выбранного уровня;
- «Запись в файл» — настройка включает запись журнала данной DDNS записи в файл.

6.1.1.3 Вкладка «Настройка таймера»

Внешний вид вкладки «Настройка таймера» показан на рисунке 6-14.

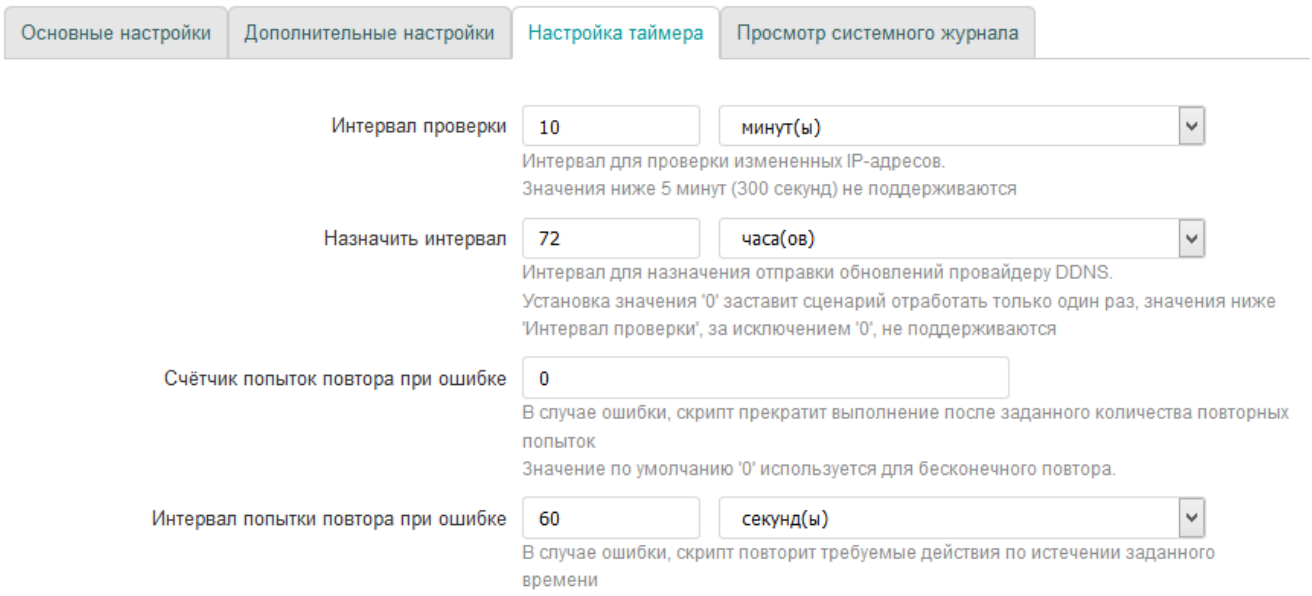


Рис. 6-14: Вкладка «Настройки таймера» страницы редактирования DDNS записи

На вкладке «Настройка таймера» расположены следующие настройки DDNS записи:

- «Интервал проверки» — интервал проверки изменения IP-адреса DDNS записи. Интервал проверки не должен быть менее 5 минут;
- «Назначить интервал» — интервал для отправки плановых обновлений провайдеру DDNS;
- «Учёт попыток повтора при ошибке» — в случае ошибки скрипт прекратит своё выполнение после заданного количества повторных попыток. Значение 0 (по умолчанию) используется для бесконечного повтора;
- «Интервал попытки повтора при ошибке» — в случае ошибки скрипт повторит требуемые действия по истечении заданного времени.

6.1.1.4 Вкладка «Просмотр системного журнала»

Внешний вид вкладки «Просмотр системного журнала» показан на рисунке 6-15.

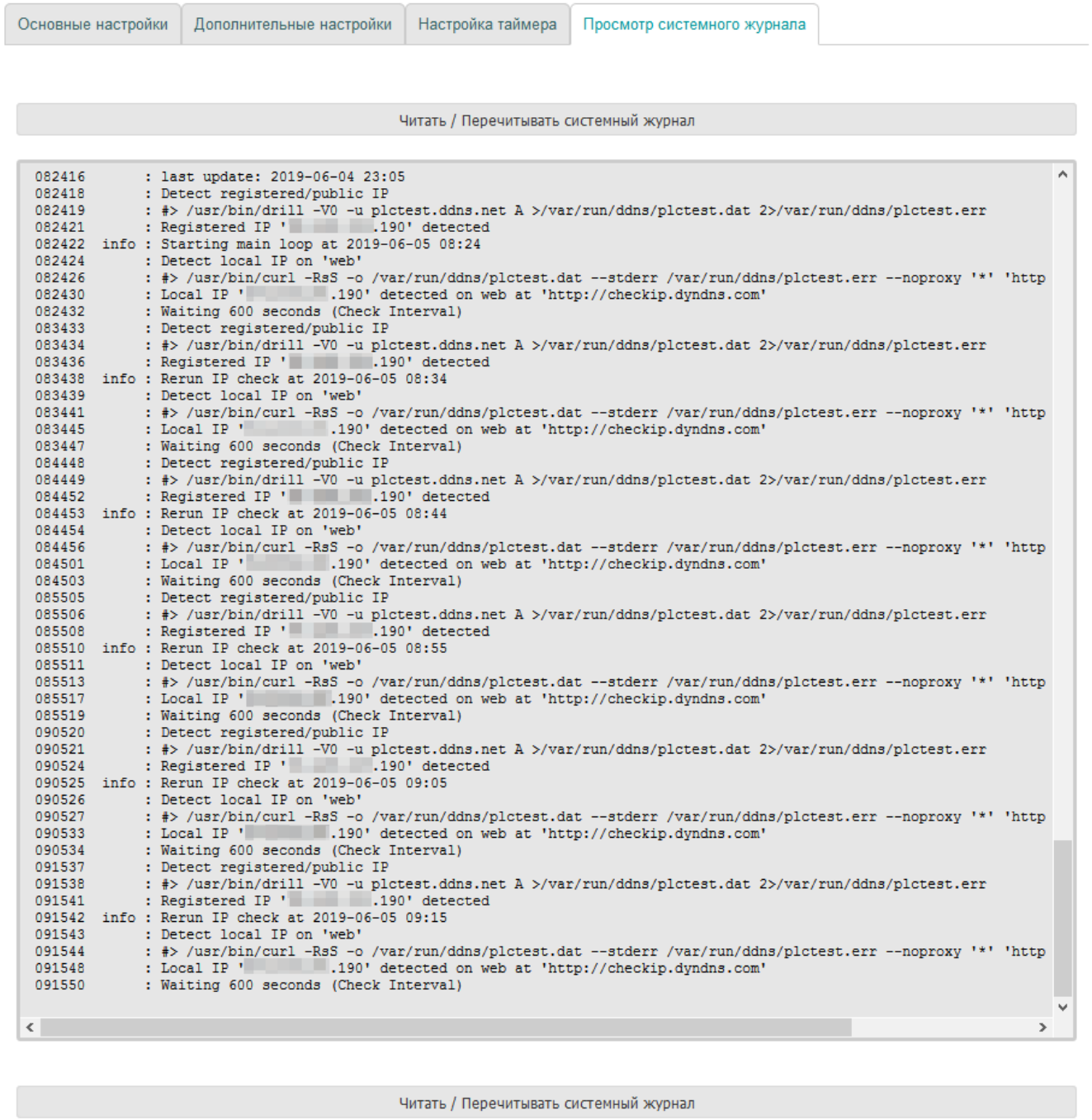


Рис. 6-15: Вкладка «Просмотр системного журнала» страницы редактирования DDNS записи

На вкладке «Просмотр системного журнала» отображается содержимое файла системного журнала данной DDNS записи.

Кнопки «Читать / перечитывать системный журнал» предназначены для перечитывания содержимого файла системного журнала.

6.1.2 Добавление DDNS записи

Под таблицей текущих DDNS записей на странице «DDNS» расположено текстовое поле с кнопкой «Добавить» справа от него (см. рисунок 6-16).

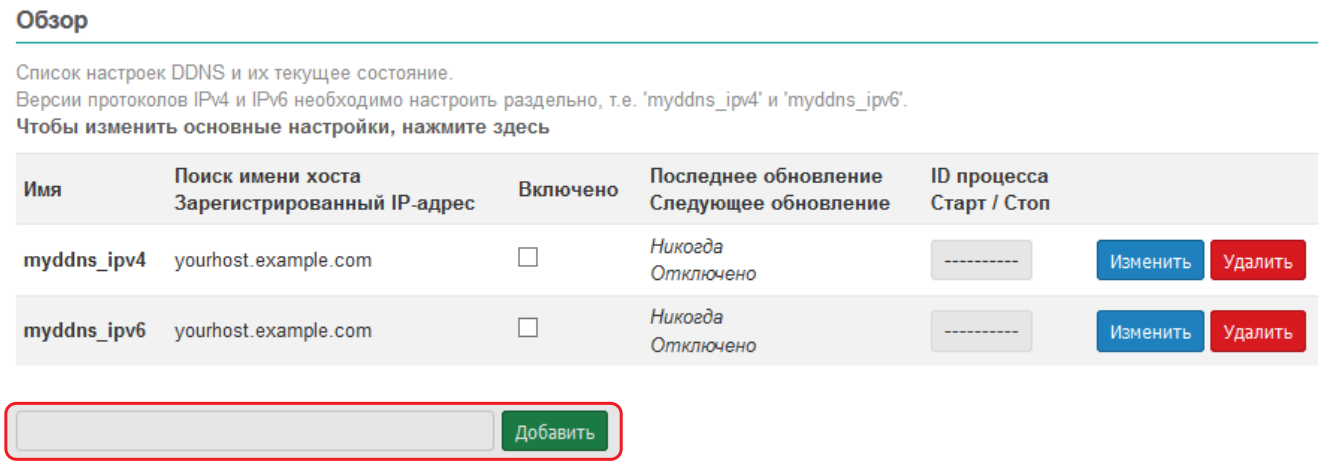


Рис. 6-16: Страница «DDNS». Кнопка добавления записи

Для добавления новой DDNS записи необходимо в текстовое поле ввести произвольное имя новой DDNS записи и нажать кнопку «Добавить». Вводимое произвольное имя новой записи должно быть уникальным и не совпадать с именами уже существующих записей.

После нажатия кнопки «Добавить» откроется страница редактирования новой DDNS записи. Редактирование DDNS записей подробно рассмотрено в разделе 6.1.1.

6.1.3 Удаление DDNS записи

Для удаления DDNS записи необходимо нажать кнопку «Удалить» для соответствующей записи в таблице на странице «DDNS» (см. рисунок 6-17).

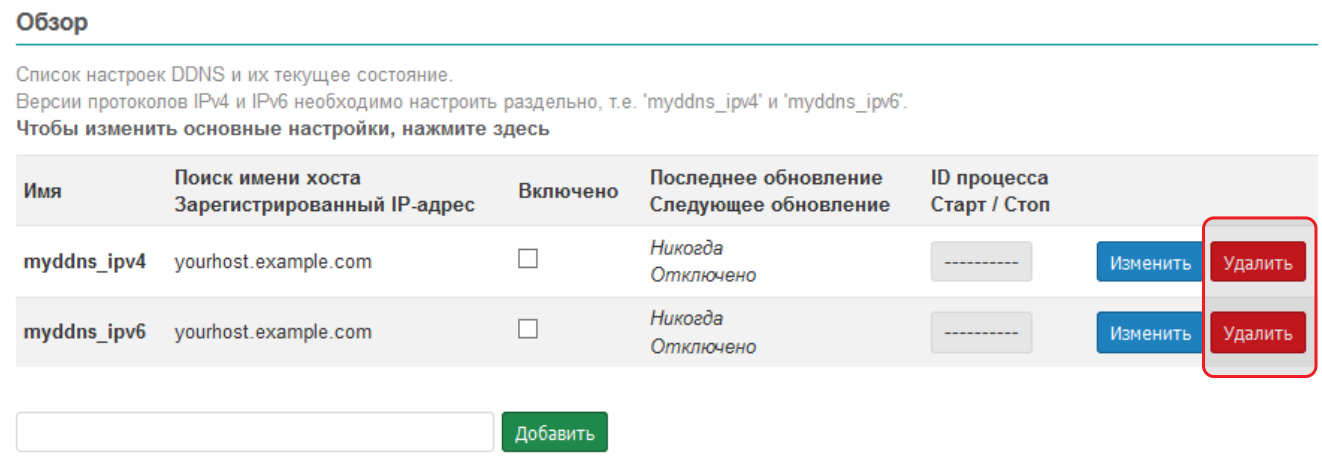


Рис. 6-17: Страница «DDNS». Кнопки удаления записи

6.2 STP/RSTP

Данный раздел присутствует только в Web-интерфейсе управления контроллеров ПЛК210.

На странице «STP/RSTP» производится мониторинг состояния и настройка службы STP/RSTP. Внешний вид страницы «STP/RSTP» показан на рисунке 6-18.

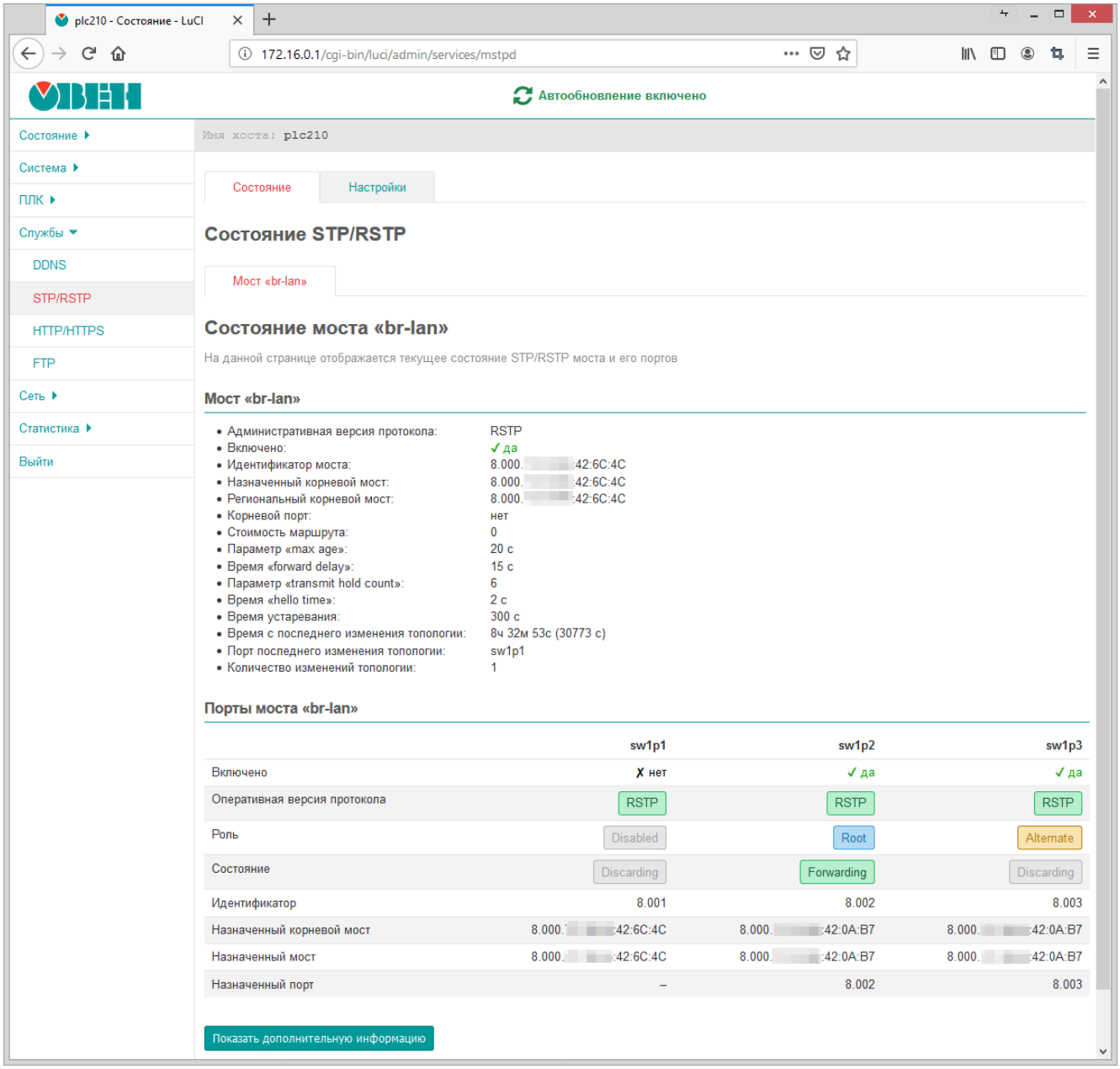


Рис. 6-18: Страница «STP/RSTP»

Состояние и настройки службы STP/RSTP разделены на соответствующие вкладки, расположенные в верхней части страницы (см. рисунок 6-18):

- «Состояние» (см. раздел 6.2.1);
- «Настройки» (см. раздел 6.2.2).

С более подробной информацией об использовании устройства ПЛК210 в сетях Ethernet с поддержкой протоколов STP/RSTP можно ознакомиться в справочном руководстве [1] и руководстве пользователя [2].

6.2.1 Состояние

На вкладке «Состояние» страницы «STP/RSTP» отображается состояние всех мостов, контролируемых службой STP/RSTP, и их портов. Вкладка «Состояние» разделена на три части (см. рисунок 6-19):

1) вкладки выбора моста, для которого необходимо отобразить информацию о текущем состоянии;
2) состояние выбранного моста в виде списка параметров моста и их текущих значений;
3) состояние портов выбранного моста в виде таблицы.

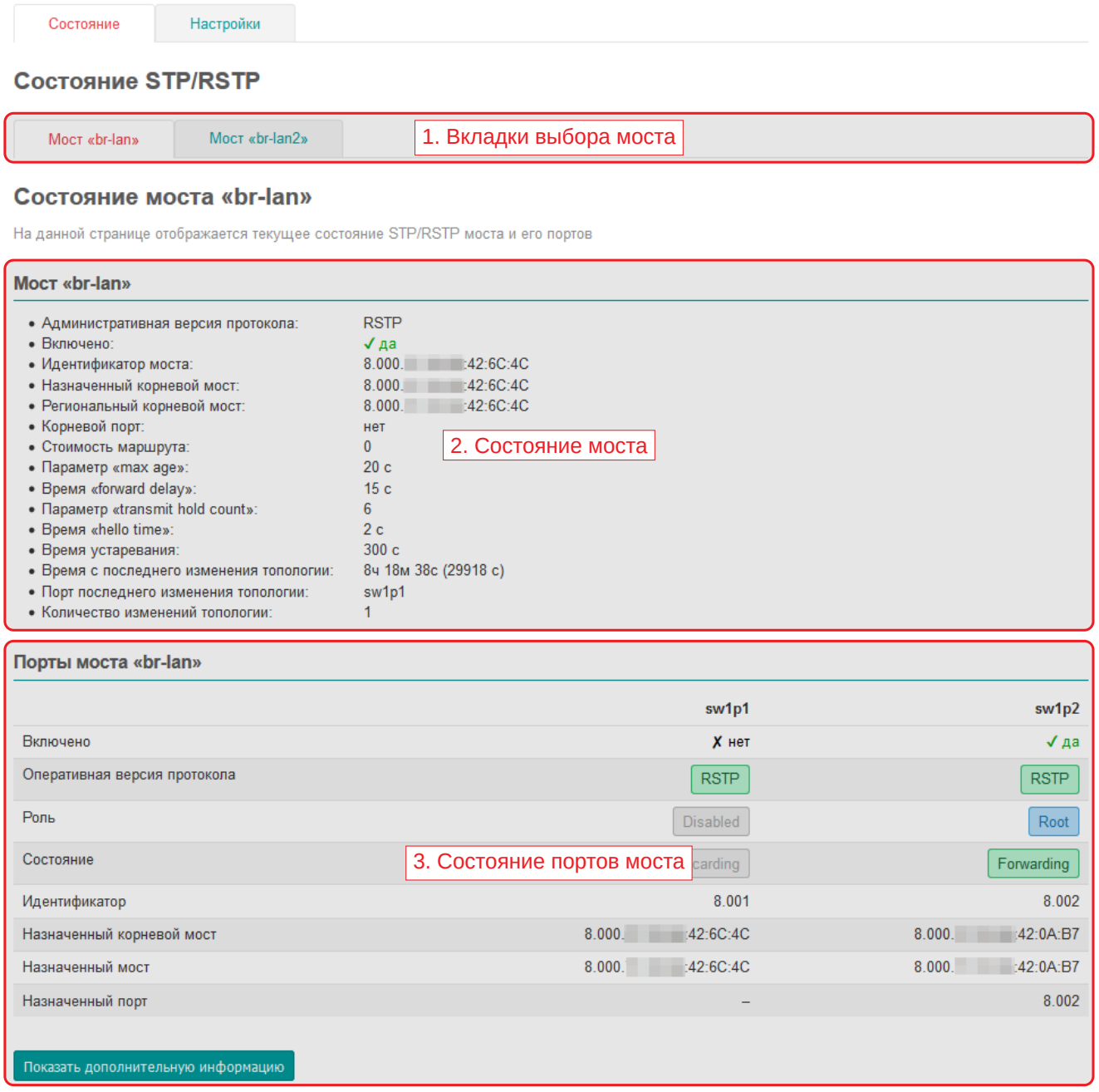


Рис. 6-19: Страница «STP/RSTP». Вкладка «Состояние»

Мост, для которого отображается состояние, выбирается при помощи вкладок с названием моста (позиция 1 на рисунке 6-19).

В области состояния моста (позиция 2 на рисунке 6-19) отображаются следующие параметры:

- «Административная версия протокола» — сконфигурированная администратором версия протокола:
  - STP;
  - RSTP;
- «Включено» — состояние включения моста (включён или нет);
- «Идентификатор моста» — идентификатор моста, состоящий из приоритета моста и собственного MAC-адреса моста. Отображается в формате:

  ```
  2.000.11:22:33:8C:37:C3
  ```

  где:
  - `2.000` — приоритет моста;
  - `11:22:33:8C:37:C3` — MAC-адрес моста.
- «Назначенный корневой мост» — идентификатор текущего назначенного корневого моста. Формат отображаемого значения соответствует формату параметра «Идентификатор моста»;
- «Региональный корневой мост» — идентификатор текущего регионального корневого моста. Формат отображаемого значения соответствует формату параметра «Идентификатор моста»;
- «Корневой порт» — имя системного интерфейса порта, который является корневым (в скобках отображается индекс порта в мосту). Отображается только в том случае, если мост сам не является корневым на текущий момент;
- «Стоимость маршрута» — текущая стоимость маршрута до корневого моста;
- «Параметр „max age“» — текущее значение параметра «max age». Определяет максимальный возраст информации, передаваемой через мост тогда, когда он является корневым;
- «Время „forward delay“» — текущее значение параметра «forward delay». Параметр определяет время перехода корневых (Root) и назначенных (Designated) портов моста в состояние Forwarding;
- «Параметр „transmit hold count“» — текущее значение параметра «transmit hold delay»;
- «Время „hello time“» — текущее значение времени «hello time». Определяет интервал времени между периодическими отправками конфигурационных сообщений BPDU в назначенные (Designated) порты;
- «Время устаревания» — текущее значение времени устаревания для моста (ageing time). Определяет время жизни записей (в секундах) в динамической таблице MAC-адресов;
- «Время с последнего изменения топологии» — время, прошедшее с последнего изменения топологии;
- «Порт последнего изменения топологии» — имя порта, инициировавшего последнее изменение топологии;
- «Количество изменений топологии» — количество изменений топологии.

В области состояния портов моста (позиция 3 на рисунке 6-19) расположена таблица, столбцы которой представляют собой порты моста, а в строках перечислены отображаемые параметры:

- «Включено» — состояние порта (включён или нет);
- «Оперативная версия протокола» — текущая оперативная версия протокола на порту.

  При совпадении оперативной версии протокола порта с административной версией протокола моста, значение отображается зелёным (см. рисунок 6-20(а)). Если оперативная версия протокола отличается от административной версии протокола моста (например, при деградации автоматической RSTP до STP), то значение будет отображено красным (см. рисунок 6-20(б));

(а) Оперативное состояние совпадает с административным

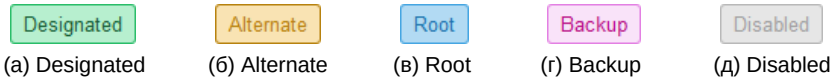
(б) Оперативное состояние отличается от административного

Рис. 6-20: Отображение оперативной версии протокола порта моста

- «Роль» — текущая STP/RSTP роль порта. Порт может иметь одну из следующих ролей:
  - Designated — назначенный порт (рисунок 6-21(а));
  - Alternate — альтернативный порт (рисунок 6-21(б));

- Root — корневой порт (рисунок 6-21(в));
- Backup — резервный порт (рисунок 6-21(г));
- Disabled — порт отключён (рисунок 6-21(д)).

Каждая роль порта отображается своим цветом, как показано на рисунке 6-21.

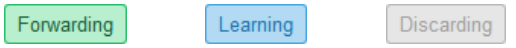


(а) Designated (б) Alternate (в) Root (г) Backup (д) Disabled

Рис. 6-21: Отображение ролей порта

- «Состояние» — текущее STP/RSTP состояние порта. Порт может находится в одном из трёх состояний:
  - Discarding — состояние отбрасывания данных (в случае протокола STP будет также отображаться для состояний Disabled, Blocking и Listening);
  - Learning — состояние обучения;
  - Forwarding — состояние передачи данных;

  Каждое состояние порта отображается своим цветом, как показано на рисунке 6-22.



(а) Forwarding (б) Learning (в) Discarding

Рис. 6-22: Отображение состояний порта

- «Идентификатор» — идентификатор порта, состоящий из приоритета порта и номера порта. Отображается в формате:

  ```
  8.001
  ```

  где:
  - 8 — приоритет порта;
  - 001 — номер порта.
- «Назначенный корневой мост» — идентификатор текущего назначенного корневого моста на данном порту. Формат отображаемого значения соответствует формату параметра моста «Идентификатор моста»;
- «Назначенный мост» — идентификатор текущего назначенного моста на данном порту. Формат отображаемого значения соответствует формату параметра моста «Идентификатор моста»;
- «Назначенный порт» — идентификатор порта текущего назначенного моста на данном порту. Формат отображаемого значения соответствует формату параметра порта «Идентификатор».

В нижней части таблицы расположена кнопка «Показать дополнительную информацию», которая позволяет расширить отображаемую информацию в таблице следующими дополнительными параметрами:

- «Стоимость маршрута порта» — текущая стоимость маршрута порта;
- «Административное пограничное состояние» — признак административной установки режима пограничного порта (Edge Port). Возможны следующие значения:
  - «да» — режим пограничного порта включён;
  - «нет» — режим пограничного порта выключен;
- «Автоматическое пограничное состояние» — признак режима автоматического определения пограничного порта (Edge Port). Возможны следующие значения:
  - «да» — включён;
  - «нет» — выключен;
- «Оперативное пограничное состояние» — признак активного (оперативного) режима пограничного порта (Edge Port). Возможны следующие значения:
  - «да» — порт находится в режиме пограничного порта (Edge Port);

  - «нет» — порт не является пограничным (non-Edge Port);
- «Административное P2P состояние» — признак административной установки режима Point-to-Point подключения для порта. Может принимать одно из следующих значений:
  - «да» — Point-to-Point подключение;
  - «нет» — не Point-to-Point подключение;
  - «авто» — автоматическое определение;
- «Оперативное P2P состояние» — признак, определяющий является ли текущее подключение порта Point-to-Point. Возможны следующие значения:
  - «да» — Point-to-Point подключение;
  - «нет» — не Point-to-Point подключение;
- «Отправлено BPDU» — количество отправленных BPDU пакетов в данный порт;
- «Получено BPDU» — количество полученных BPDU пакетов на данном порту;
- «Отправлено TCN» — количество отправленных TCN пакетов в данный порт;
- «Получено TCN» — количество полученных TCN пакетов на данном порту.

На рисунке 6-23 приведён пример внешнего вида таблицы состояния портов моста с включёнными дополнительными параметрами.

Порты моста «br-lan»

	sw1p1	sw1p2	sw1p3
Включено	✗ нет	✓ да	✓ да
Оперативная версия протокола	RSTP	RSTP	RSTP
Роль	Disabled	Root	Alternate
Состояние	Discarding	Forwarding	Discarding
Идентификатор	8.001	8.002	8.003
Назначенный корневой мост	8.000. :42:6C:4C	8.000. :42:0A:B7	8.000. :42:0A:B7
Назначенный мост	8.000. :42:6C:4C	8.000. :42:0A:B7	8.000. :42:0A:B7
Назначенный порт	–	8.002	8.003
Стоимость маршрута порта	200000000	200000	200000
Административное пограничнное состояние	✗ нет	✗ нет	✗ нет
Автоматическое пограничное состояние	✓ да	✓ да	✓ да
Оперативное пограничное состояние	✗ нет	✗ нет	✗ нет
Административное P2P состояние	Автоматически	Автоматически	Автоматически
Оперативное P2P состояние	✗ нет	✓ да	✓ да
Отправлено BPDU	–	4	4
Получено BPDU	–	32748	32748
Отправлено TCN	–	3	–
Получено TCN	–	2	2

Рис. 6-23: Страница «STP/RSTP». Расширенная таблица состояния портов моста

6.2.2 Настройки

На вкладке «Настройки» страницы «STP/RSTP» расположены настройки службы STP/RSTP. Внешний вид страницы настроек показан на рисунке 6-24.

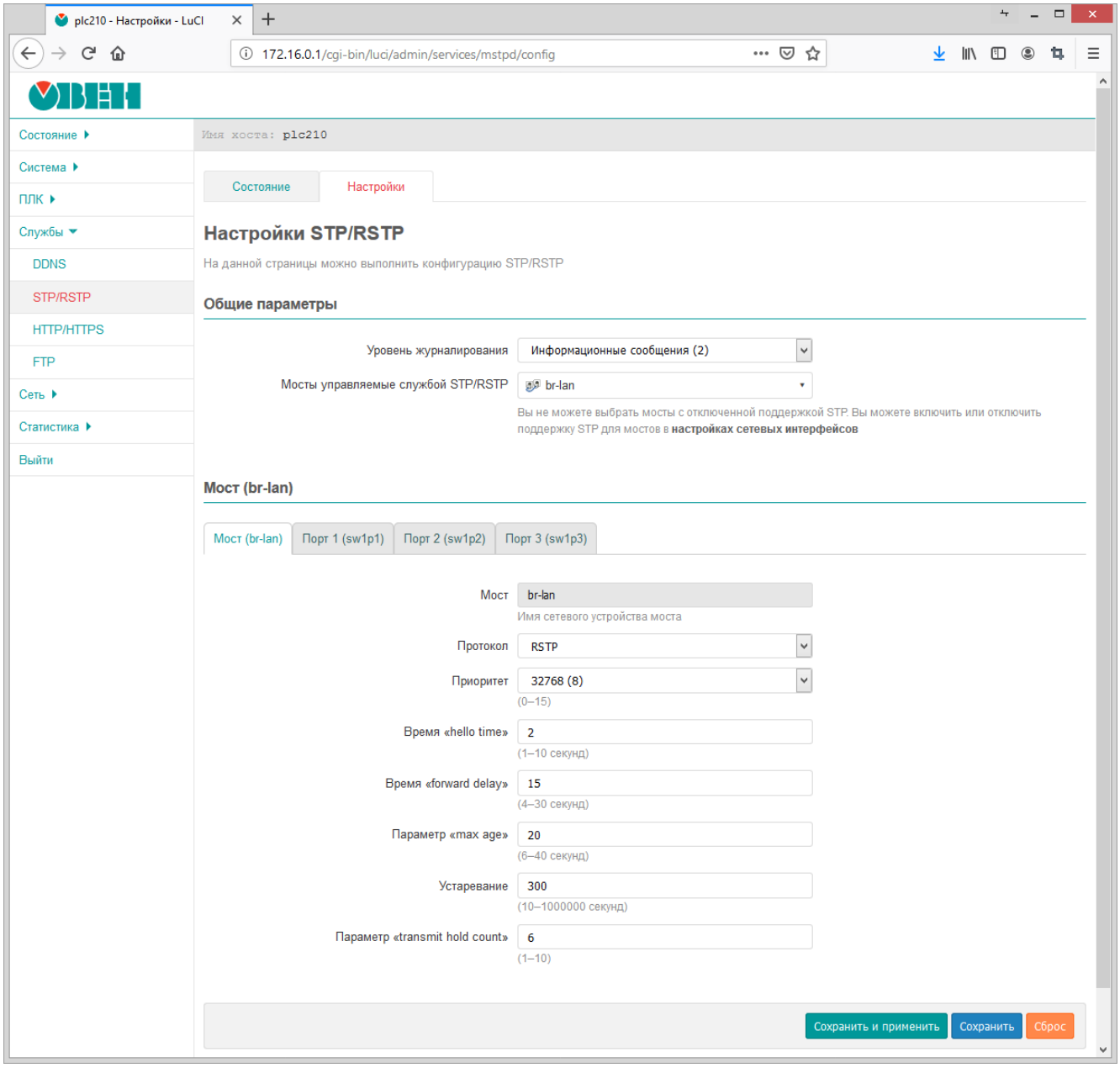


Рис. 6-24: Страница «STP/RSTP». Вкладка «Настройки»

Страница настроек разделена на подразделы общих настроек и подразделы настроек контролируемых службой STP/RSTP мостов.

6.2.2.1 Общие настройки

При помощи выпадающего списка «Уровень журналирования» выбирается уровень журналирования службы STP/RSTP. Доступны следующие уровни:

- «Отключено» — журналирование отключено;
- «Ошибки» — журналируются только сообщения об ошибках;
- «Информационные сообщения» — журналируются только информационные сообщения и сообщения об ошибках;

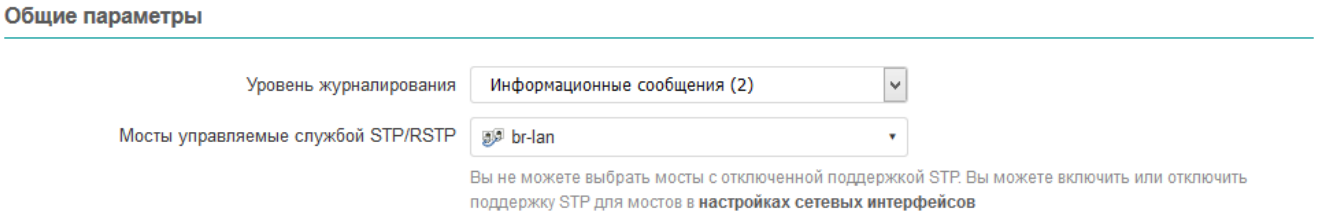


Рис. 6-25: Общие настройки службы STP/RSTP

- «Отладочные сообщения» — журналируются все сообщения, включая отладочные, кроме сообщений о переходах машины состояний;
- «Переходы машины состояний» — журналируются все сообщения, в том числе о переходах машины состояний.

Список «Мосты управляемые службой STP/RSTP» предназначен для выбора мостов, которые должны управляться службой STP/RSTP. В этом списке отображаются лишь те мосты, для которых включена поддержка STP в настройках сетевых интерфейсов (см. раздел 7.1.1.2).

Если мост не выбран в списке «Мосты управляемые службой STP/RSTP», но при этом включена опция поддержки STP в настройках сетевых интерфейсов, то работа протокола STP для такого моста будет обеспечиваться встроенным в Linux ядро алгоритмом поддержки STP, а не службой STP/RSTP. Настройка параметров STP для таких мостов, на странице настроек службы STP/RSTP невозможна.

6.2.2.2 Настройки моста и его портов

Следом за общими настройками расположены подразделы настроек выбранных мостов и их портов.

Для настройки доступны лишь те мосты, которые выбраны для управления службой STP/RSTP в списке «Мосты управляемые службой STP/RSTP» общих настроек службы (см. раздел 6.2.2.1).

Настройки моста и его портов организованы в виде вкладок. В первой вкладке расположены настройки моста (см. рисунок 6-26). В последующих вкладках размещены настройки для портов моста (см. рисунок 6-27), где каждому порту соответствует своя вкладка.

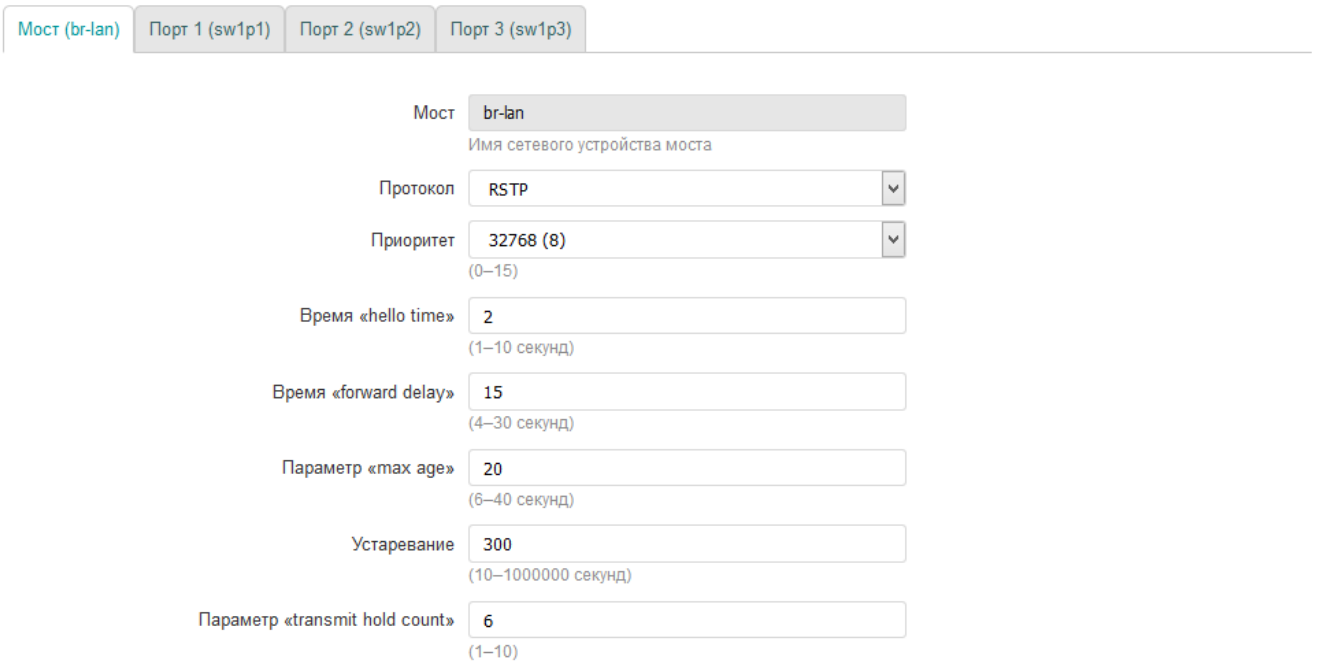


Рис. 6-26: Настройки моста, управляемого службой STP/RSTP

Во вкладке настроек моста размещены следующие настройки (см. рисунок 6-26):

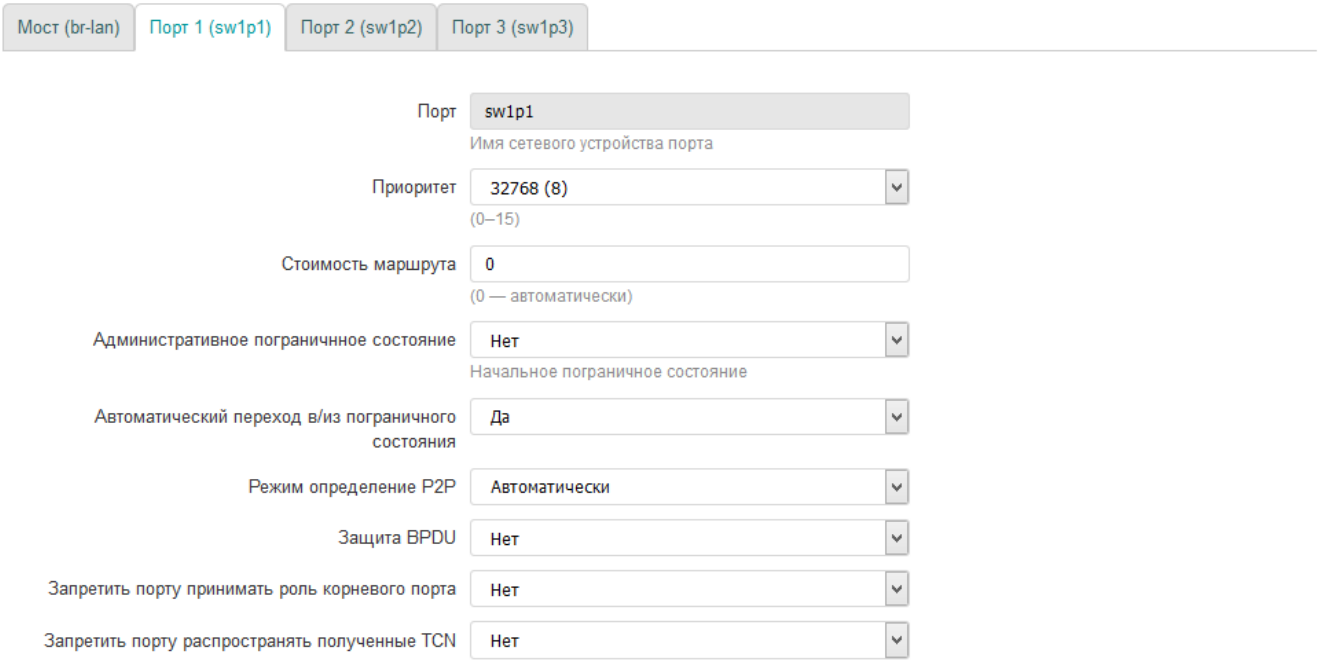


Рис. 6-27: Настройки портов моста, управляемого службой STP/RSTP

- «Мост» — имя системного сетевого устройства моста;
- «Протокол» — выбор административной версии протокола. Поддерживаемые протоколы:
  - STP;
  - RSTP;
- «Приоритет» — выбор приоритета моста;
- «Время „hello time“» — установка значения времени «hello time», которое определяет интервал между отправками BPDU сообщений;
- «Время „forward delay“» — установка значения времени «forward delay»;
- «Параметр „max age“» — установка значения параметра «max age»;
- «Устаревание» — установка значения времени устаревания (ageing time);
- «Параметр „transmit hold count“» — установка значения параметра «transmit hold count».

Во вкладках настроек портов моста размещены следующие настройки (см. рисунок 6-27):

- «Порт» — имя системного сетевого устройства порта;
- «Приоритет» — выбор приоритета порта;
- «Стоимость маршрута» — установка стоимости маршрута порта. Для автоматического определения используется значение 0;
- «Административное пограничное состояние» — административная установка режима пограничного порта (Edge Port). Возможные значения:
  - «да» — режим пограничного порта включён;
  - «нет» — режим пограничного порта выключен.
- «Автоматический переход в/из пограничного состояния» — установка режима автоматического определения пограничного порта (Edge Port). Возможные значения:
  - «да» — включён;
  - «нет» — выключен.
- «Режим определения P2P» — административная установка режима Point-to-Point подключения для порта. Возможные значения:
  - «да» — Point-to-Point подключение;
  - «нет» — не Point-to-Point подключение;
  - «авто» — автоматическое определение;

- «Защита BPDU» — включение или отключение функции BPDU Guard на порту. Возможные значения:
  - «да» — функция BPDU Guard включена;
  - «нет» — функция BPDU Guard выключена (значение по умолчанию).
- «Запретить порту принимать роль корневого порта» — настройка позволяет запретить порту принимать роль корневого (Root) порта. Возможные значения:
  - «да» — порту запрещено принимать роль корневого порта;
  - «нет» — порт может быть корневым (значение по умолчанию).
- «Запретить порту распространять полученные TCN» — настройка позволяет запретить дальнейшее распространение TCN пакетов принятых на данном порту. Возможные значения:
  - «да» — распространение TCN запрещено;
  - «нет» — распространение TCN разрешено (значение по умолчанию).

6.3 HTTP/HTTPS

На странице «HTTP/HTTPS» раздела «Службы» расположены настройки лёгкого однопоточного Web-сервера «uHTTPd» (см. рисунок 6-28).

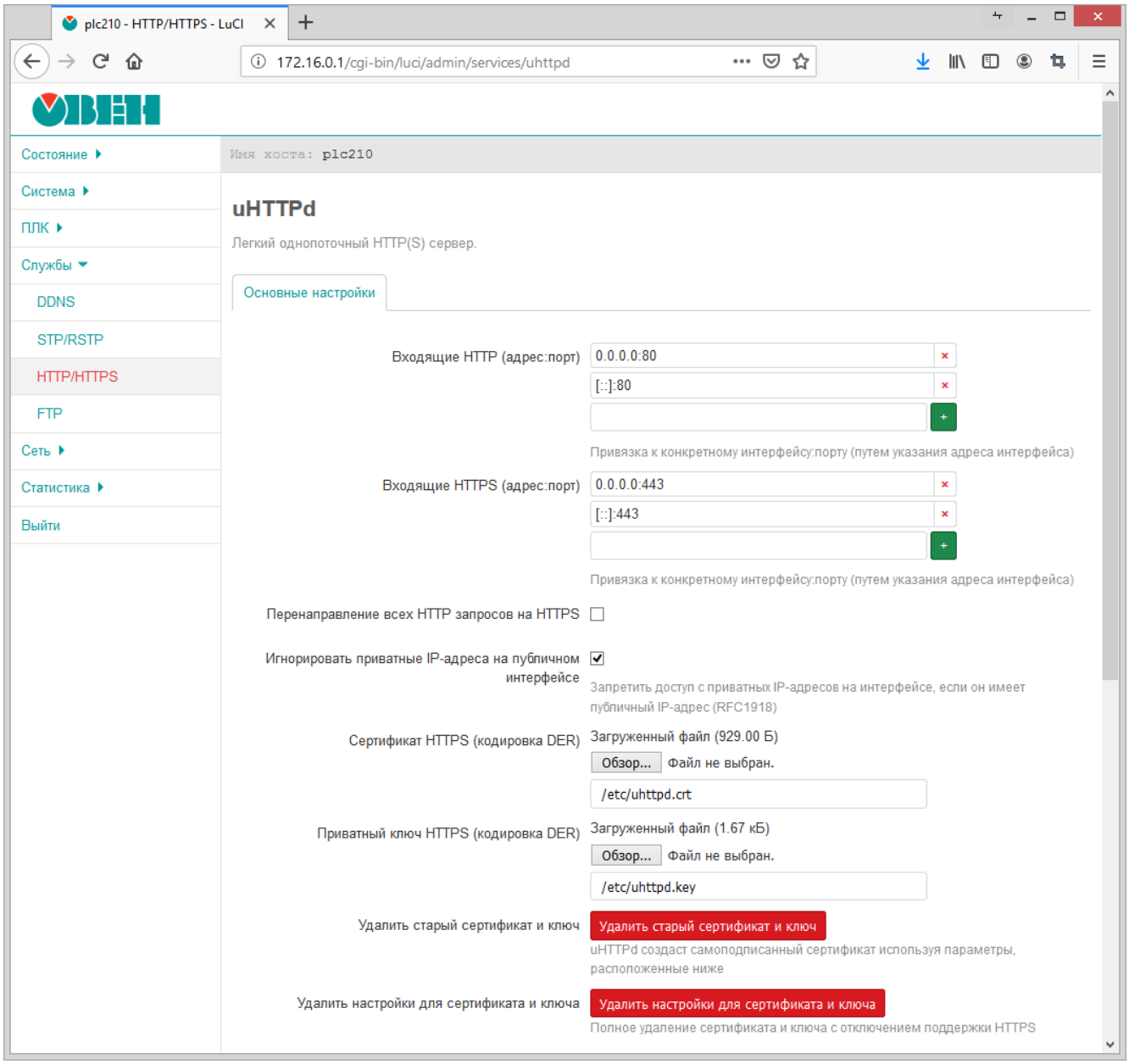


Рис. 6-28: Страница «HTTP/HTTPS»

На странице «HTTP/HTTPS» представлены следующие основные настройки:

- «Входящие HTTP (адрес:порт)» — адрес и порт для входящих запросов по протоколу HTTP (по умолчанию используется порт 80);
- «Входящие HTTPS (адрес:порт)» — адрес и порт для входящих запросов по протоколу HTTPS (по умолчанию используется порт 443);
- «Перенаправление всех HTTP запросов на HTTPS» — установка данного параметра позволяет перенаправлять все входящие запросы по протоколу HTTP на HTTPS;
- «Игнорировать приватные IP-адреса на публичном интерфейсе» — установка данного параметра позволяет запретить доступ с приватных IP-адресов на интерфейсе, если он имеет публичный IP-адрес (RFC1918 [10]);
- «Сертификат HTTPS (кодировка DER)» — путь к файлу сертификата в файловой системе устройства (по умолчанию «/etc/uhttpd.crt»). При помощи кнопки «Обзор...» возможно выполнить загрузку нового файла сертификата в формате DER;

- «Приватный ключ HTTPS (кодировка DER)» — путь к файлу приватного ключа на файловой системе устройства (по умолчанию «/etc/uhttpd.key»). При помощи кнопки «Обзор...» возможно выполнить загрузку нового файла приватного ключа в формате DER;
- «Удалить старый сертификат и ключ» — нажатие этой кнопки удаляет существующий сертификат и приватный ключ. При этом будет выполнена генерация нового самоподписанного сертификата с использованием настроек из подраздела «Параметры самоподписанного сертификата» (см. раздел 6.3.1);
- «Удалить настройки для сертификата и ключа» — нажатие этой кнопки удаляет существующий сертификат и приватный ключ, а также отключает поддержку протокола HTTPS.

6.3.1 Параметры самоподписанного сертификата

В подразделе «Параметры самоподписанного сертификата» страницы «HTTP/HTTPS» представлены настройки, используемые для генерации самоподписанного сертификата службы HTTP/HTTPS-сервера (см. рисунок 6-29).

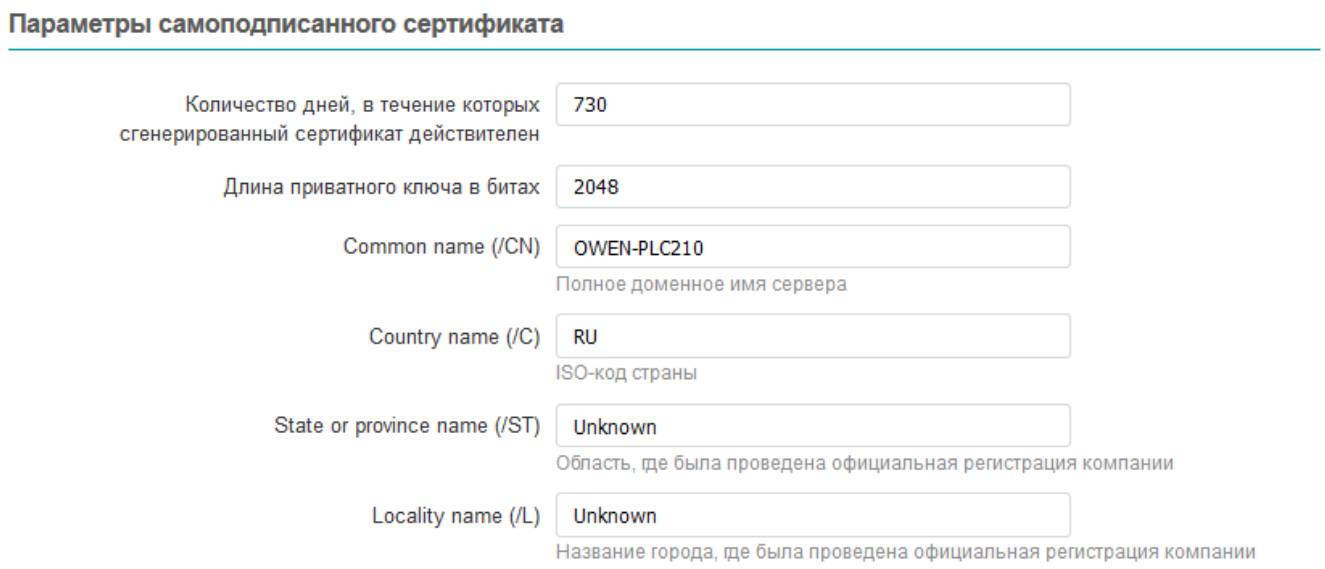


Рис. 6-29: Страница «HTTP/HTTPS». Параметры самоподписанного сертификата

Автоматическая генерация самоподписанного сертификата и приватного ключа выполняется при первом включении устройства или в случае удаления существующего сертификата или приватного ключа.

Для конфигурации доступны следующие настройки:

- «Количество дней, в течение которых сгенерированный сертификат действителен» — срок действия сертификата в днях (по умолчанию 730);
- «Длина приватного ключа в битах» — длина приватного ключа шифрования в битах (по умолчанию 2048);
- «Common name (/CN)» — полное доменное имя сервера, имя хоста;
- «Country name (/C)» — двухбуквенный ISO-код страны;
- «State or province name (/ST)» — область, где была проведена официальная регистрация компании;
- «Locality name (/L)» — название города, где была проведена официальная регистрация компании.

6.4 FTP

На странице «FTP» раздела «Службы» расположены настройки FTP-сервера. Внешний вид страницы «FTP» показан на рисунке 6-30.

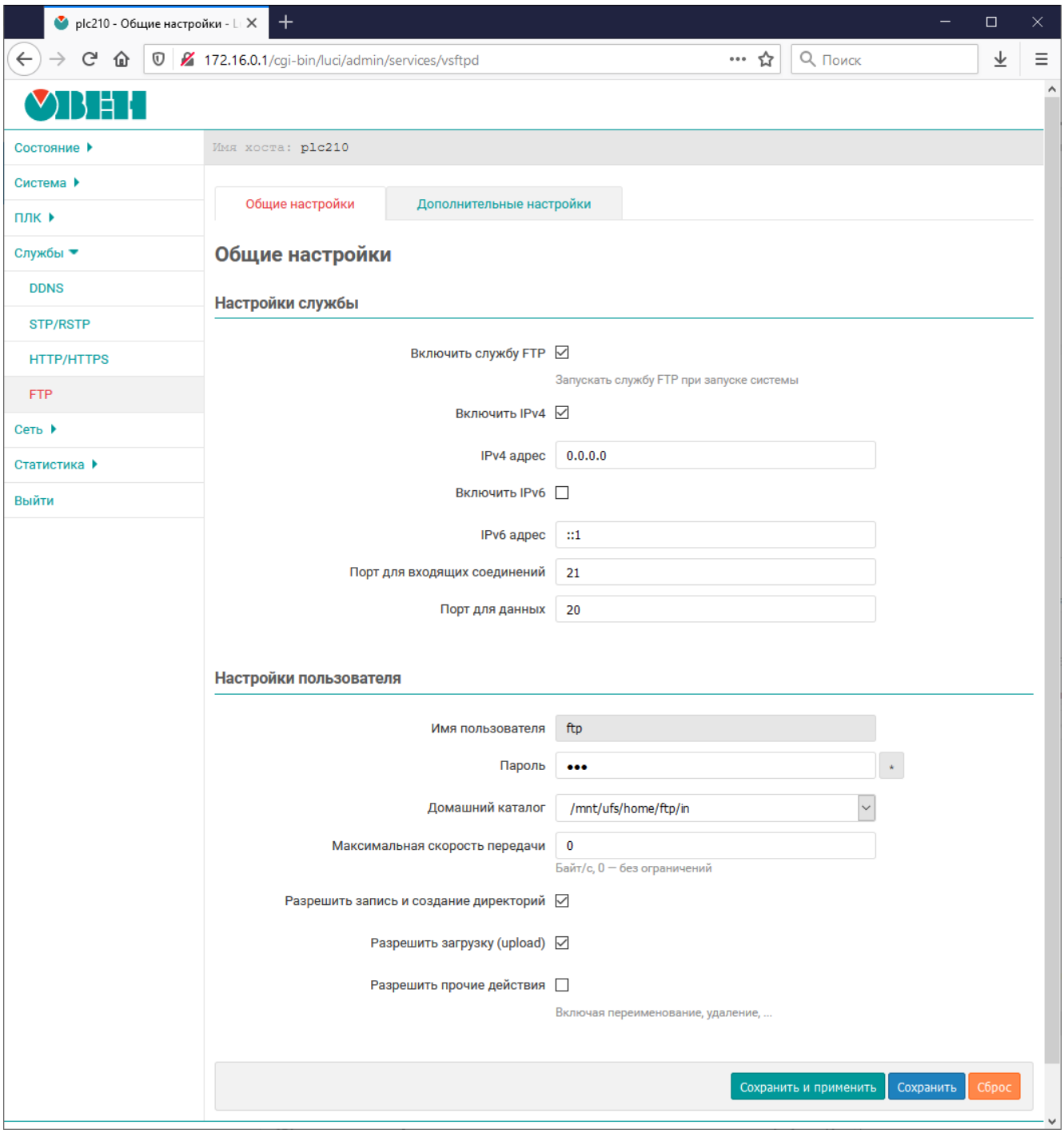


Рис. 6-30: Страница «FTP». Общие настройки

В приложении Б приводится пример выполнения подключения к устройству по протоколу FTP.

Настройки FTP-сервера разделены на две вкладки:

- «Общие настройки» (см. раздел 6.4.1);
- «Дополнительные настройки» (см. раздел 6.4.2).

6.4.1 Общие настройки

К общим настройкам FTP-сервера (см. рисунок 6-30) относятся настройки службы FTP-сервера и настройки пользователя для доступа к содержимому FTP-сервера.

6.4.1.1 Настройки службы

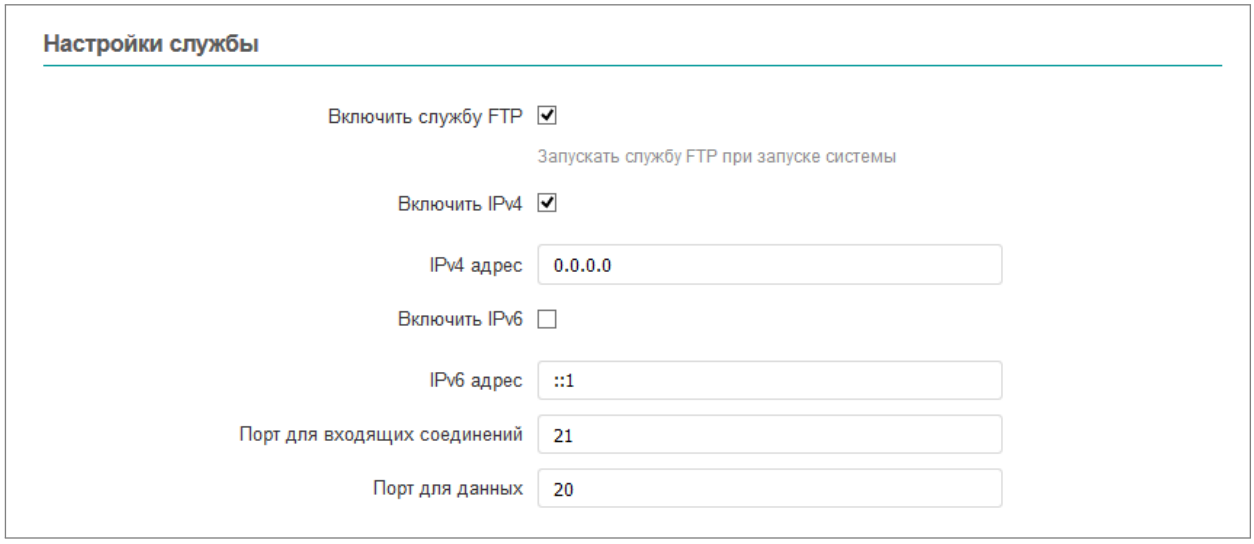


Рис. 6-31: Страница «FTP». Настройки службы

Настройки службы FTP-сервера находятся в подразделе «Настройки службы» (см. рисунок 6-31) и позволяют выполнить конфигурацию следующих параметров:

- «Включить службу FTP» — полное включение или отключение службы FTP. Если опция включена, то служба FTP будет автоматически запускаться при запуске системы;
- «Включить IPv4» — включение или отключение работы службы FTP по протоколу IP версии 4;
- «IPv4 адрес» — IP-адрес для входящих запросов к службе FTP-сервера с использованием IP протокола версии 4;
- «Включить IPv6» — включение или отключение работы службы FTP по протоколу IP версии 6;
- «IPv6 адрес» — IP-адрес для входящих запросов к службе FTP-сервера с использованием IP протокола версии 6;
- «Порт для входящих соединений» — номер порта для входящих запросов к службе FTP-сервера (по умолчанию 21);
- «Порт для данных» — номер порта для исходящих соединений типа PORT (по умолчанию 20).

6.4.1.2 Настройки пользователя

Настройки пользователя находятся в подразделе «Настройки пользователя» (см. рисунок 6-32) и позволяют выполнить конфигурацию следующих параметров:

- «Имя пользователя» — имя пользователя для доступа к содержимому FTP-сервера;
- «Пароль» — пароль пользователя для доступа к содержимому FTP-сервера (по умолчанию «ftp»);
- «Домашний каталог» — выбор домашнего каталога FTP-сервера;
- «Максимальная скорость передачи» — ограничение максимальной скорости передачи данных (байт в секунду). Значение 0 соответствует режиму работы без ограничений скорости;
- «Разрешить запись и создание директорий» — установка данного параметра разрешает пользователю запись файлов и создание директорий;
- «Разрешить загрузку (upload)» — установка данного параметра разрешает загружать файлы на FTP-сервер;
- «Разрешить прочие действия» — включение данного параметра разрешает не только создавать, но и удалять каталоги и файлы.

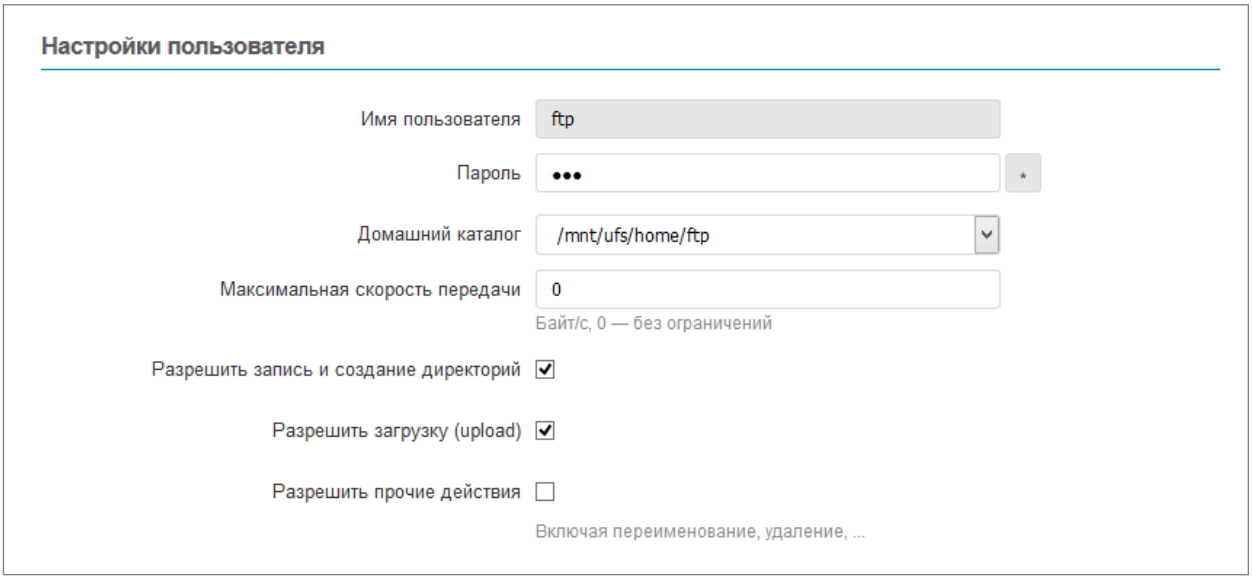


Рис. 6-32: Страница «FTP». Настройки пользователя

6.4.2 Дополнительные настройки

Дополнительные настройки расположены во вкладке «Дополнительные настройки». К дополнительным настройкам FTP-сервера относятся глобальные настройки, настройки подключения и настройки журналирования.

6.4.2.1 Глобальные настройки

Глобальные настройки FTP-сервера находятся в подразделе «Глобальные настройки» (см. рисунок 6-33) и позволяют выполнить конфигурацию следующих параметров:

- «Разрешить запись» — глобальное разрешение или запрет записи. Если настройка отключена, все запросы на запись будут вызывать ошибку доступа;
- «Разрешить скачивание (download)» — глобальное разрешение или запрет скачивания с FTP-сервера файлов. Если настройка отключена, все запросы на скачивание будут вызывать ошибку доступа;
- «Разрешить просмотр списка директорий» — глобальное разрешение или запрет просмотра списка файлов директорий. Если настройка отключена, все запросы на просмотр списка файлов каталога будут вызывать ошибку доступа;
- «Разрешить рекурсивный просмотр каталогов» — разрешение или запрет рекурсивного просмотра содержимого директорий (команда «`ls -R`»);
- «Показывать скрытые файлы (dot files)» — разрешение или запрет просмотра скрытых файлов (файлы, имя которых начинается с символа точки);
- «Режим создания файлов (umask)» — маска режима создания файлов (по умолчанию 022);

При указании значения в восьмеричном виде, необходимо помнить о необходимости префикса «0», иначе значение будет воспринято как десятичное число.

- «Сообщение сервера (FTP баннер)» — приветственное сообщение, которое выводится при подключении к FTP-серверу;
- «Включить сообщения при входе в каталоги» — включение отображения сообщений при переходе в каталоги. Каталог сканируется на наличие файла, имя которого указано в настройке «Имя файла сообщения директории»;
- «Имя файла сообщения директории» — имя файла с сообщением, который отображается при переходе в новый каталог, если включена настройка «Включить сообщения при входе в каталоги».

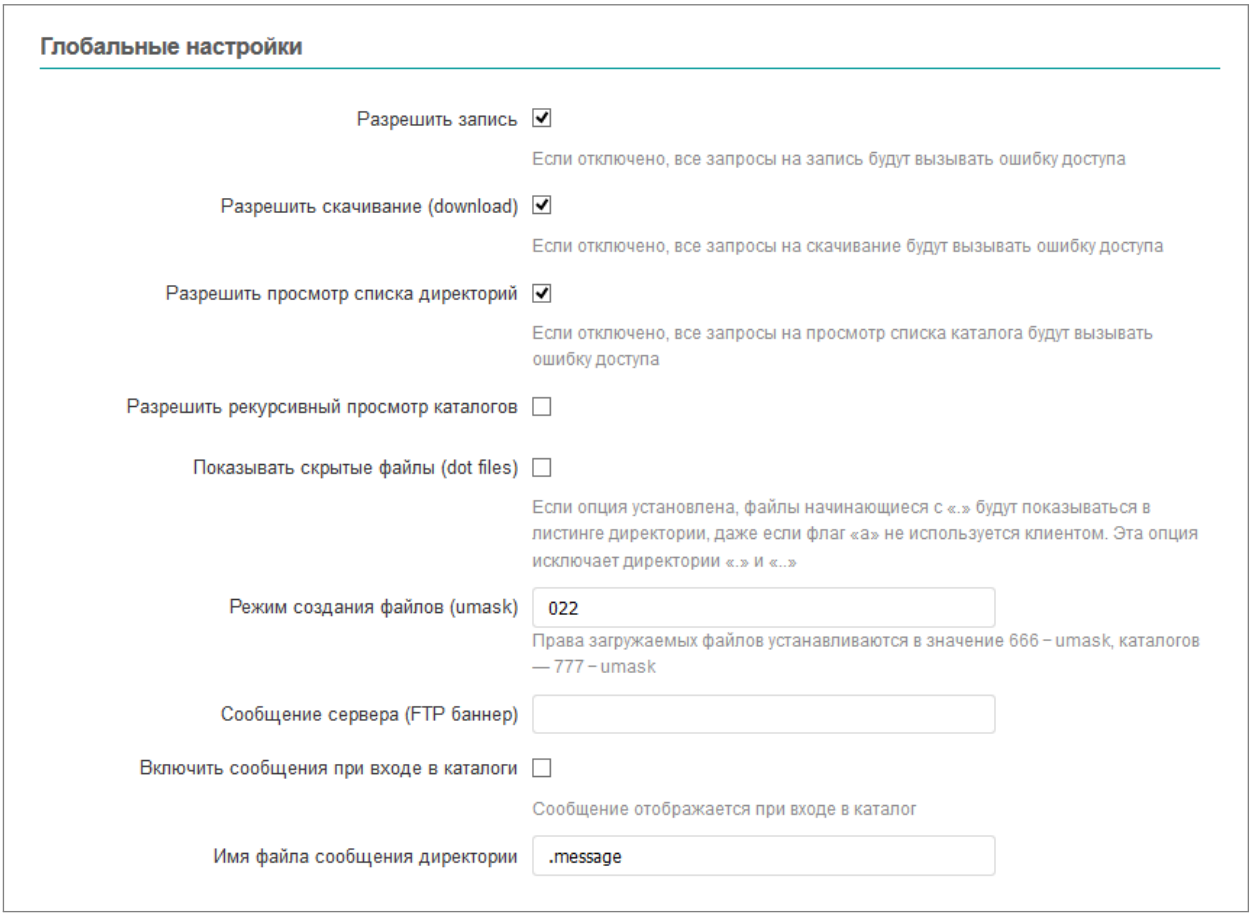


Рис. 6-33: Страница «FTP». Глобальные настройки

6.4.2.2 Настройки подключения

Настройки подключения FTP-сервера находятся в подразделе «Настройки подключения» (см. рисунок 6-34) и позволяют выполнить конфигурацию следующих параметров:

- «Включить режим PORT» — разрешает или запрещает метод PORT для получения информации о соединении;
- «Включить режим PASV» — разрешает или запрещает метод PASV для получения информации о соединении;
- «Номер порта, начиная с которого размещаются порты для PASV режима» — номер порта, начиная с которого размещаются порты для PASV режима (по умолчанию 10050);
- «Номер порта, до которого размещаются порты для PASV режима» — номер порта, до которого размещаются порты для PASV режима (по умолчанию 10100);
- «Режим ASCII» — режим ASCII передачи текстовых файлов. Доступны следующие варианты работы режима ASCII:
  - «Отключено» — режим ASCII отключён;
  - «Только для скачивания (download)» — режим ASCII используется только для скачиваемых с FTP-сервера файлов;
  - «Только для загрузки (upload)» — режим ASCII используется только для загружаемых на FTP-сервер файлов;
  - «Для скачивания и загрузки» — режим ASCII используется для скачиваемых с FTP-сервера и загружаемых на FTP-сервер файлов;
- «Таймаут неактивной сессии» — по истечению указанного таймаута, при неактивной сессии, будет выполняться принудительное отключение клиента;
- «Максимальное количество клиентов» — максимальное количество одновременно подключённых к FTP-серверу клиентов.

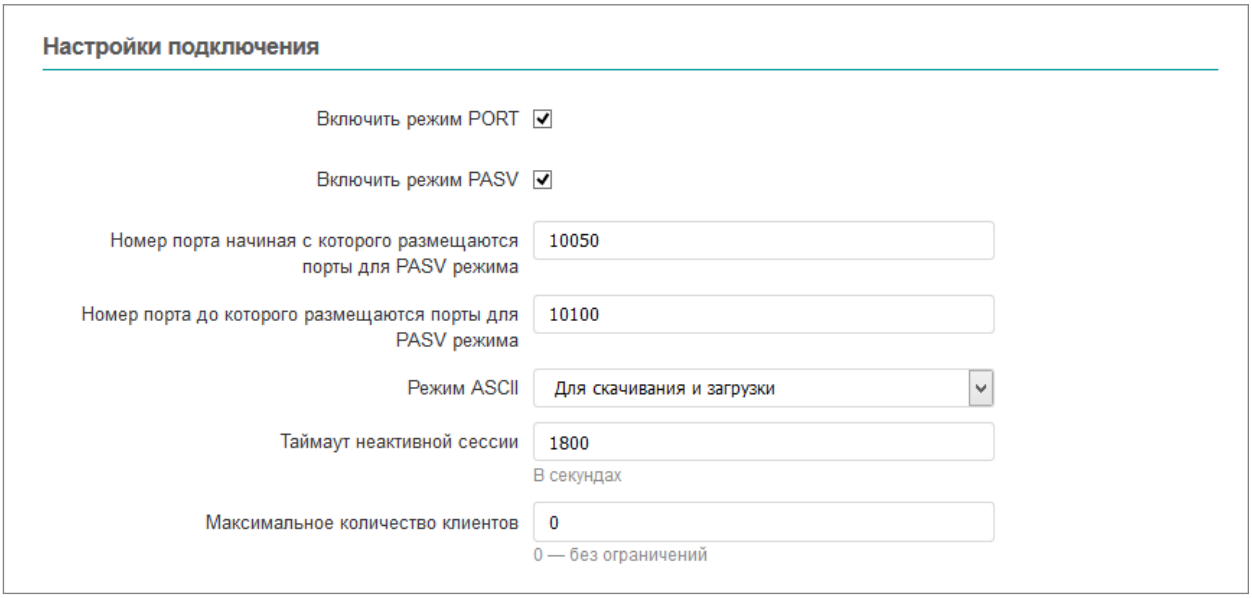


Рис. 6-34: Страница «FTP». Настройки подключения

6.4.2.3 Настройки журналирования

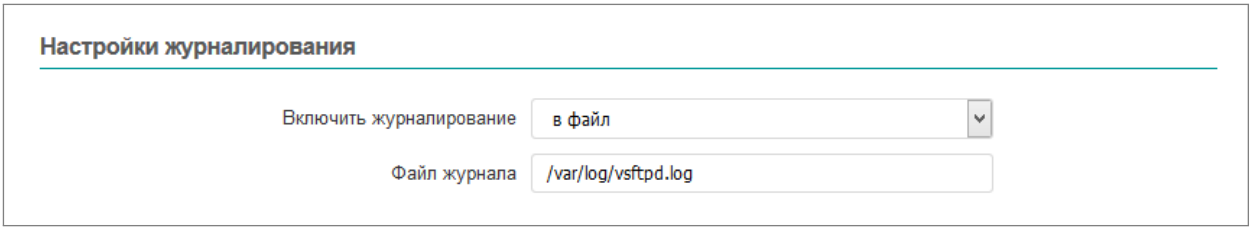


Рис. 6-35: Страница «FTP». Настройки журналирования

Настройки журналирования FTP-сервера находятся в подразделе «Настройки журналирования» (см. рисунок 6-35) и позволяют выполнить конфигурацию следующих параметров:

- «Включить журналирование» — выбор режима журналирования. Доступны следующие режимы:
  - «отключить» — журналирование отключено;
  - «в файл» — журналирование выполняется в файл, путь к которому указан в настройке «Файл журнала»;
  - «в syslog» — журналирование выполняется в системный журнал (syslog).

    Страница просмотра содержимого системного журнала описана в разделе 3.4 данного документа.
- «Файл журнала» — имя файла журнала для режима журналирования «в файл» (по умолчанию «/var/log/vsftpd.log»).

7 Сеть

7.1 Интерфейсы

Для управления сетевыми интерфейсами системы предназначена страница «Интерфейсы» раздела «Сеть». Внешний вид страницы «Интерфейсы» показан на рисунке 7-1.

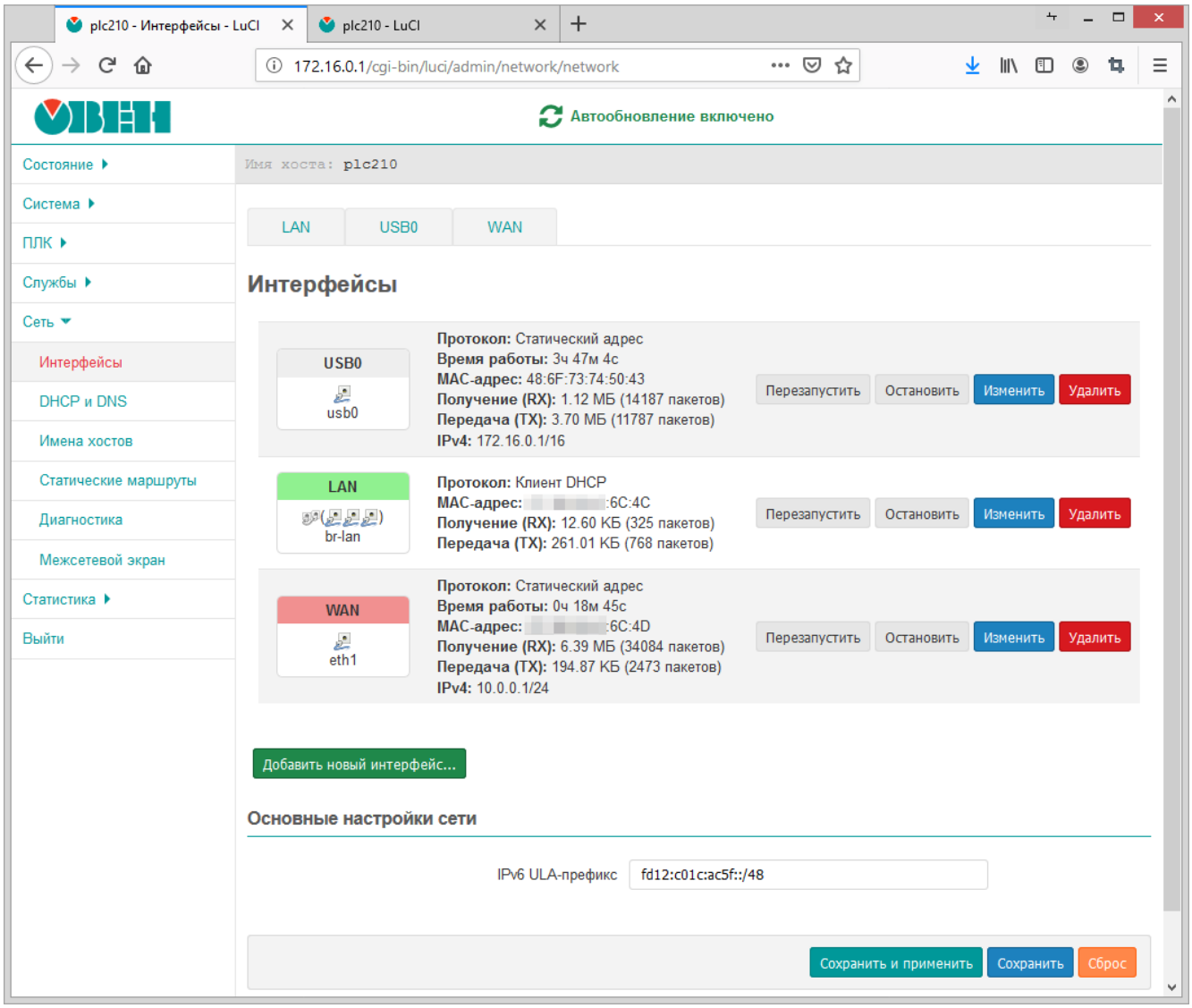


Рис. 7-1: Страница «Интерфейсы»

На самом верху страницы расположены ссылки в виде вкладок на страницы редактирования соответствующих интерфейсов (на рисунке 7-1 это интерфейсы «USB0», «WAN» и «LAN»). Редактирование интерфейсов подробно описано в разделе 7.1.1.

Далее на странице расположена таблица «Интерфейсы», в которой перечислены имеющиеся сетевые интерфейсы в системе. Для каждого интерфейса в первом столбце таблицы приведён значок, который содержит следующую информацию:

- название интерфейса;
- тип интерфейса (ethernet, мост, тоннель или беспроводной) и состояние подключения:
  - ethernet: (подключено), (отключено);
  - мост: (подключено), (отключено);
  - тоннель: (подключено), (отключено);
  - беспроводной: (подключено), (отключено).

- если интерфейс является мостом, то количество портов моста определяется количеством иконок интерфейсов, указанных в скобках;
- название системного сетевого интерфейса, соответствующего данному интерфейсу;
- прикреплённая к данному интерфейсу зона межсетевого экрана (определяется цветом фона заголовка значка).

Примеры значков сетевых интерфейсов приведены на рисунке 7-2.

(а) Значок интерфейса-моста «LAN» (б) Значок интерфейса «WAN»

Рис. 7-2: Значки сетевых интерфейсов

На рисунке 7-2(а) показан значок интерфейса «LAN», который является мостом, в который входят три ethernet порта (интерфейса). Системный сетевой интерфейс, соответствующий интерфейсу «LAN», имеет имя «br-lan». Зона межсетевого экрана, прикреплённая к данному интерфейсу, имеет светло-зелёный цвет, как и заголовок данного интерфейса. Интерфейс «LAN» находится в подключённом состоянии, так как тип интерфейса представлен цветной иконкой.

На рисунке 7-2(б) показан значок интерфейса «WAN», который является обычным ethernet интерфейсом. Системный сетевой интерфейс, соответствующий интерфейсу «WAN», имеет имя «eth1». Зона межсетевого экрана, прикреплённая к данному интерфейсу, имеет светло-красный цвет, как и заголовок данного интерфейса. Интерфейс «WAN» находится в отключённом состоянии, так как тип интерфейса представлен черно-белой иконкой.

Во втором столбце таблицы для каждого интерфейса выводится краткая информация и статистика в режиме реального времени:

- «Протокол» — протокол интерфейса.
- «Время работы» — время работы данного интерфейса.
- «MAC-адрес» — MAC-адрес интерфейса (если это применимо для протокола интерфейса).
- «Получение (RX)» — количество принятых байт (пакетов) с момента запуска.
- «Передача (TX)» — количество переданных байт (пакетов) с момента запуска.
- «IPv4» — текущий IPv4 адрес, назначенный интерфейсу (если назначен).
- «IPv6» — текущий IPv6 адрес, назначенный интерфейсу (если назначен).
- «IPv6-PD» — текущий IPv6 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 (см. раздел 7.1.1).
- «Удалить» — удаляет соответствующий интерфейс.

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

7.1.1 Редактирование интерфейсов

Внешний вид страницы редактирования сетевого интерфейса показан на рисунке 7-3.

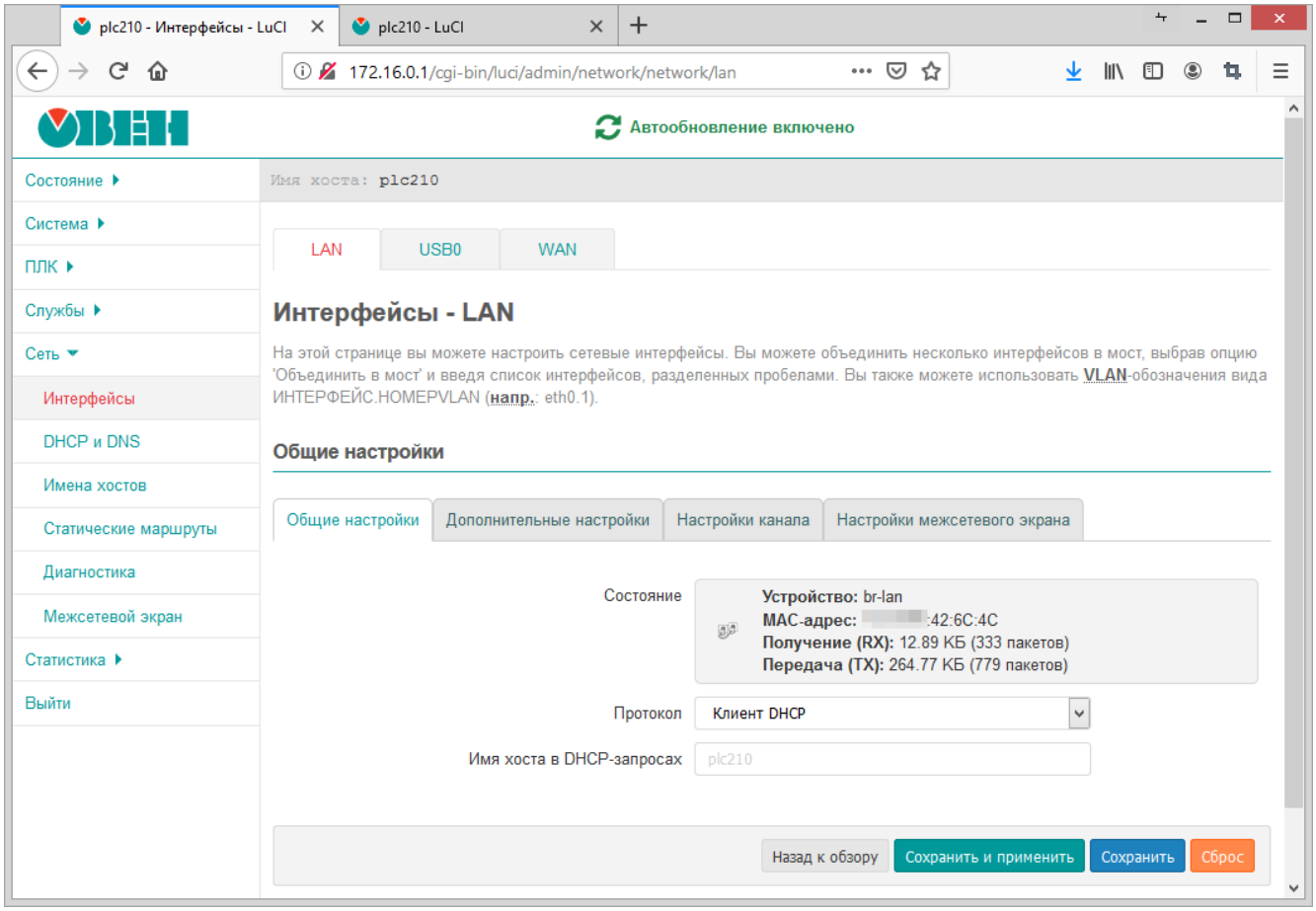


Рис. 7-3: Страница редактирования сетевого интерфейса

Страница редактирования сетевого интерфейса разделена на вкладки:

- «Общие настройки» и «Дополнительные настройки» (см. раздел 7.1.1.1);
- «Настройки канала» (см. раздел 7.1.1.2);
- «Настройки межсетевого экрана» (см. раздел 7.1.1.3).

7.1.1.1 Общие и дополнительные настройки

На вкладках «Общие настройки» (см. рисунок 7-4) и «Дополнительные настройки» (см. рисунок 7-7) представлены настройки интерфейса, набор которых во многом зависит от выбранного протокола.

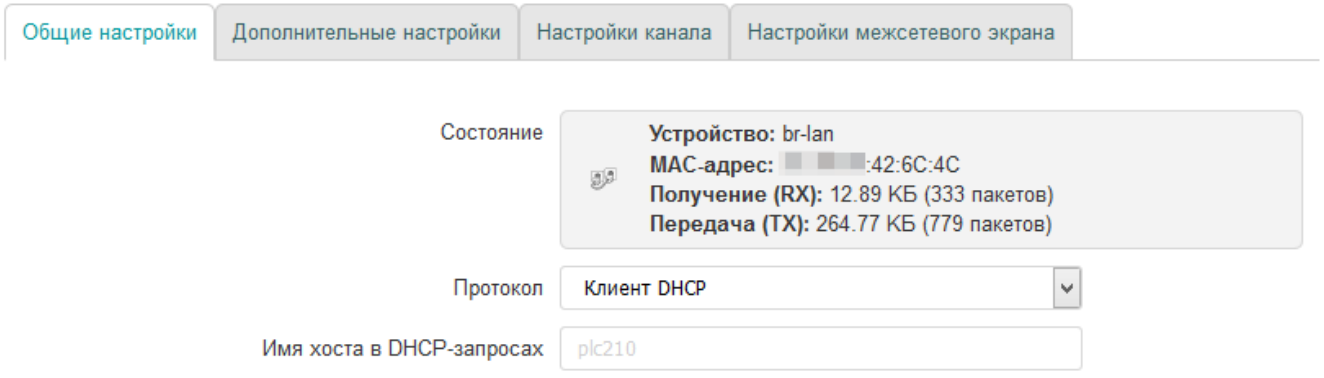


Рис. 7-4: Общие настройки сетевого интерфейса

Выбор протокола производится при помощи выпадающего списка «Протокол» на вкладке «Общие настройки» (см. рисунок 7-4). Выпадающий список выбора протокола показан на рисунке 7-5.

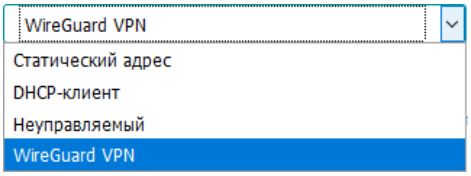


Рис. 7-5: Выпадающий список выбора протокола интерфейса

После выбора нового протокола, на странице основных настроек будет отображена кнопка «Изменить протокол», как показано на рисунке 7-6.

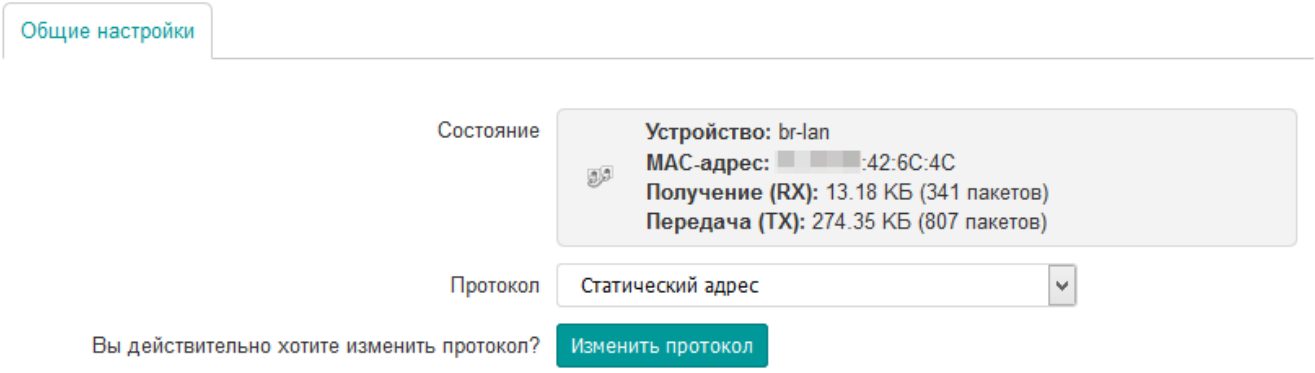


Рис. 7-6: Кнопка смены протокола сетевого интерфейса

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.

Подробное описание некоторых из доступных протоколов сетевых интерфейсов и их настройки приведены в разделе 7.1.2 данного руководства.

Среди общих для всех протоколов, можно выделить следующие настройки, расположенные на вкладке «Дополнительные настройки»:

- «Запустить при загрузке» — включает или отключает автоматический запуск интерфейса при загрузке системы;
- «Использовать встроенный IPv6-менеджмент» — включает или отключает использование встроенного IPv6 менеджмента для данного интерфейса;
- «Активировать соединение» — устанавливать параметры интерфейсу независимо от состояния подключения. Если опция включена, изменение состояния подключения не будет вызывать hotplug обработчики.

На рисунке 7-7, для примера, приведён внешний вид вкладки «Дополнительные настройки» для протокола «DHCP-клиент».

7.1.1.2 Настройки канала

Вкладка «Настройки канала» (см. рисунок 7-8) доступна только для Ethernet интерфейсов с протоколами «Статический адрес», «DHCP-клиент» и «Неуправляемый».

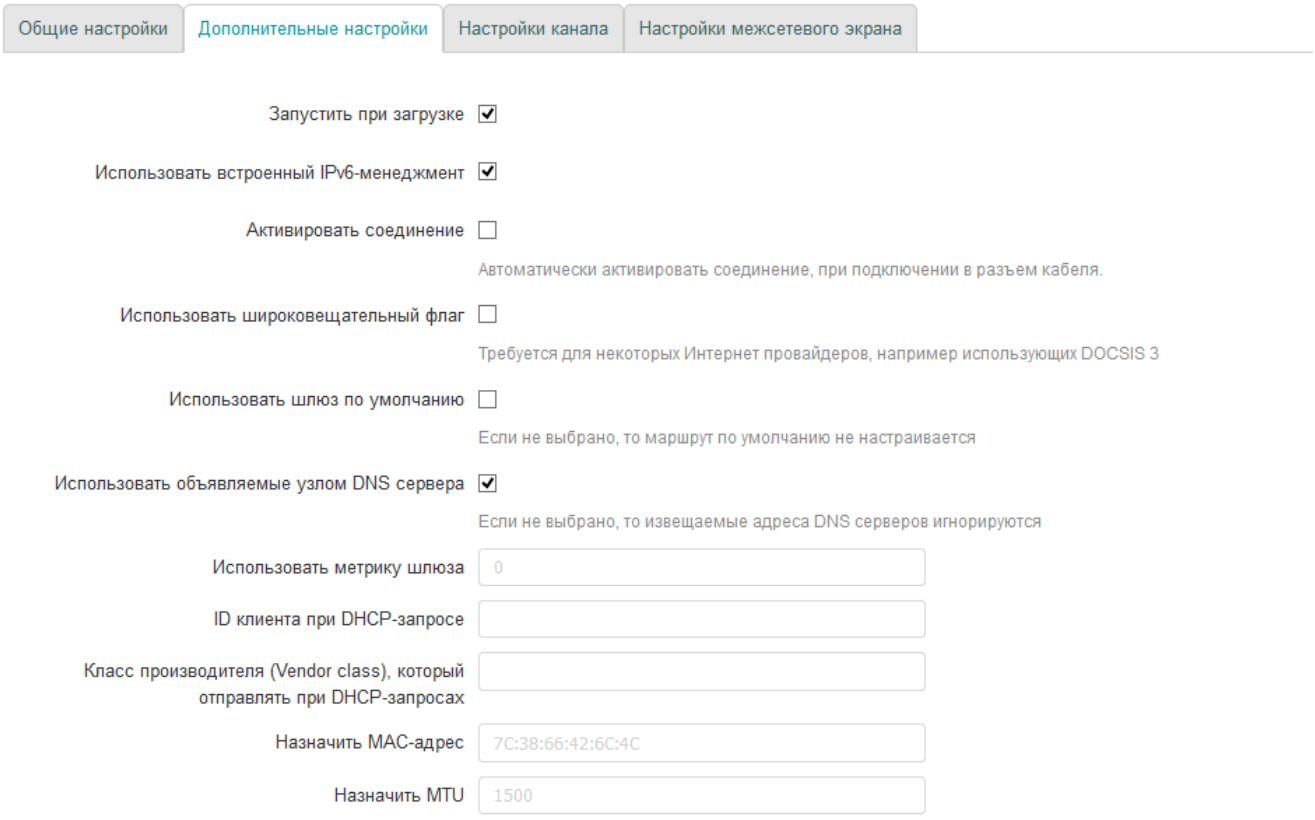


Рис. 7-7: Дополнительные настройки сетевого интерфейса для протокола «DHCP-клиент»

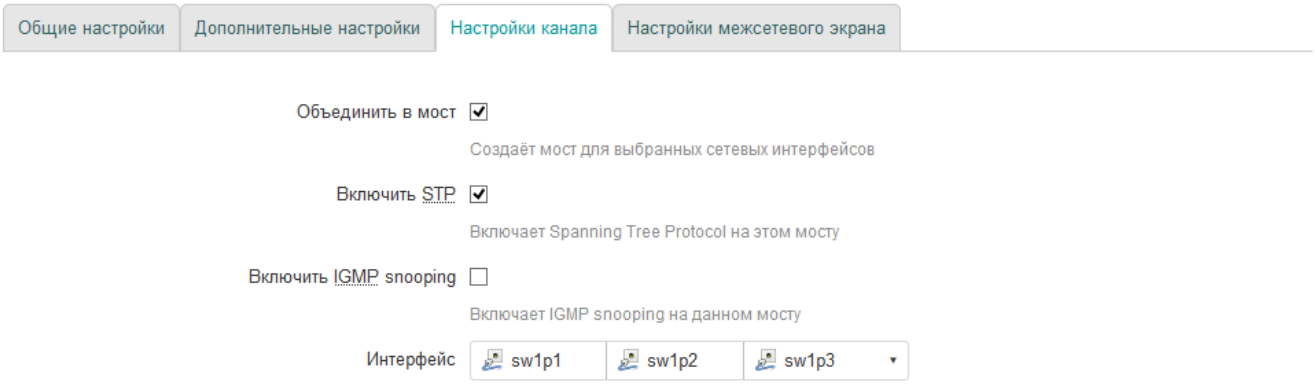
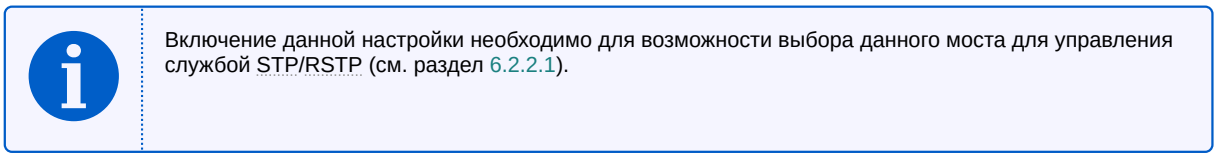
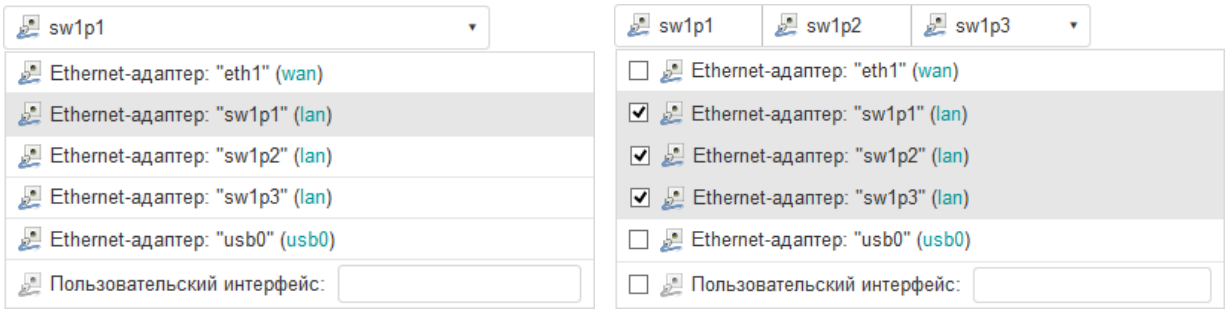


Рис. 7-8: Настройки канала сетевого интерфейса

На данной вкладке представлены следующие настройки сетевого интерфейса:

- «Объединить в мост» — настройка позволяет выполнить объединение нескольких системных сетевых интерфейсов в сетевой мост [11]. В этом случае становятся доступны дополнительные настройки:
  - «Включить STP» — включает или отключает протокол STP [12] на сетевом мосту.

    
    Включение данной настройки необходимо для возможности выбора данного моста для управления службой STP/RSTP (см. раздел 6.2.2.1).
  - «Включить IGMP snooping» — включает или отключает функцию IGMP snooping [13] на сетевом мосту.
- «Интерфейс» — в данном выпадающем списке производится выбор системного сетевого интерфейса, привязанного к редактируемому интерфейсу (см. рисунок 7-9(а)).



(а) Обычный сетевой интерфейс (б) Сетевой интерфейс-мост

Рис. 7-9: Выбор привязанных системных сетевых интерфейсов

В том случае, если выбрана опция «Объединить в мост», в данном списке производится выбор нескольких системных сетевых интерфейсов, которые необходимо объединить в сетевой мост (см. рисунок 7-9(б)).

7.1.1.3 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 7-10.

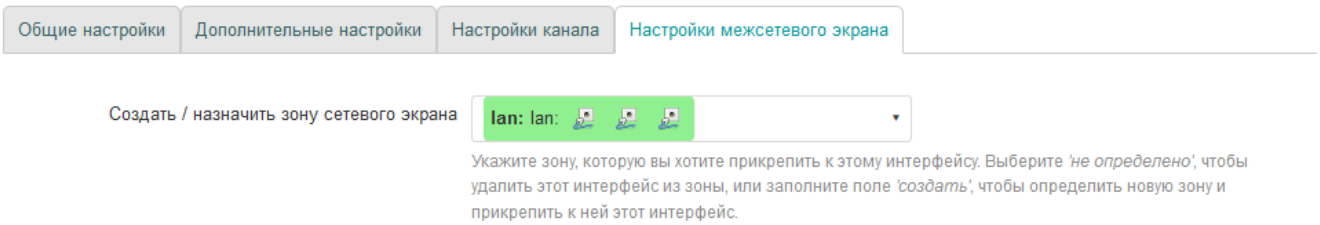


Рис. 7-10: Настройки межсетевого экрана сетевого интерфейса

На вкладке размещён только один элемент управления — выпадающий список «Создать / назначить зону сетевого экрана» (см. рисунок 7-11).

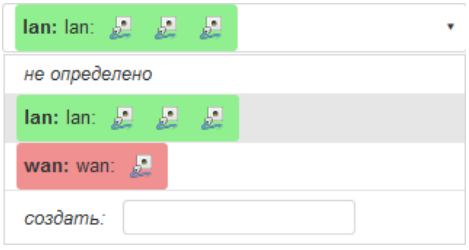


Рис. 7-11: Выпадающий список выбора зоны межсетевого экрана

При помощи данного выпадающего списка можно выбрать существующую зону межсетевого экрана или создать новую, введя её имя в поле «создать». При выборе «не определено», редактируемый сетевой интерфейс будет удалён из зоны, к которой он был прикреплён ранее.

7.1.2 Протоколы сетевых интерфейсов

В данном разделе приведено описание некоторых из доступных протоколов сетевых интерфейсов и описание их параметров.

7.1.2.1 Протокол «DHCP-клиент»

Данный протокол предназначен для интерфейсов, конфигурация которых производится при помощи DHCP-запросов.

Для данного протокола во вкладке «Общие настройки» (см. раздел 7.1.1.1) доступны следующие настройки:

- «Имя хоста в DHCP-запросах» — выбор имени хоста, которое будет использовано в DHCP-запросах.

Во вкладке «Дополнительные настройки» (см. раздел 7.1.1.1) доступны следующие настройки:

- «Использовать широковещательный флаг» — настройка включения широковещательного флага (broadcast flag) в DHCP-запросах. Данная функция может потребоваться для некоторых провайдеров.
- «Использовать шлюз по умолчанию» — настройка использования данного интерфейса в качестве маршрута по умолчанию.

  Если данная настройка включена, то данный интерфейс будет использоваться в качестве маршрута по умолчанию. В противном случае, маршрут по умолчанию настраиваться не будет.
- «Использовать объявляемые узлом DNS сервера» — настройка использования DNS-серверов, полученных от DHCP-сервера.

  Если настройка включена, то полученные от DHCP-сервера адреса DNS-серверов будут использованы в качестве основных. В противном случае, полученные от DHCP-сервера адреса DNS-серверов игнорируются.
- «Использовать метрику шлюза» — указание метрики шлюза для данного интерфейса.
- «ID клиента при DHCP-запросе» — настройка идентификатора клиента, используемого в DHCP-запросах.
- «Класс производителя (Vendor class), который отправлять при DHCP-запросах» — настройка класса производителя, используемого в DHCP-запросах.
- «Назначить MAC-адрес» — настройка MAC-адреса сетевого интерфейса. Если не указано, то будет использован оригинальный MAC-адрес.
- «Назначить MTU» — настройка MTU сетевого интерфейса.

7.1.2.2 Протокол «Статический адрес»

Данный протокол предназначен для Ethernet интерфейсов, для которых настройка IP-адресов и прочих параметров производится вручную, без использования автоматического получения адреса при помощи DHCP.

Для данного протокола во вкладке «Общие настройки» (см. раздел 7.1.1.1) доступны следующие настройки:

- «IPv4-адрес» — IP-адрес сетевого интерфейса для IP протокола версии 4.
- «Маска сети IPv4» — маска подсети для IP протокола версии 4.
- «IPv4-адрес шлюза» — IP-адрес шлюза для IP протокола версии 4.
- «Широковещательный IPv4-адрес» — широковещательный адрес сети для IP протокола версии 4.
- «Использовать собственные DNS сервера» — настройка позволяет указать собственные адреса DNS-серверов для данного сетевого интерфейса.
- «IPv6 назначение длины» — устанавливает длину IPv6 префикса, делегируемую интерфейсу.

  Если выбрано значение «выключено», то доступны следующие настройки:
  - «IPv6-адрес» — IP-адрес сетевого интерфейса для IP протокола версии 6.
  - «IPv6-адрес шлюза» — маска подсети для IP протокола версии 6.
  - «IPv6 направление префикса» — префикс маршрутизации для IP протокола версии 6.

  Если значение параметра задано, то доступны настройки:
  - «IPv6 подсказка присвоения» — шестнадцатеричный идентификатор подпрефикса, который используется для назначения частей префикса IPv6.

- «IPv6 суффикс» — суффикс IPv6 адреса. Допустимые значения:
  - `eui64` — IPv6-адрес генерируется с использованием EUI-64;
  - `random` — IPv6-адрес генерируется случайным образом;
  - любое фиксированное значение, например `::1` или `::1:2`.

Во вкладке «Дополнительные настройки» (см. раздел 7.1.1.1) доступны следующие настройки:

- «Использовать метрику шлюза» — указание метрики шлюза для данного интерфейса.
- «Назначить MAC-адрес» — настройка MAC-адреса сетевого интерфейса. Если не указано, то будет использован оригинальный MAC-адрес.
- «Назначить MTU» — настройка MTU сетевого интерфейса.

7.1.2.2.1 Настройки DHCP-сервера

При выборе протокола «Статический адрес» для сетевого интерфейса появляется возможность запуска DHCP-сервера на данном интерфейсе (по умолчанию выключен).

Настройки DHCP-сервера представлены в подразделе «DHCP-сервер» страницы редактирования настроек сетевого интерфейса (см. рисунок 7-12)

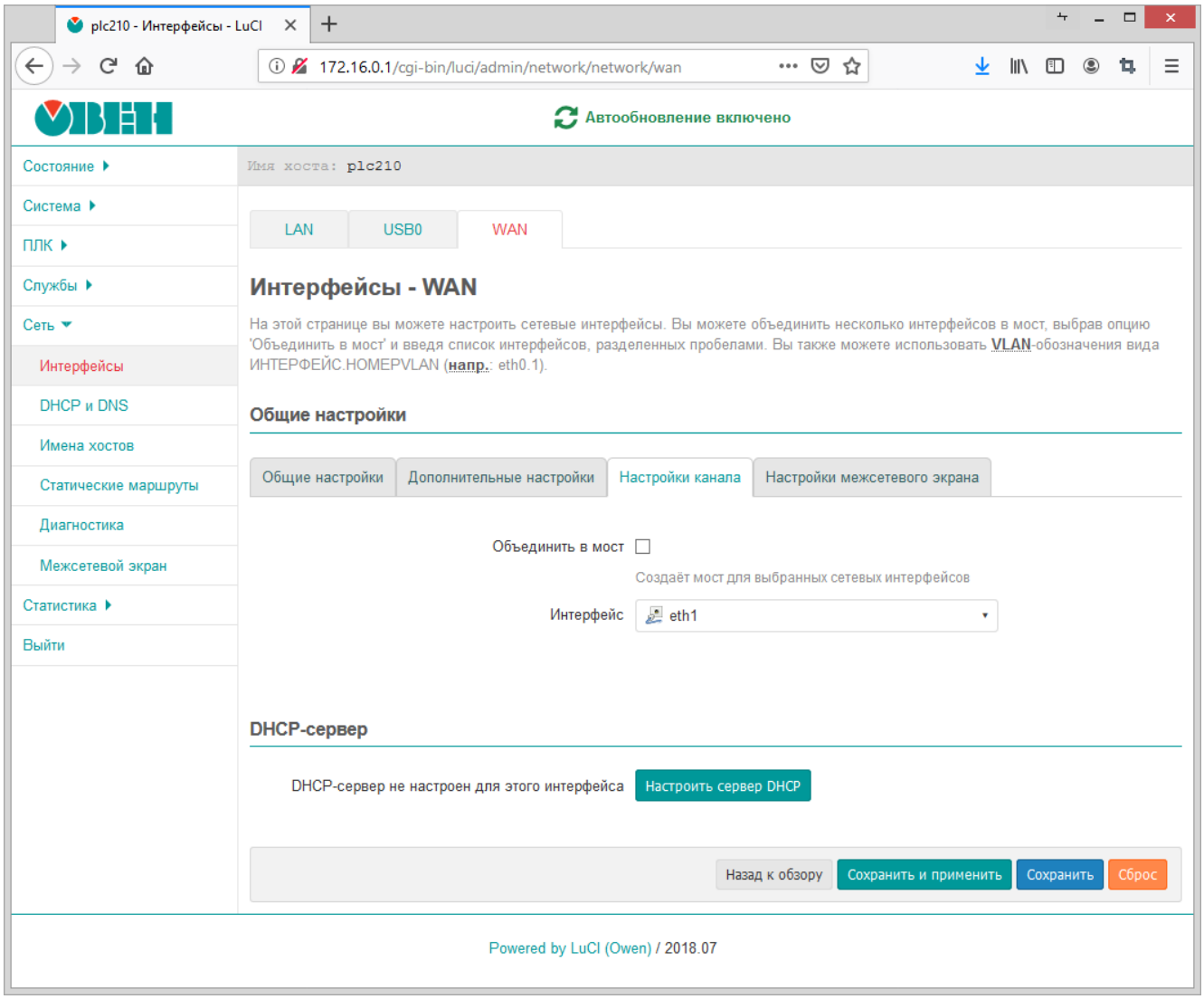


Рис. 7-12: Подраздел настроек DHCP на странице редактирования интерфейса

Для включения DHCP-сервера на интерфейсе, необходимо нажать кнопку «Настроить сервер DHCP».

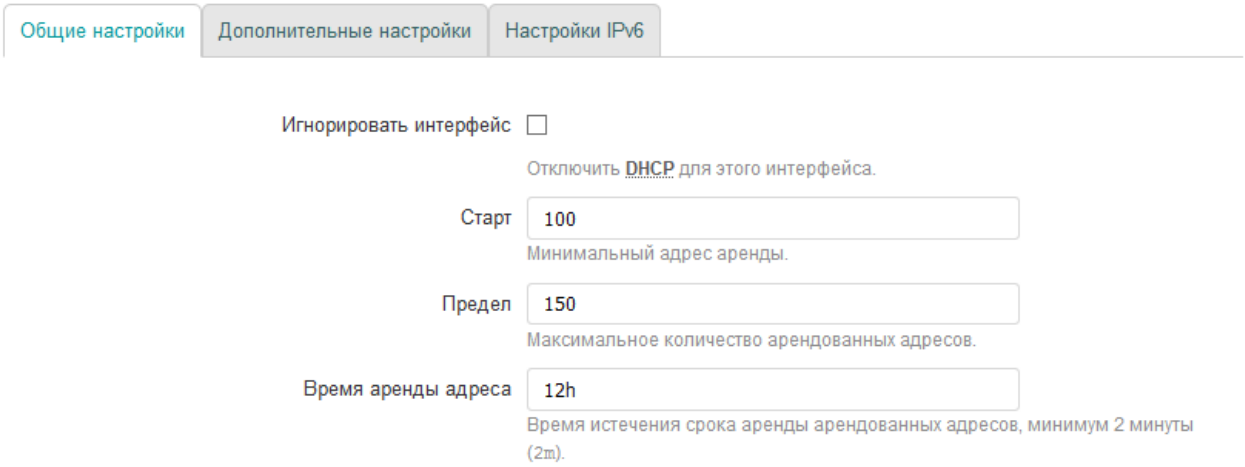


Рис. 7-13: Основные настройки DHCP-сервера сетевого интерфейса

Основные настройки DHCP-сервера представлены во вкладке «Основные настройки» подраздела «DHCP-сервер» (см. рисунок 7-13):

- «Игнорировать интерфейс» — включение данной настройки отключает работу DHCP-сервера на данном интерфейсе.
- «Старт» — начальный адрес аренды.
- «Предел» — максимальное количество адресов, выдаваемых в аренду DHCP-сервером.
- «Время аренды адреса» — время истечения срока аренды арендованных адресов. Минимальное значение — 2 минуты (2m).

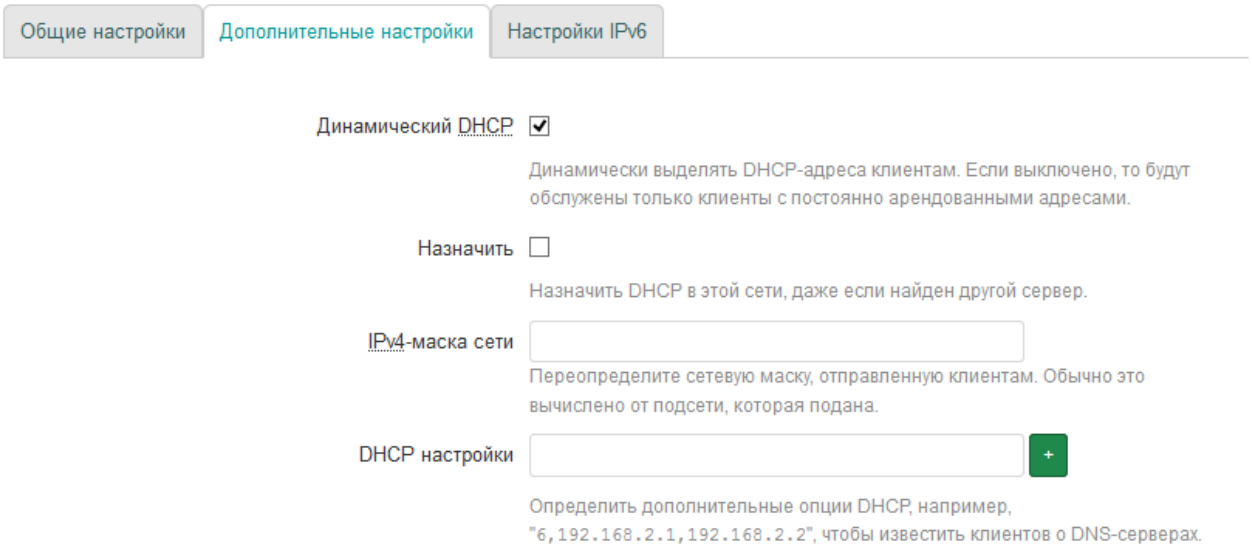


Рис. 7-14: Дополнительные настройки DHCP-сервера сетевого интерфейса

Если DHCP-сервер на интерфейсе включён, то во вкладке «Дополнительные настройки» подраздела «DHCP-сервер» (см. рисунок 7-14) представлены следующие дополнительные настройки DHCP-сервера:

- «Динамический DHCP» — настройка включает или отключает режим динамического выделения адресов клиентам. Если настройка выключена, то будут обслужены только клиенты с постоянно арендованными адресами.

Настройка постоянных аренд DHCP-сервера описана в разделе 7.2.4 данного руководства.

- «Назначить» — назначать DHCP-сервер для данного интерфейса, даже если обнаружен другой DHCP-сервер в этой же сети.
- «IPv4-маска сети» — переопределение маски подсети, которая отдаётся клиентам.
- «DHCP настройки» — настройка позволяет определить произвольные DHCP опции [14], отдаваемые клиентам.

  Параметр задаётся в формате:

  ```
  <номер_опции>,<значение_1>,<значение_2>,...
  ```

  Например, опция

  ```
  6,192.168.2.1,192.168.2.2
  ```

  извещает DHCP-клиентов об адресах DNS-сервера 192.168.2.1 и 192.168.2.2.

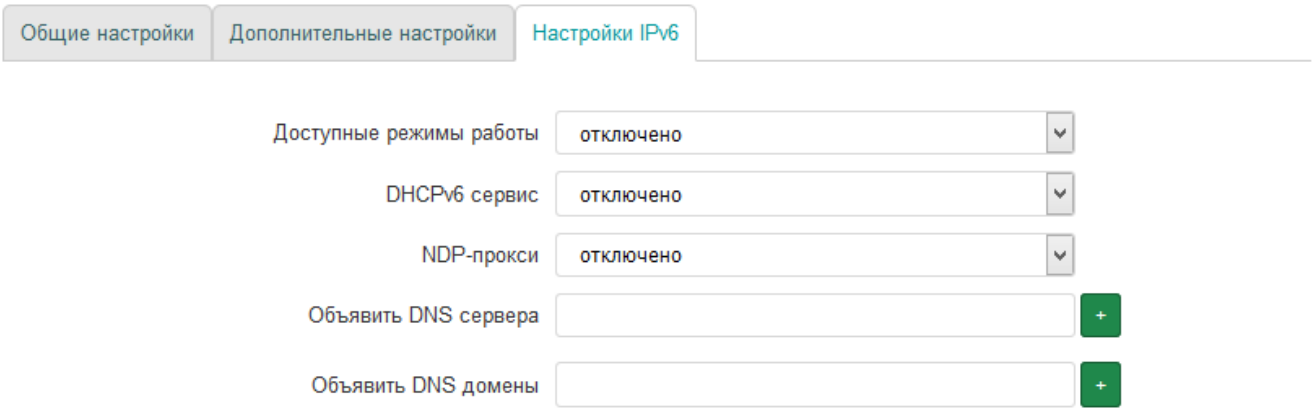


Рис. 7-15: IPv6 настройки DHCP-сервера сетевого интерфейса

Во вкладке «Настройки IPv6» раздела «DHCP-сервер» дополнительно размещены настройки DHCP-сервера, относящиеся к IP протоколу версии 6 (см. рисунок 7-15):

- «Доступные режимы работы» — режим работы службы RA для автоматической конфигурации и маршрутизации. Доступные варианты:
  - «отключено» — служба RA выключена;
  - «режим сервера» — служба RA работает в режиме сервера (только принимает сообщения);
  - «режим передачи» — служба RA работает в режиме передачи (только передаёт сообщения);
  - «гибридный режим» — служба RA передаёт и отправляет сообщения.

  Для режима работы «режим сервера» и «гибридный режим» доступна также следующая настройка:
  - «Объявлять всегда, как маршрутизатор по умолчанию» — при включении этой опции данное устройство будет всегда объявляться в качестве маршрутизатора по умолчанию.
- «DHCPv6 сервис» — выбор режима работы DHCP-сервера для протокола IPv6. Доступные варианты:
  - «отключено» — DHCP-сервер выключен;
  - «режим сервера» — DHCP-сервер включён и работает только как сервер;
  - «режим передачи» — DHCP-сервер включён и работает в режиме ретрансляции (relay) запросов;
  - «гибридный режим» — гибридный режим работы DHCP-сервер.

  Для значений «режим сервера» и «гибридный режим» доступны также следующие настройки:
  - «DHCPv6 режим» — режим автоконфигурации. Доступны варианты:
    - «stateless» — позволяет хостам автоматически получать IPv6 адреса в сети без DHCP сервера через использование NDP;
    - «stateful» — автоконфигурация возможна только с использованием DHCP сервера;
    - «stateless + stateful» (значение по умолчанию) — могут использоваться одновременно оба вида автоконфигурации.
- «NDP-прокси» — режим работы NDP-прокси. Доступны варианты:

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

- «Объявить DNS сервера» — список объявляемых DNS-серверов.
- «Объявить DNS домены» — список объявляемых DNS-доменов.

7.1.2.3 Протокол «WireGuard VPN»

Данный протокол предназначен для создание защищенного производительного WireGuard интерфейса, позволяющего организовать доступ через VPN-тунель к серверу с минимальными значениями задержки. Более подробная информация о настройке WireGuard VPN приведена на официальном сайте проекта[1].

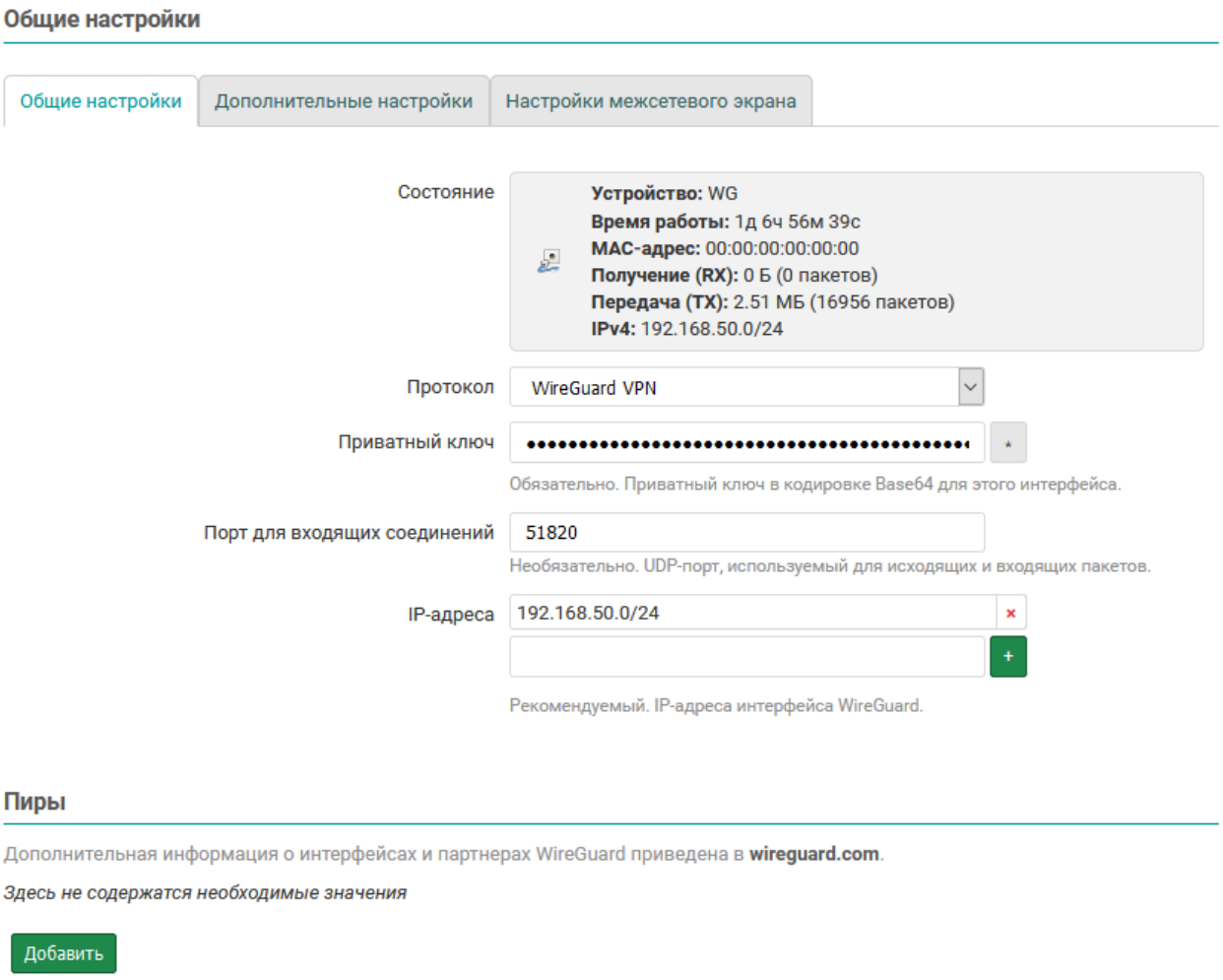


Рис. 7-16: Общие настройки интерфейса «WireGuard VPN»

Для протокола «WireGuard VPN» во вкладке «Общие настройки» (см. рисунок 7-16) доступны следующие настройки:

- «Приватный ключ» — строка, куда вставляется сгенерированный в кодировке Base64 закрытый (приватный) ключ для интерфейса WireGuard.
- «Порт для входящих соединений» — UDP-порт для входящих пакетов. По умолчанию, 51820.
- «IP-адреса» — разрешенные IP-адреса интерфейса WireGuard.
- «Пиры» — настройки удаленных WireGuard-серверов (пиров), активируются после нажатия кнопки «Добавить».

[1] https://www.wireguard.com/xplatform/

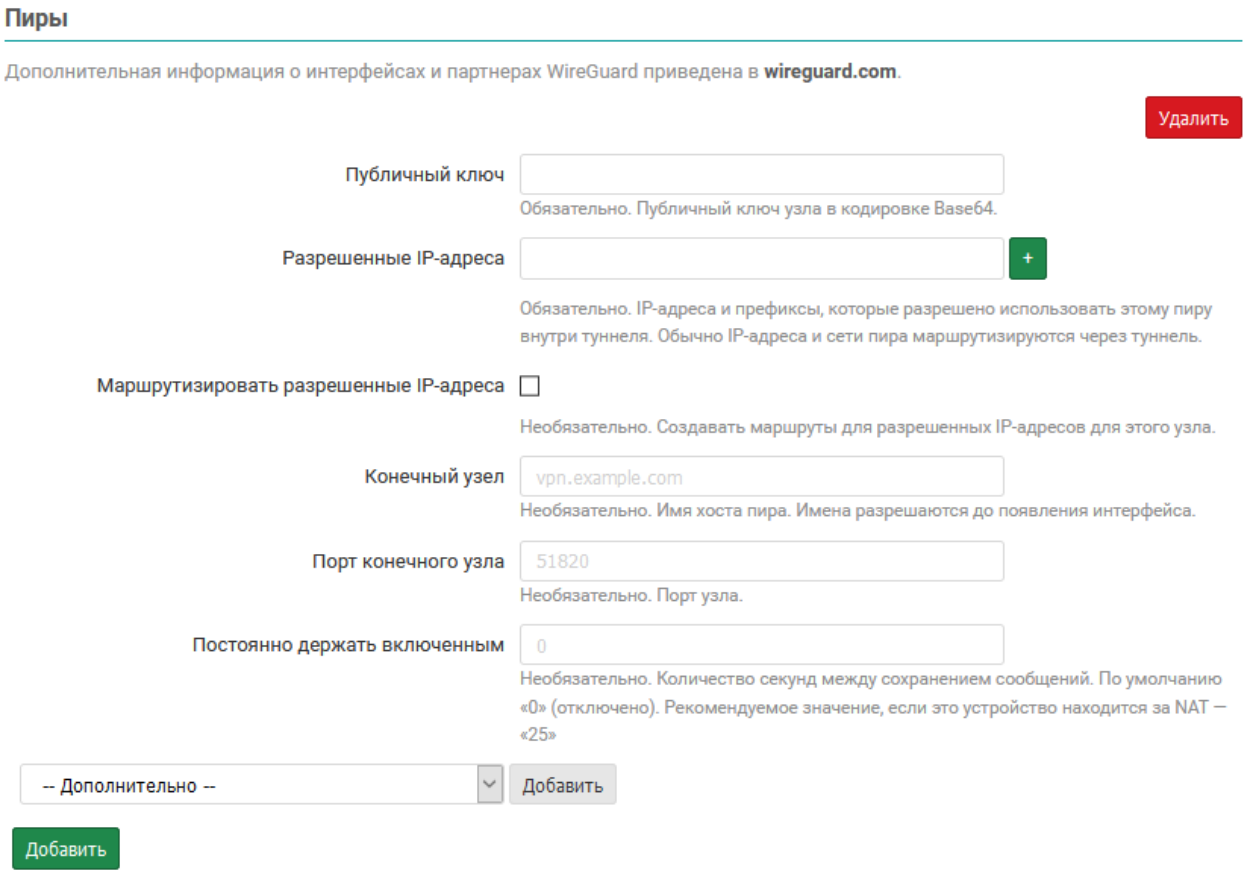


Рис. 7-17: Дополнительные настройки удаленного WireGuard-сервера (Пиры)

После нажатия кнопки «Добавить» в подразделе «Пиры» появляются следующие дополнительные настройки удаленного WireGuard-сервера (пира) (см. рисунок 7-17):

- «Публичный ключ» — строка, куда вставляется сгенерированный в кодировке Base64 публичный ключ для интерфейса WireGuard.
- «Разрешенные IP-адреса» — IP-адрес и префиксы, с которых будет допущен трафик.
- «Маршрутизировать разрешенные IP-адреса» — установка данного параметра позволяет создавать маршруты для разрешенных IP-адресов для конечного узла.
- «Конечный узел» — доменное имя или IP-адрес конечного устройства.
- «Порт конечного узла» — порт для входящих и исходящих пакетов конечного узла. По умолчанию, 51820.
- «Постоянно держать включенным» — количество секунд между сохранением сообщений. По умолчанию, «0» (отключено). Рекомендуемое значение, если это устройство находится за NAT — «25».
- «– Дополнительно –» — позволяет выполнить настройку следующих двух параметров (см. рисунок 7-18):
  - «Описание» — описание для интерфейса «WireGuard VPN».
  - «Предварительный ключ» — шифрованный общий ключ, в кодировке Base64, который добавляет дополнительный слой криптографии с симметричным ключом для постквантовой устойчивости.

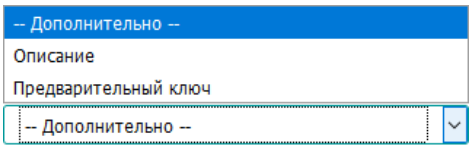


Рис. 7-18: Опциональные настройки интерфейса «WireGuard VPN»

7.1.2.4 Протокол «Неуправляемый»

Данный протокол не имеет дополнительных настроек и предназначен для интерфейсов, которые не управляются службой netifd.

7.1.3 Создание нового интерфейса

Для создания нового интерфейса предназначена кнопка «Добавить новый интерфейс» (см. рисунок 7-1), расположенная внизу таблицы интерфейсов.

При нажатии кнопки «Добавить новый интерфейс» будет открыта страница создания нового сетевого интерфейса, как показано на рисунке 7-19, на которой следует указать основные настройки создаваемого интерфейса, включая символьное имя и протокол интерфейса.

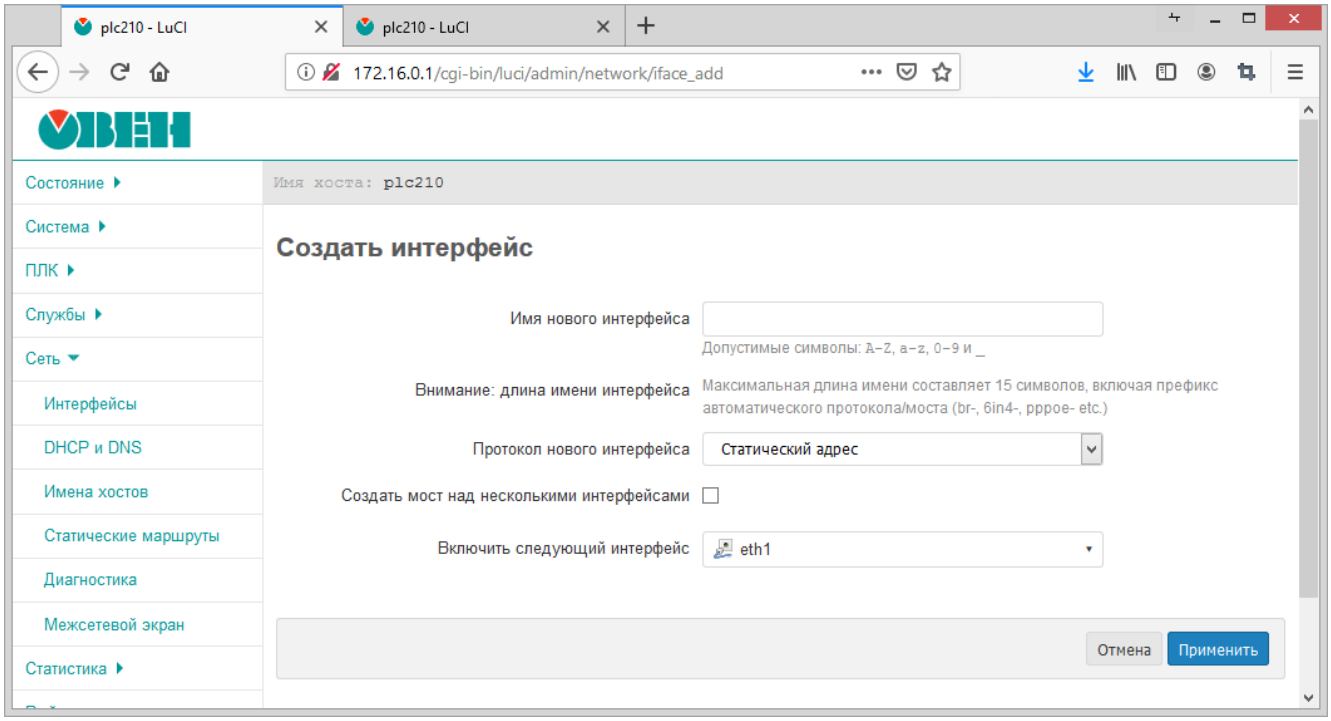


Рис. 7-19: Создание нового сетевого интерфейса

После ввода основных параметров интерфейса, для его создания следует нажать кнопку «Применить». Если основные параметры создаваемого интерфейса были введены без ошибок, произойдёт переход на страницу редактирования нового интерфейса, которая подробна описана в разделе 7.1.1 данного руководства.

7.1.4 Удаление интерфейсов

Для удаления интерфейса предназначена кнопка «Удалить» (см. рисунок 7-1), расположенная в строке соответствующего интерфейса.

При нажатии кнопки «Удалить» будет отображено окно подтверждения, показанное на рисунке 7-20.

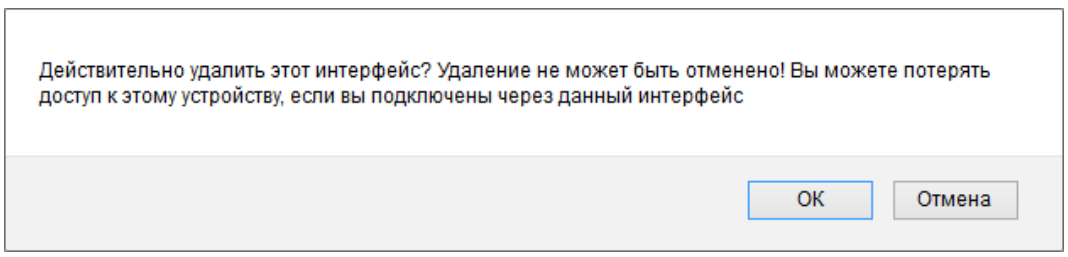


Рис. 7-20: Подтверждение удаления сетевого интерфейса

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

7.2 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 7-21.

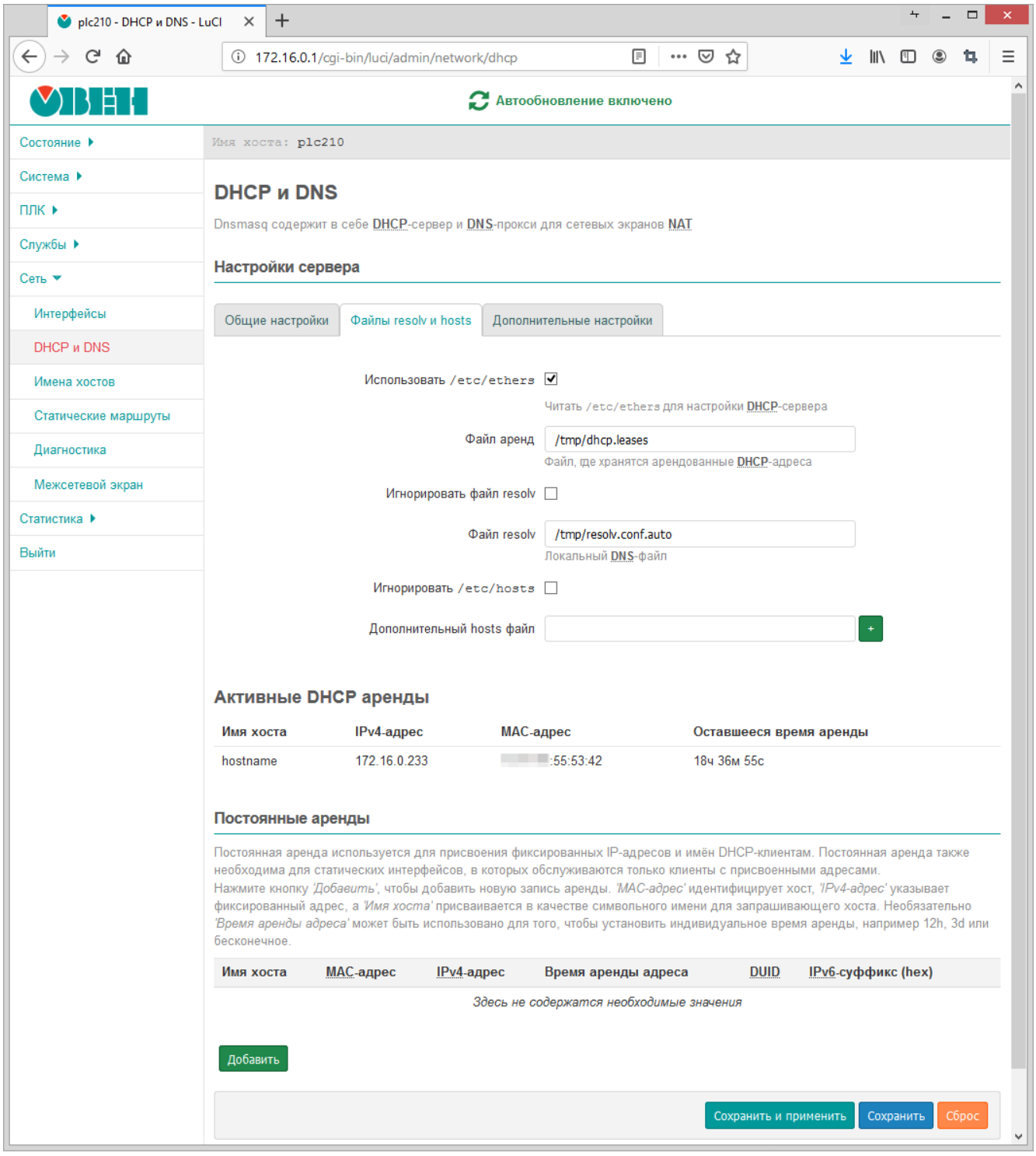


Рис. 7-21: Страница «DHCP и DNS»

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

- «Общие настройки» (см. раздел 7.2.1);
- «Дополнительные настройки» (см. раздел 7.2.2);
- «Файлы resolv и hosts» (см. раздел 7.2.3).

Дополнительно, на странице «DHCP и DNS» в подразделе «Активные DHCP аренды» приводится таблица текущих арендованных адресов для IP протоколов версий 4 и 6 (см. рисунок 7-22).

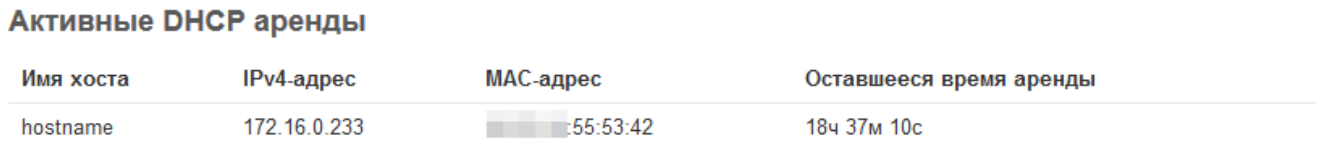


Рис. 7-22: Активные аренды DHCP-сервера

Аналогичный подраздел с таблицей арендованных адресов для IP протоколов версий 4 и 6 имеется также и на странице «Обзор» раздела «Состояние» (см. раздел 3.1.6).

В подразделе «Постоянные аренды» страницы «DHCP и DNS» (см. рисунок 7-23) производится настройка постоянных аренд DHCP-сервера, которая подробно рассмотрена в разделе 7.2.4.

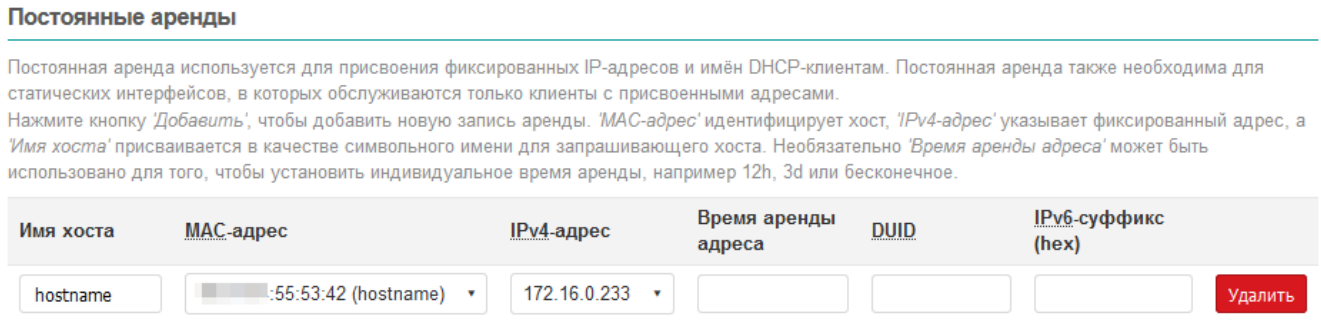


Рис. 7-23: Подраздел «Постоянные аренды» страницы «DHCP и DNS»

7.2.1 Общие настройки

Общие настройки службы dnsmasq расположены во вкладке «Общие настройки» страницы «DHCP и DNS». Внешний вид вкладки «Общие настройки» показан на рисунке 7-24.

Во вкладке доступны следующие основные настройки:

- «Требуется домен» — не перенаправлять DNS-запросы без DNS-имени.
- «Основной» — настройка, определяющая единственный ли это DHCP-сервер в локальной сети.
- «Локальный сервер» — имена, соответствующие данному домену никогда не передаются. Данные имена разрешаются только из файла DHCP («/etc/config/dhcp») или файла хостов («/etc/hosts»).
- «Локальный домен» — суффикс локального домена, который будет добавлен к DHCP-именам и записям файла хостов («/etc/hosts»).
- «Запись запросов» — записывать полученные DNS-запросы в системный журнал.
- «Перенаправление запросов DNS» — список DNS-серверов для перенаправления запросов.
- «Защита от DNS Rebinding» — включает или отключает функционал защиты от атаки DNS rebinding [15].

  Если опция включена, то доступны также дополнительные настройки:

  - «Разрешить локальный хост» — разрешить ответы внешней сети в диапазоне 127.0.0.0/8.
  - «Белый список доменов» — список доменов, для которых разрешены ответы RFC1918 [10].
- «Только локальный DNS» — ограничение службы DNS для подсетей интерфейса использующего DNS.
- «Не использовать wildcard» — включает соединение только с определёнными интерфейсами, не использующими подстановочные адреса (wildcard).

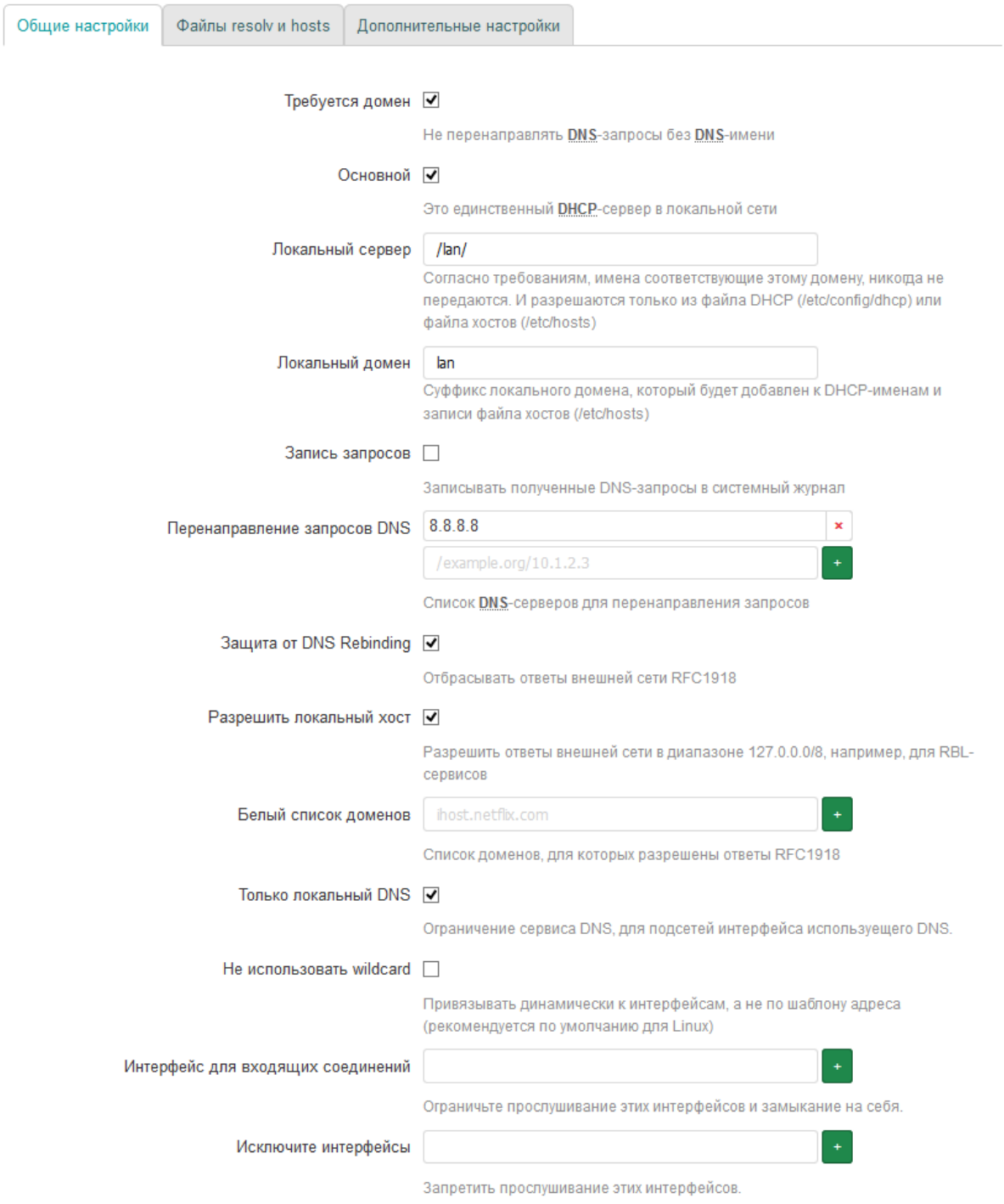


Рис. 7-24: Общие настройки службы dnsmasq

7.2.2 Дополнительные настройки

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

Внешний вид вкладки «Дополнительные настройки» показан на рисунке 7-25.

Во вкладке доступны следующие настройки:

- «Подавить логирование» — подавить логирование работы протоколов службы dnsmasq (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.
- «Фильтровать бесполезные» — не перенаправлять запросы, которые не могут быть обработаны публичными DNS-серверами.
- «Локализовывать запросы» — локализовывать имя хоста в зависимости от запрашиваемой подсети, если доступно несколько IP-адресов.
- «Расширять имена узлов» — добавить локальный суффикс домена для имён из файла хостов («/etc/hosts»).
- «Отключить кэш отрицательных ответов» — не кешировать отрицательные ответы, в том числе для несуществующих доменов.
- «Дополнительные файлы серверов» — путь к дополнительному файлу серверов. В файле должны содержаться строки в виде

  ```
  server=/domain/1.2.3.4
  ```

  или

  ```
  server=1.2.3.4
  ```

- «Строгий порядок» — если данная настройка включена, то DNS-сервера будут опрашиваться строго в порядке, определённом в «resolv» файле.
- «Все серверы» — опрашивать все имеющиеся внешние DNS-серверы.
- «Переопределение поддельного NX-домена» — список хостов, поставляющих поддельные результаты домена NX.
- «DNS порт сервера» — номер порта для входящих DNS-запросов.
- «DNS порт запроса» — номер порта для исходящих DNS-запросов.
- «Макс. кол-во аренд DHCP аренды» — максимальное количество активных арендованных DHCP-адресов.
- «Макс.EDNS0 размер пакета» — максимально допустимый размер EDNS.0 UDP пакетов.
- «Макс. кол-во одновременных запросов» — максимально допустимое количество одновременных DNS-запросов.
- «Размер кэша DNS запроса» — количество кэшированных DNS записей. Максимально возможное значение — «10000». При указании значения «0» кеширование DNS-запросов будет отключено.

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

Во вкладке «Файлы resolv и hosts» страницы «DHCP и DNS» расположены настройки, касающиеся файлов «resolv.conf» [16] и «hosts» [17]. Внешний вид вкладки «Файлы resolv и hosts» показан на рисунке 7-26.

На вкладке «Файлы resolv и hosts» доступны следующие настройки:

- «Использовать /etc/ethers» — указание использовать конфигурационный файл «/etc/ethers» [18] 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». Данная опция недоступна, если включена опция «Игнорировать файл resolv».
- «Игнорировать /etc/hosts» — указание службе dnsmasq игнорировать данные файла «/etc/hosts».

Рис. 7-25: Дополнительные настройки службы dnsmasq

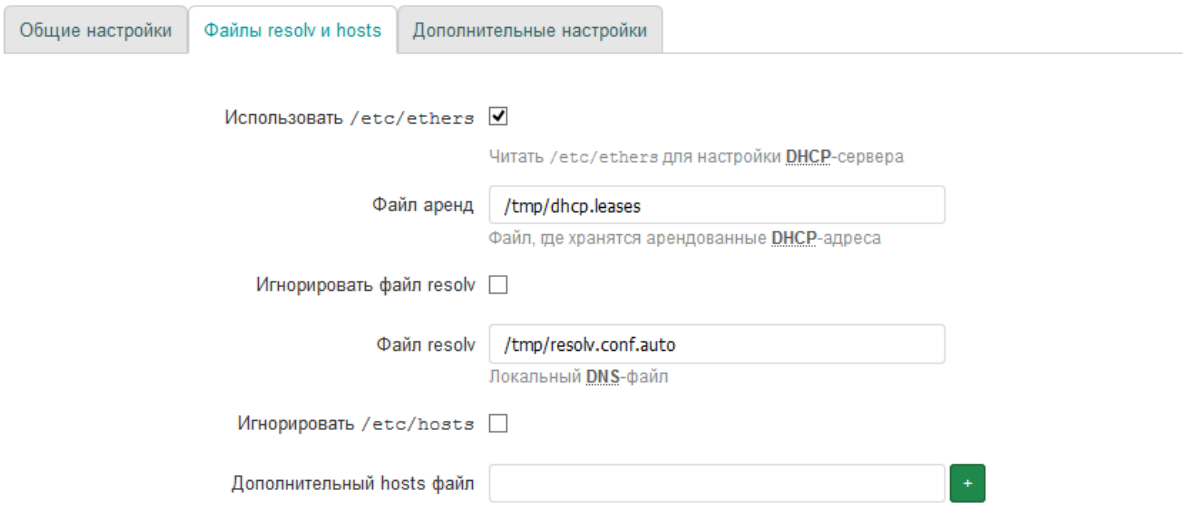


Рис. 7-26: Настройки файлов resolv.conf и hosts службы dnsmasq

- «Дополнительный hosts файл» — позволяет указать один или несколько дополнительных файлов «hosts». Указанные файлы будут использоваться вместе со стандартным файлом «/etc/hosts». Данная опция недоступна, если включена опция «Игнорировать /etc/hosts».

7.2.4 Настройка постоянных аренд DHCP-сервера

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 подраздела «Постоянные аренды» показан на рисунке 7-27.

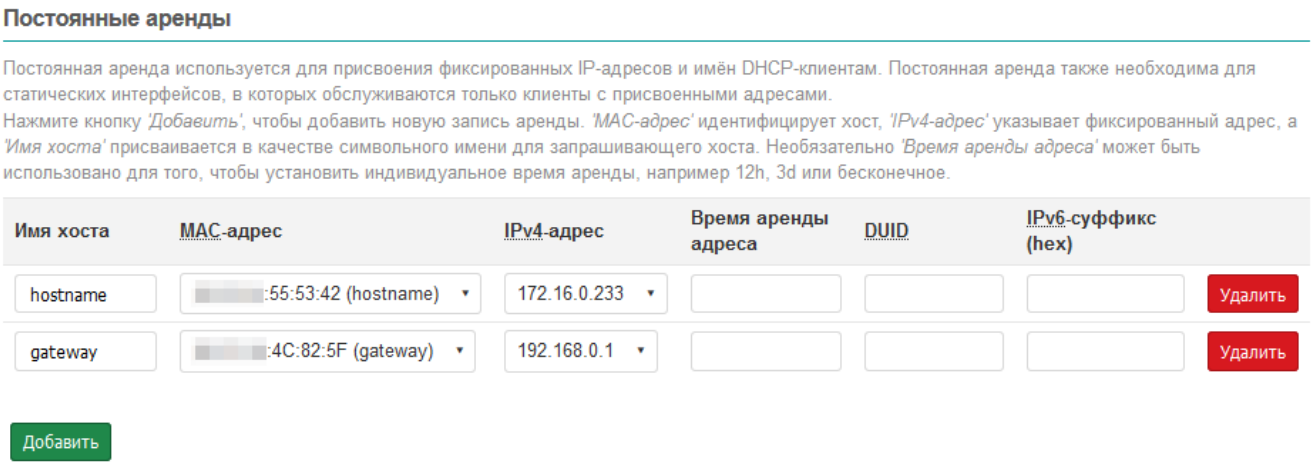


Рис. 7-27: Настройка постоянных аренд DHCP-сервера

Добавление новой постоянной аренды осуществляется нажатием кнопки «Добавить» с последующим указанием параметров постоянной аренды в добавленной строке таблицы (см. рисунок 7-28).

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

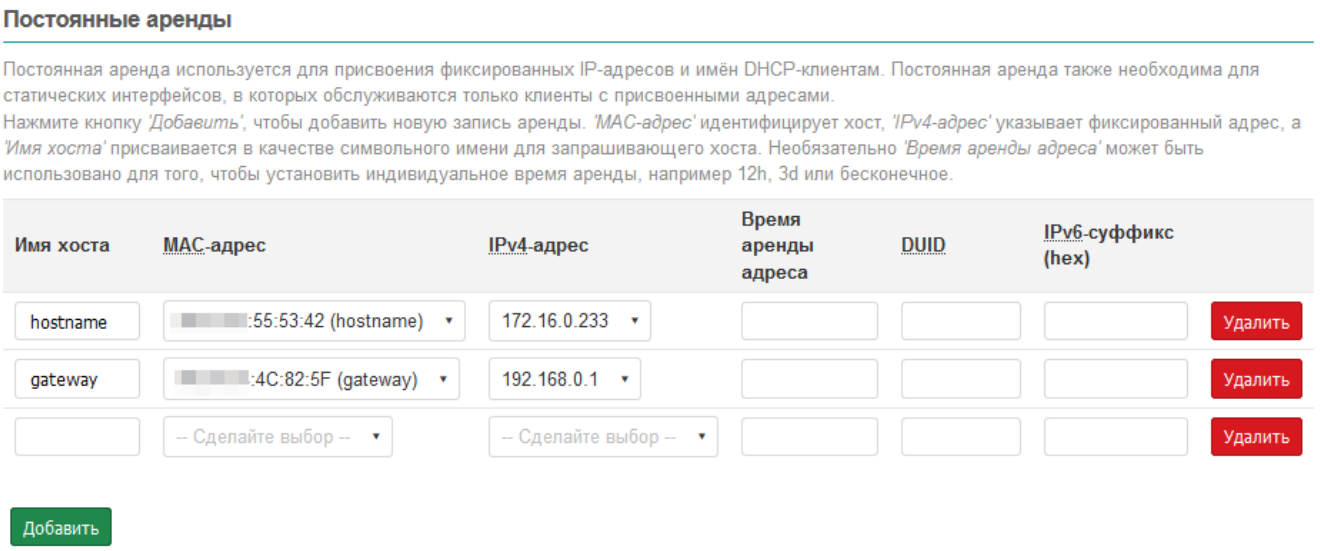


Рис. 7-28: Добавление записи постоянной аренды DHCP-сервера

7.3 Имена хостов

На странице «Имена хостов» раздела «Сеть» можно определить пользовательский список хостов и соответствующие им IP-адреса. Внешний вид страницы «Имена хостов» показан на рисунке 7-29.

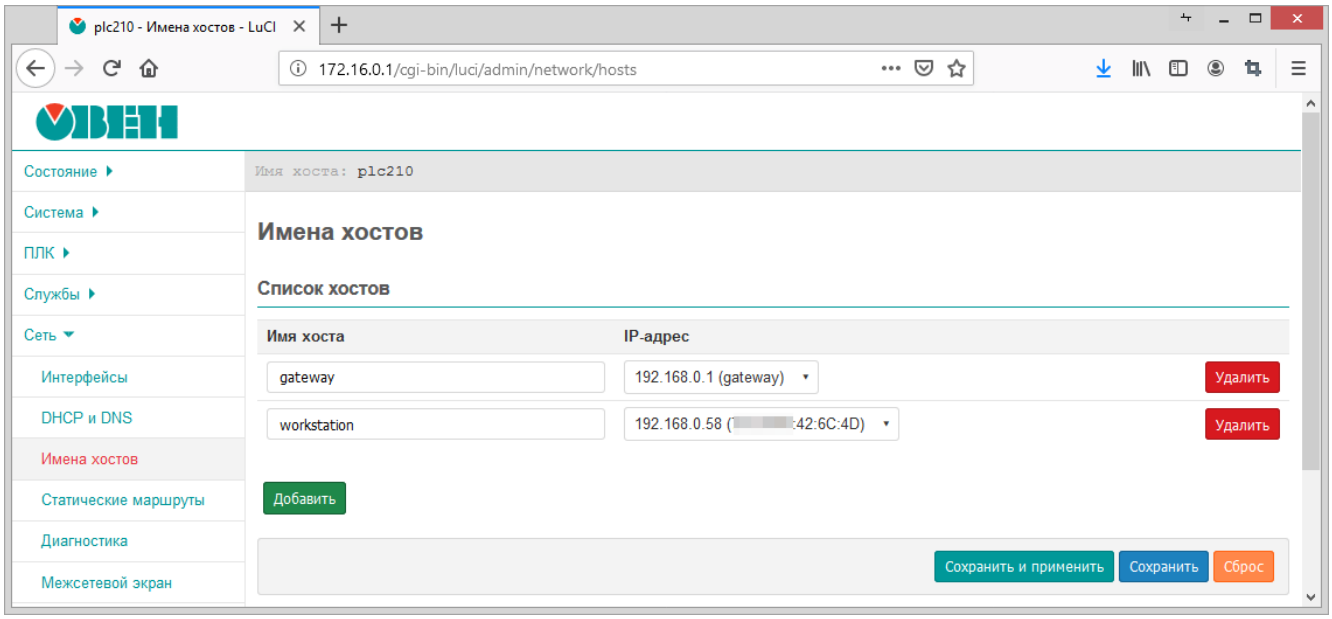


Рис. 7-29: Страница «Имена хостов»

Добавление нового имени хоста осуществляется нажатием кнопки «Добавить» с последующим указанием имени хоста и соответствующего ему IP-адреса в добавленной строке таблицы (см. рисунок 7-30).

Рис. 7-30: Страница «Имена хостов». Добавление новой записи

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

7.4 Статические маршруты

Настройки статических IPv4 и IPv6 маршрутов расположены на странице «Статические маршруты» раздела «Сеть». Данные настройки позволяют добавлять в IPv4 и IPv6 таблицы маршрутизации пользовательские маршруты (статические маршруты).

Внешний вид страницы «Статические маршруты» показан на рисунке 7-31.

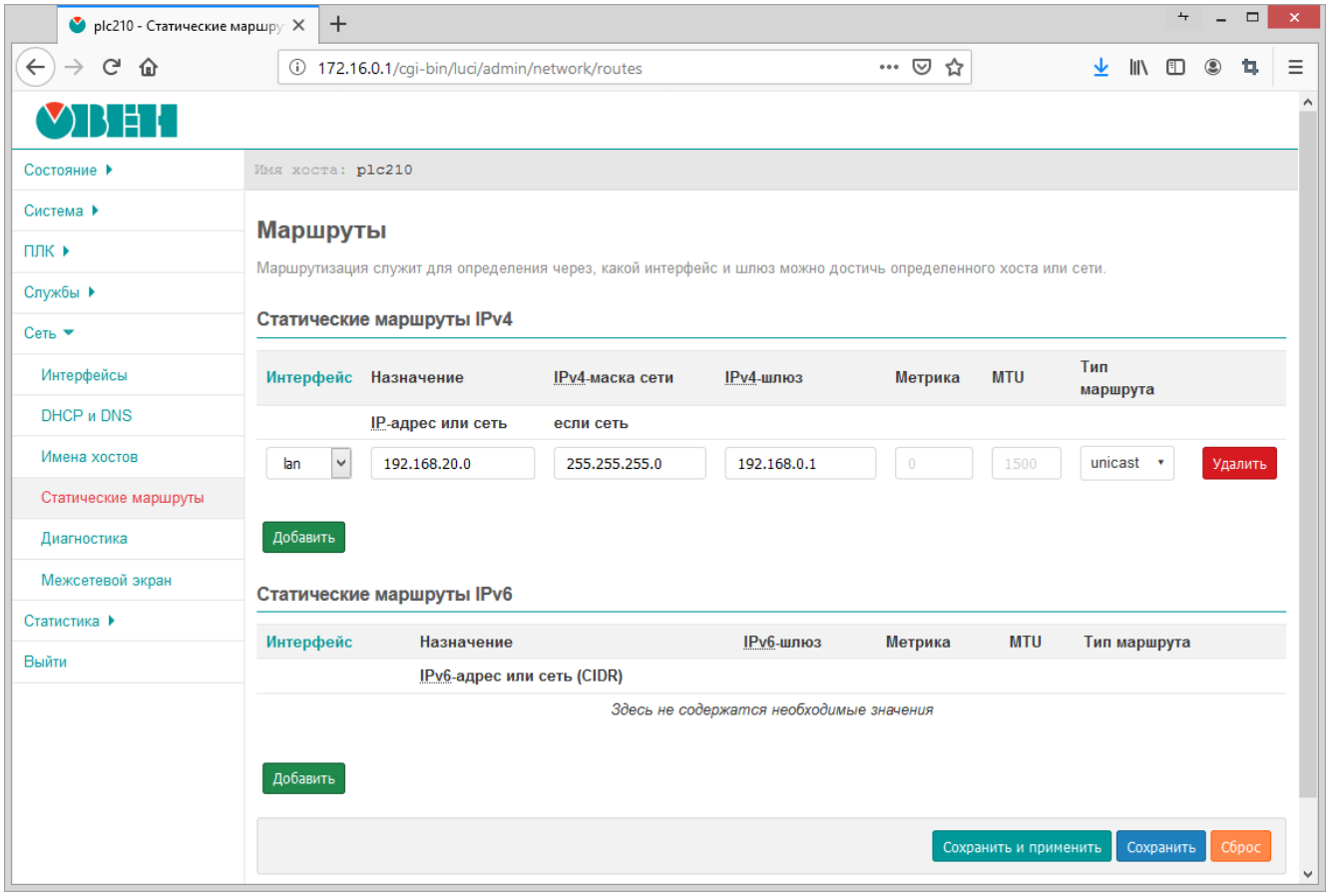


Рис. 7-31: Страница «Статические маршруты»

Добавление нового статического маршрута осуществляется нажатием кнопки «Добавить» с последующим указанием параметров маршрута в добавленной строке таблицы (см. рисунок 7-32).

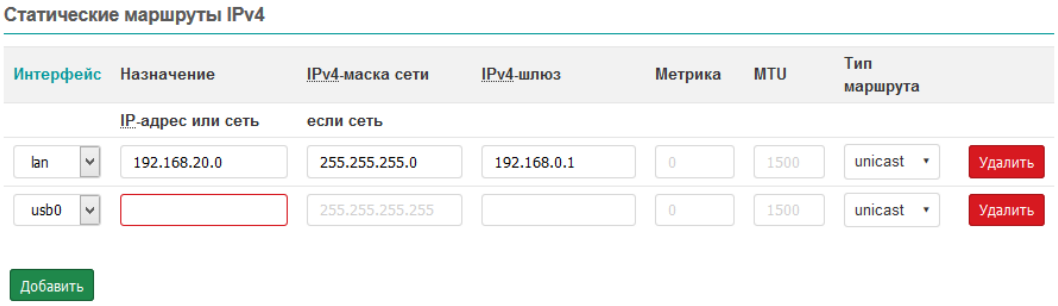


Рис. 7-32: Страница «Статические маршруты». Добавление нового маршрута

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

7.5 Межсетевой экран

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

- «Общие настройки» — основные настройки межсетевого экрана (см. раздел 7.5.1) и настройка зон (см. раздел 7.5.2).
- «Перенаправление портов» — настройка правил перенаправления портов (см. раздел 7.5.3)
- «Правила для трафика» — настройка правил межсетевого экрана для входящего, исходящего и перенаправляемого трафика (см. раздел 7.5.4).
- «Пользовательские правила» — настройка пользовательских правил межсетевого экрана (см. раздел 7.5.5).

7.5.1 Общие настройки

Внешний вид страницы «Межсетевой экран» с открытой вкладкой «Общие настройки» показан на рисунке 7-33.

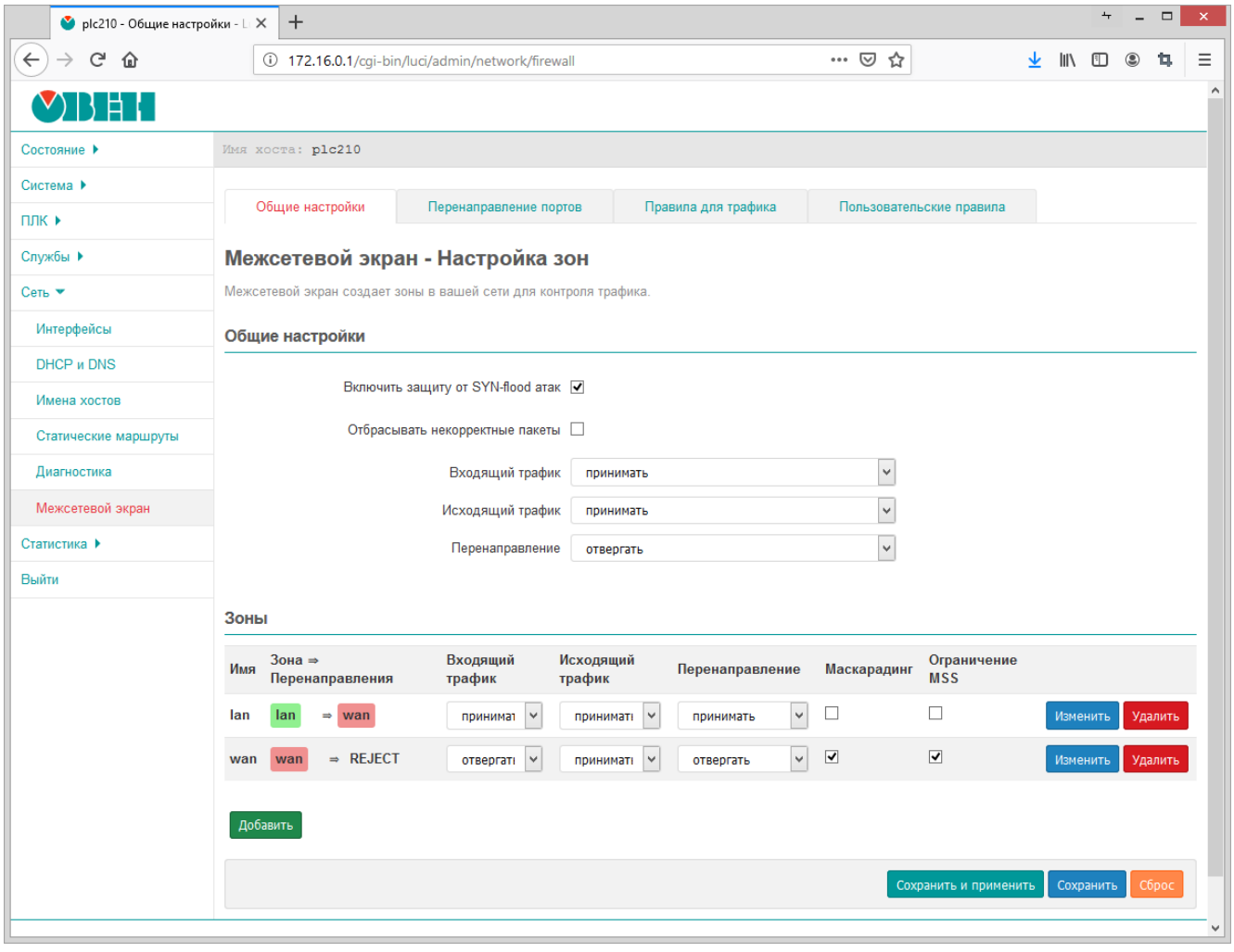


Рис. 7-33: Общие настройки межсетевого экрана

На данной вкладке содержатся следующие настройки межсетевого экрана:

- «Включить защиту от SYN-flood атак» — управление функцией защиты от SYN-flood атак [19].
- «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).

7.5.2 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 7-34).

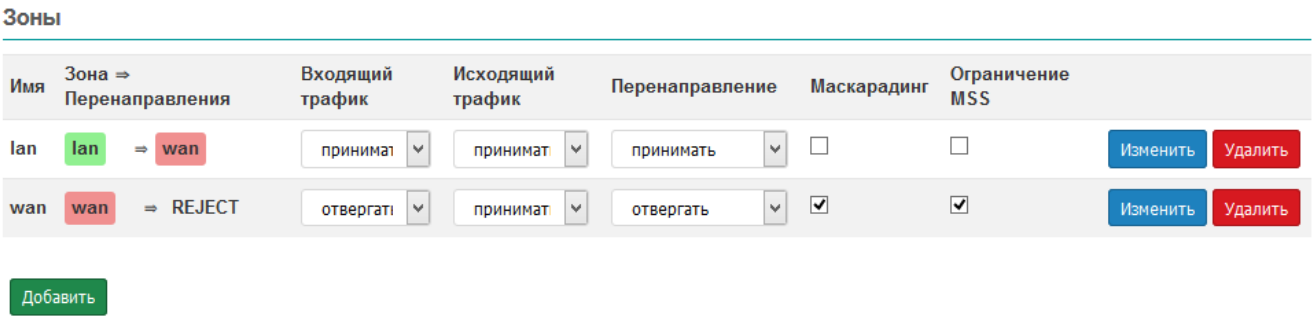


Рис. 7-34: Настройка зон межсетевого экрана. Таблица зон

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

- «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 для указанной зоны.
- «Ограничение MSS» — включает или отключает ограничение MSS при передаче для данной зоны.

Дополнительно, в таблице приведены следующие параметры зон:

- «Имя» — уникальное символьное имя зоны;
- «Зона => Перенаправления» — зона источник и зоны назначения, в которые разрешено перенаправление трафика (см. раздел 7.5.2.1).

7.5.2.1 Редактирование зон

Основные параметры зоны можно изменить в строке таблицы зон при помощи соответствующих элементов управления (см. рисунок 7-34). Для изменения дополнительных параметров зоны необходимо нажать кнопку «Изменить» в строке соответствующей зоны. При этом откроется страница редактирования параметров зоны с двумя вкладками: «Общие настройки» и «Дополнительные настройки», как показано на рисунках 7-35 и 7-36.

На вкладке «Общие настройки», в дополнение к уже перечисленным ранее основным настройкам зон (раздел 7.5.2) доступны следующие настройки:

- «Имя» — уникальное символьное имя зоны.
- «Использовать сети» — выбор сетевых интерфейсов, входящих в указанную зону.

На вкладке «Дополнительные настройки» доступны следующие настройки:

- «Использовать протокол» — выбор версии используемого IP-протокола в указанной зоне. Возможен выбор из вариантов:
  - только IPv4;
  - только IPv6;
  - IPv4 и IPv6.

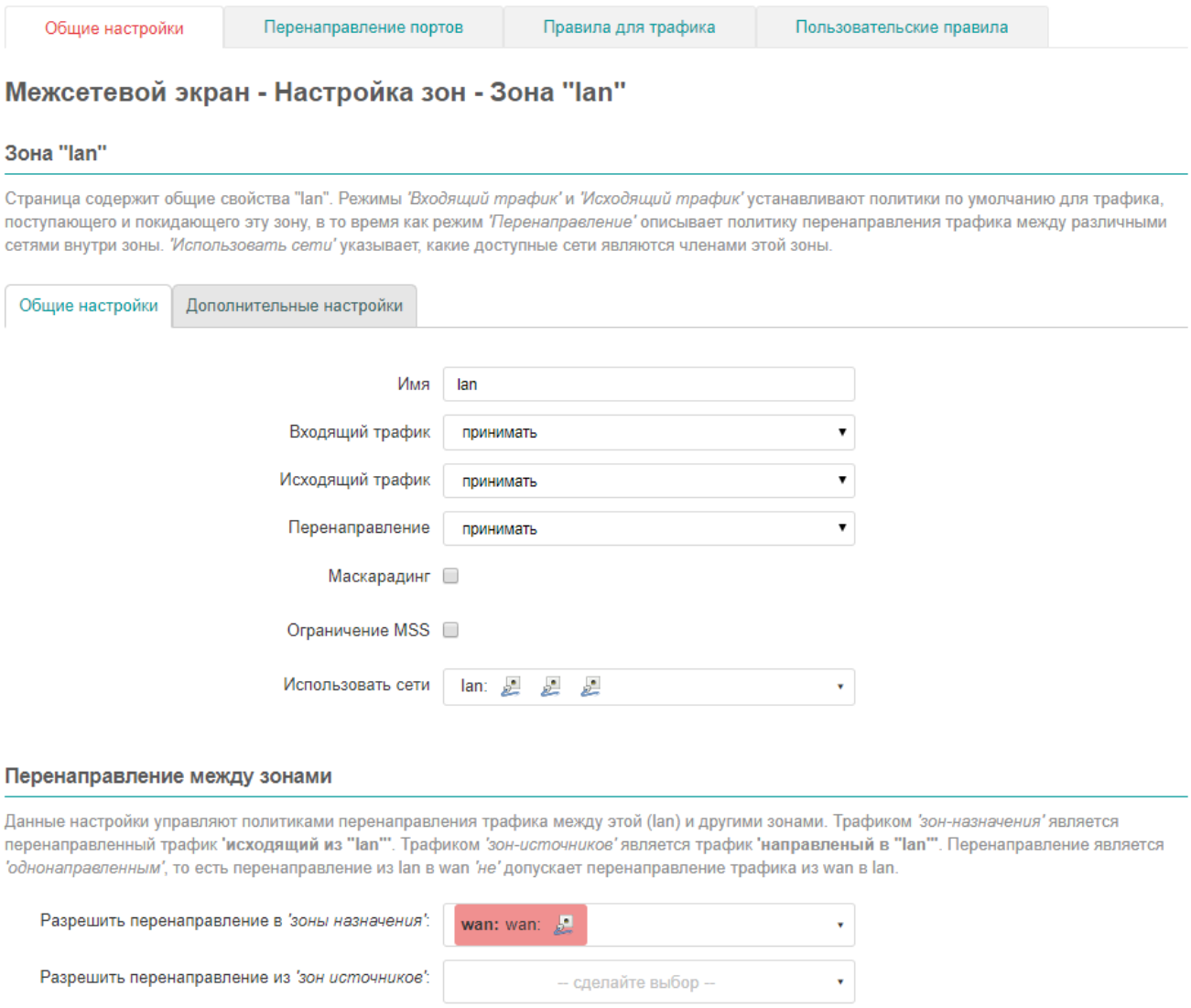


Рис. 7-35: Настройка зон межсетевого экрана. Общие настройки

- «Использовать маскарадинг только для указанных подсетей-отправителей» — позволяет ограничить использование трансляции адресов указанными подсетями-отправителями.
- «Использовать маскарадинг только для указанных подсетей-получателей» — позволяет ограничить использование трансляции адресов указанными подсетями-получателями.
- «Включить отслеживание соединений» — включает или отключает механизм отслеживания соединений (conntrack) для данной зоны.
- «Включить журналирование в этой зоне» — включает или отключает запись срабатывания правил межсетевого экрана для данной зоны в системный журнал

Для каждой зоны указываются настройки перенаправления между зонами в подразделе «Перенаправление между зонами» (см. рисунок 7-35).

Данные настройки управляют политиками перенаправления трафика между редактируемой зоной и другими зонами:

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

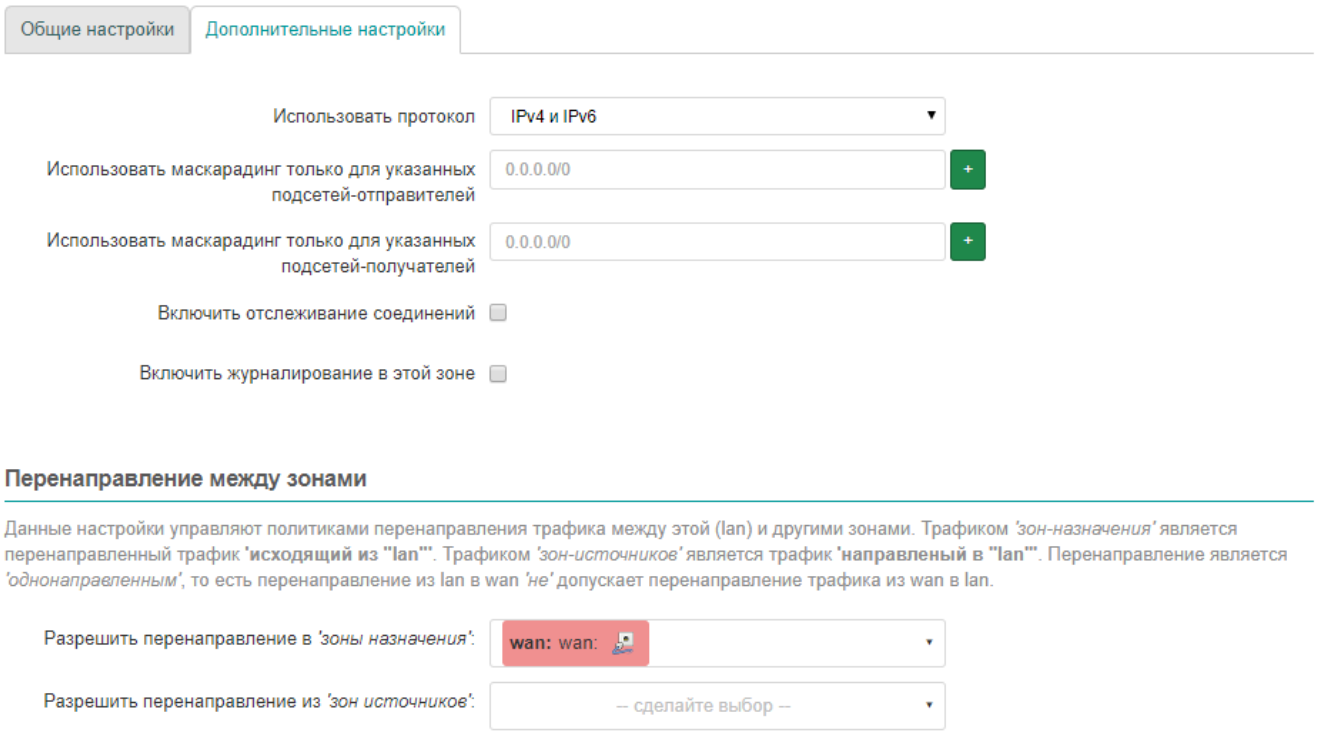


Рис. 7-36: Настройка зон межсетевого экрана. Дополнительные настройки

Трафиком зон-назначения является перенаправленный трафик, исходящий из редактируемой зоны.

Трафиком зон-источников является трафик, направленный в редактируемую зону.

Перенаправление является однонаправленным, то есть перенаправление из одной зоны в другую зону не допускает перенаправление трафика в обратную сторону.

7.5.2.2 Добавление зон

Для добавления новой зоны предназначена кнопка «Добавить», расположенная снизу таблицы зон (см. рисунок 7-34). При этом открывается такая же страница редактирования параметров зоны, как и при изменении существующей зоны (см. раздел 7.5.2.1).

7.5.2.3 Удаление зон

Удаление существующей зоны выполняется при помощи кнопки «Удалить», расположенной в строке соответствующей зоны (см. рисунок 7-34).

7.5.3 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 7-37.

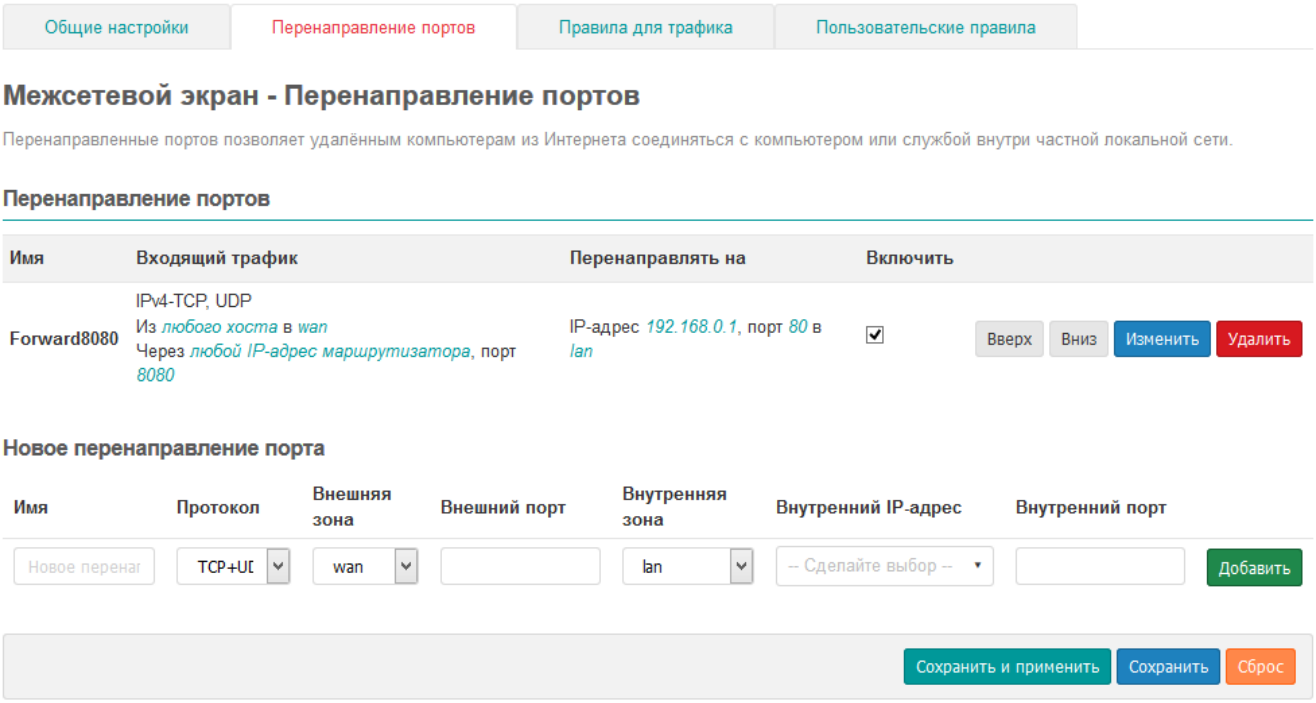


Рис. 7-37: Вкладка «Перенаправление портов» страницы «Межсетевой экран»

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

- «Имя» — уникальное символьное имя правила перенаправления.
- «Входящий трафик» — в данном столбце приведены условия для входящего трафика, при совпадении которых данное правило будет применяться.
- «Перенаправлять на» — 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.

7.5.3.1 Порядок применения правил перенаправления портов

Правила перенаправления применяются в том порядке (сверху вниз), в котором они указаны в таблице. Для изменения порядка правил предназначены кнопки «Вверх» и «Вниз» (см. рисунок 7-37), позволяющие переместить соответствующее правило вверх или вниз соответственно.

7.5.3.2 Редактирование правил перенаправления портов

Для редактирования правил перенаправления портов необходимо нажать кнопку «Изменить» (см. рисунок 7-37), расположенную в строке соответствующего правила. При этом откроется страница редактирования правила перенаправления портов, как показано на рисунке 7-38.

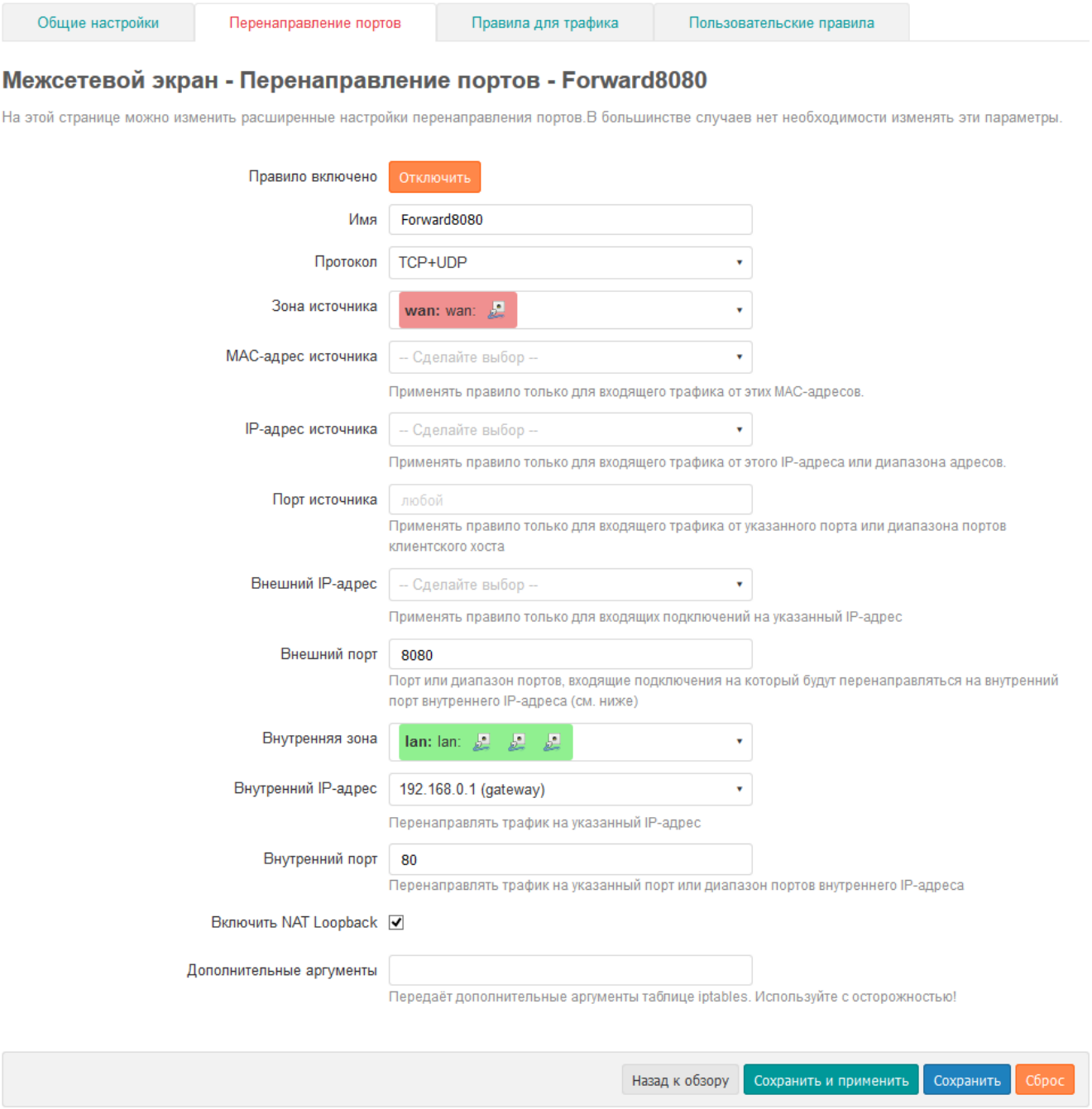


Рис. 7-38: Настройка правила перенаправления портов межсетевого экрана

На данной странице доступны для редактирования следующие настройки правила перенаправления портов:

- «Правило включено» — кнопка-переключатель, позволяющая включить или отключить применение редактируемого правила.
- «Имя» — уникальное символьное имя правила.
- «Протокол» — выбор протокола правила. Возможен выбор из вариантов:
  - UDP;
  - TCP;
  - UDP + TCP;
  - ICMP;
  - пользовательский (произвольное имя протокола).

  В зависимости от выбранного протокола набор настроек может несущественно меняться.

- «Зона источника» — выбор зоны источника трафика для правила.
- «MAC-адрес источника» — позволяет указать один или несколько MAC-адресов источника трафика для правила. Если MAC-адреса заданы, то правило будет применяться только для входящего трафика от указанных MAC-адресов.
- «IP-адрес источника» — позволяет указать один или несколько IP-адресов источника трафика для правила. Если IP-адреса заданы, то правило будет применяться только для входящего трафика от указанных IP-адресов.
- «Порт источника» — позволяет указать порт или диапазон портов источника трафика для правила. Если этот параметр задан, то правило будет применяться только для входящего трафика от указанного порта или диапазона портов устройства источника трафика. Данная настройка доступна только для UDP и TCP протоколов.
- «Внешний IP-адрес» — позволяет ограничить применение правила для входящих подключений на указанный IP-адрес. Если не задан (значение «любой»), то правило применяется к входящим подключениям на все IP-адреса устройства.
- «Внешний порт» — позволяет ограничить применение правила для входящих подключений на указанный порт или диапазон портов. Данная настройка доступна только для UDP и TCP протоколов.
- «Внутренняя зона» — выбор зоны назначения (перенаправления) трафика для правила.
- «Внутренний IP-адрес» — выбор IP-адреса для перенаправления трафика. Трафик правила будет перенаправляться на указанный IP-адрес.
- «Внутренний порт» — выбор порта для перенаправления трафика. Трафик правила будет перенаправляться на указанный порт внутреннего IP-адреса. Данная настройка доступна только для UDP и TCP протоколов.
- «Включить NAT Loopback» — включить для данного правила технологию NAT Loopback [20].

  Данная технология позволяет считать пакет, пришедший из внутренней сети на внешний IP-адрес устройства, как пакет пришедший извне. Таким образом, для такого пакета работают правила брандмауэра, относящиеся к внешним соединениям.
- «Дополнительные аргументы» — позволяет указать дополнительные аргументы для команды iptables.

7.5.3.3 Добавление правил перенаправления портов

Для добавления нового правила перенаправления портов необходимо заполнить основные параметры нового правила перенаправления в таблице подраздела «Новое перенаправление порта» (см. рисунок 7-39) и нажать кнопку «Добавить».

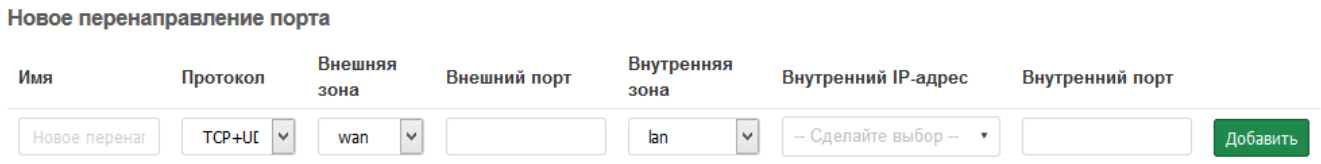


Рис. 7-39: Добавление правила перенаправления портов межсетевого экрана

Значения параметров добавляемого правила описаны в разделе редактирования параметров правил перенаправления портов (раздел 7.5.3.2).

7.5.3.4 Удаление правил перенаправления портов

Для удаления правила перенаправления портов предназначена кнопка «Удалить» (см. рисунок 7-37), расположенная в строке соответствующего правила.

7.5.4 Правила для трафика

Управление правилами для трафика межсетевого экрана осуществляется на вкладке «Правила для трафика» страницы «Межсетевой экран» (см. рисунок 7-40).

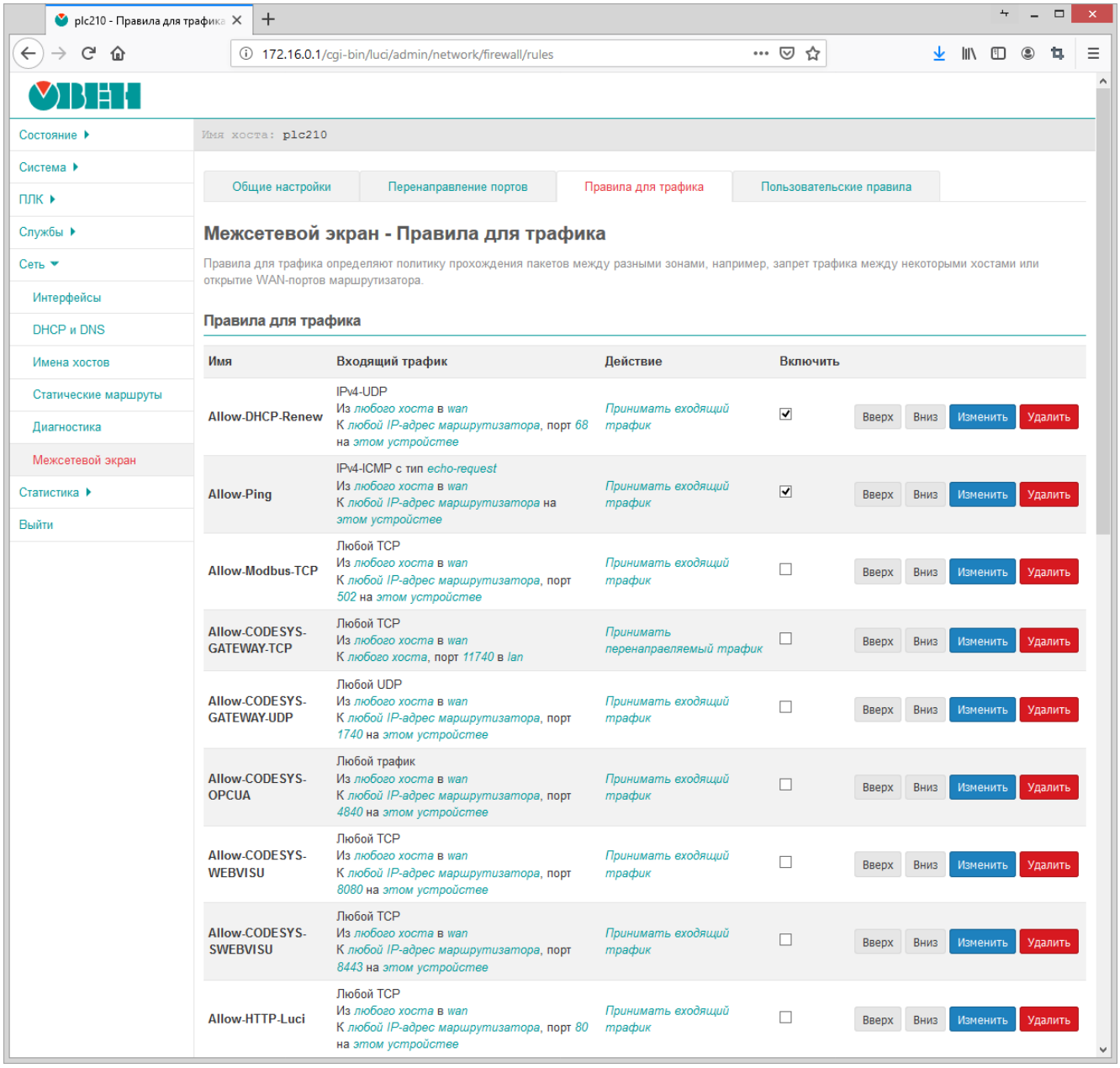


Рис. 7-40: Правила для трафика межсетевого экрана

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

- «Имя» — уникальное символьное имя правила.
- «Входящий трафик» — 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. Если правило выключено, то оно не будет применяться к входящему трафику.

7.5.4.1 Порядок применения правил для трафика

Правила для трафика применяются в том порядке (сверху вниз), в котором они указаны в таблице. Для изменения порядка правил предназначены кнопки «Вверх» и «Вниз» (см. рисунок 7-40), позволяющие переместить соответствующее правило вверх или вниз соответственно.

7.5.4.2 Редактирование правил для трафика

Для редактирования правила для трафика необходимо нажать кнопку «Изменить» (см. рисунок 7-40), расположенную в строке соответствующего правила. При этом откроется страница редактирования правила для трафика, как показано на рисунке 7-41.

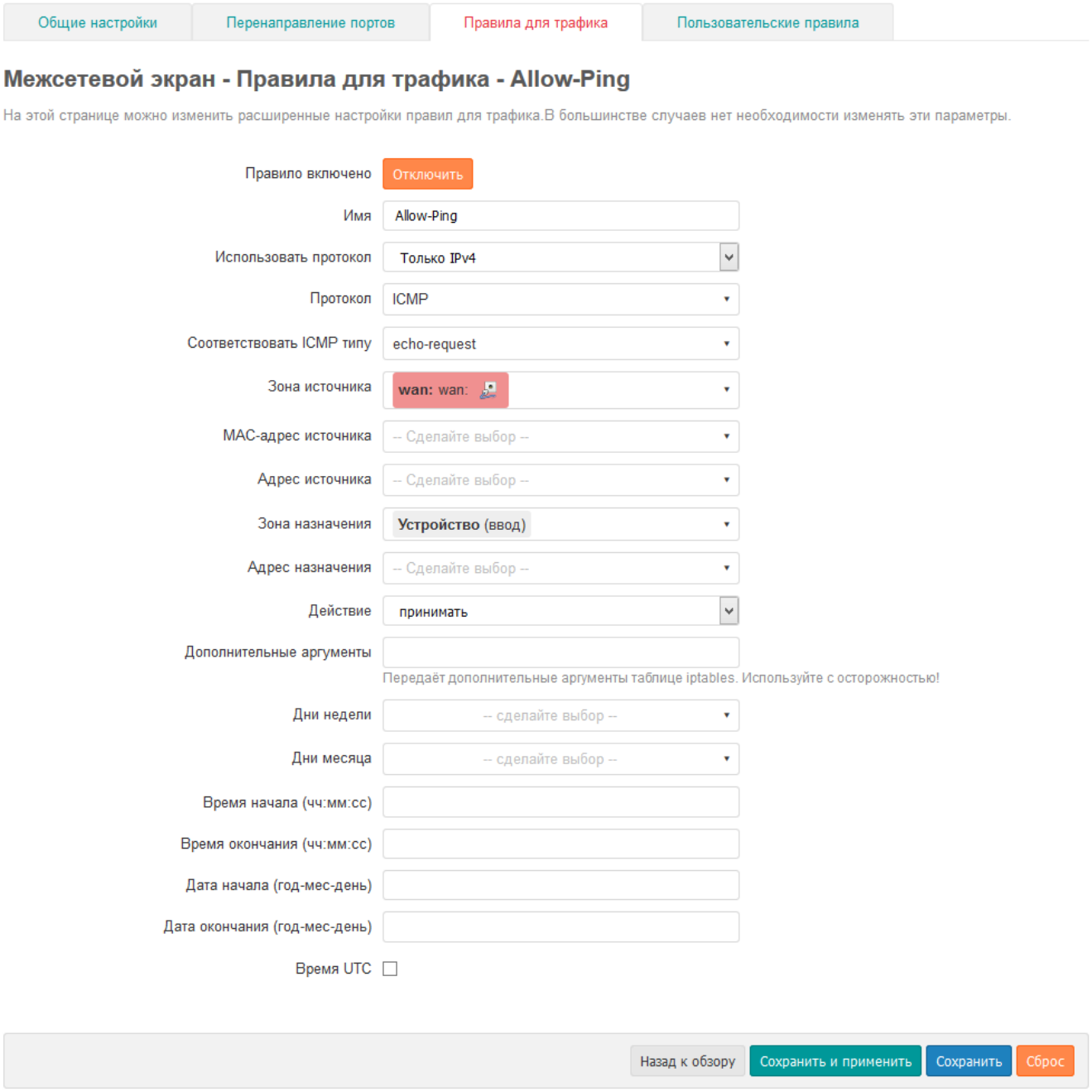


Рис. 7-41: Настройка правила для трафика межсетевого экрана

На данной странице доступны для редактирования следующие настройки правила для трафика:

- «Правило включено» — кнопка-переключатель, позволяющая включить или отключить применение редактируемого правила.
- «Имя» — уникальное символьное имя правила.

- «Использовать протокол» — выбор версий IP-протокола для данного правила. Возможен выбор из вариантов:
  - только IPv4;
  - только IPv6;
  - IPv4 и IPv6.
- «Протокол» — выбор протокола входящего трафика правила. Возможен выбор из вариантов:
  - Любой;
  - UDP;
  - TCP;
  - UDP + TCP;
  - ICMP;
  - пользовательский (произвольное имя протокола).

  В зависимости от выбранного протокола набор настроек может несущественно меняться.
- «Соответствовать ICMP типу» — выбор типов ICMP пакетов, для которых данное правило будет применяться. Настройка доступна только в случае выбора ICMP протокола.
- «Зона источника» — выбор источника трафика для правила. Кроме конкретной зоны возможно указать следующие варианты:
  - Устройство — любой исходящий трафик на любом IP-адресе устройства;
  - Любая зона — источником трафика для данного правила является любой входящий трафик от любого хоста любой зоны межсетевого экрана.
- «MAC-адрес источника» — позволяет указать один или несколько MAC-адресов источника трафика для правила. Если MAC-адреса заданы, то правило будет применяться только для входящего трафика от указанных MAC-адресов.
- «Адрес источника» — позволяет указать один или несколько IP-адресов источника трафика для правила. Если IP-адреса заданы, то правило будет применяться только для входящего трафика от указанных IP-адресов.
- «Порт источника» — позволяет указать порт или диапазон портов источника трафика для правила. Если этот параметр задан, то правило будет применяться только для входящего трафика от указанного порта или диапазона портов устройства источника трафика. Данная настройка доступна только для UDP и TCP протоколов.
- «Зона назначения» — выбор назначения трафика для правила. Кроме конкретной зоны возможно указать следующие варианты:
  - не определено — любой трафик;
  - Устройство — любой исходящий трафик на любой IP-адрес устройства;
  - Любая зона — любой исходящий трафик на любой хост в любой зоне межсетевого экрана.
- «Адрес назначения» — для правил перенаправления указывается IP-адрес для перенаправления. Трафик правила будет перенаправляться на указанный IP-адрес.
- «Порт назначения» — для правил перенаправления указывается порт для перенаправления трафика. Трафик правила будет перенаправляться на указанный порт адреса назначения. Данная настройка доступна только для UDP и TCP протоколов.
- «Действие» — выбор действия, применяемого для входящего (или перенаправляемого) трафика данного правила. Возможен выбор из вариантов:
  - принимать;
  - отвергать;
  - не обрабатывать;
  - не отслеживать.
- «Дополнительные аргументы» — позволяет указать дополнительные аргументы для команды iptables.
- «Дни недели», «дни месяца» — позволяет указать дни недели и/или дни месяца, в которые данное правило должно применяться. Если данные настройки указаны, то правило будет применяться только в указанные дни.

- «Время начала», «время окончания» — позволяет указать время начала и окончания действия правила. Если данные настройки указаны, то правило будет применяться только в указанный период времени.
- «Дата начала», «дата окончания» — позволяет указать даты начала и окончания действия правила. Если данные настройки указаны, то правило будет применяться только в указанный период дат.
- «Время UTC» — если данная настройка включена, то время действия правила указывается в UTC. В противном случае время указывается в локальной временной зоне.

7.5.4.3 Добавление правил для трафика

Для добавления нового правила для трафика предназначены подразделы «Открыть порты на маршрутизаторе» и «Новое правило перенаправления» (см. рисунок 7-42), которые следуют сразу же за таблицей «Правила для трафика» на вкладке «Правила для трафика» страницы «Межсетевой экран».

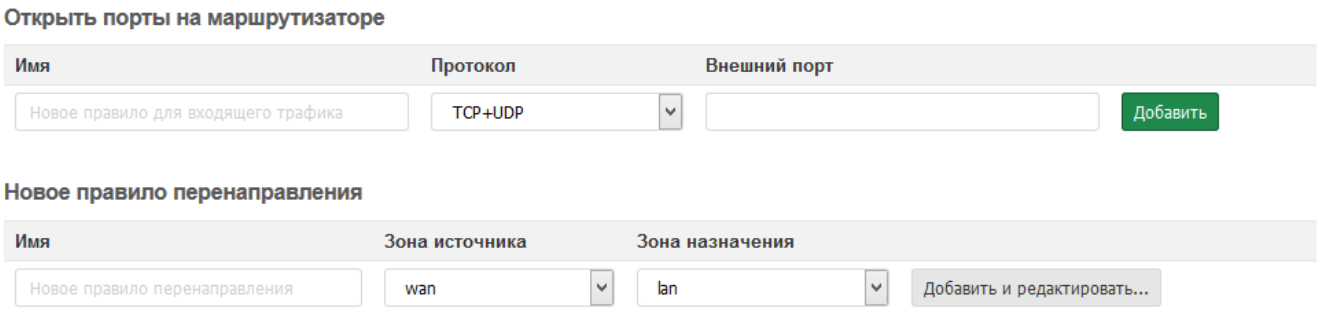


Рис. 7-42: Добавление правил для трафика межсетевого экрана

В разделе «Открыть порты на маршрутизаторе» необходимо указать символьное имя создаваемого правила, протокол и номер внешнего порта, после чего нажать кнопку «Добавить». В этом случае будет создано новое правило для трафика с указанным именем, в котором в качестве зоны источника будет выступать зона «wan», а в качестве зоны назначения будет выступать устройство (т.е. любой IP-адрес устройства).

В разделе «Новое правило перенаправления» необходимо указать символьное имя создаваемого правила, зону источника и зону назначения, после чего нажать кнопку «Добавить и редактировать...». В этом случае будет открыто окно редактирования правил для трафика (см. раздел 7.5.4.2), где в качестве имени зоны, зоны источника и зоны назначения будут указаны выбранные значения.

7.5.4.4 Удаление правил для трафика

Для удаления правила для трафика предназначена кнопка «Удалить» (см. рисунок 7-40), расположенная в строке соответствующего правила.

7.5.5 Пользовательские правила

На вкладке «Пользовательские правила» настроек межсетевого экрана (см. рисунок 7-43) расположено поле ввода, в котором можно указывать произвольные команды iptables [5]. Данные команды будут автоматически выполняться после каждой перезагрузки службы межсетевого экрана следом за загрузкой правил по умолчанию.

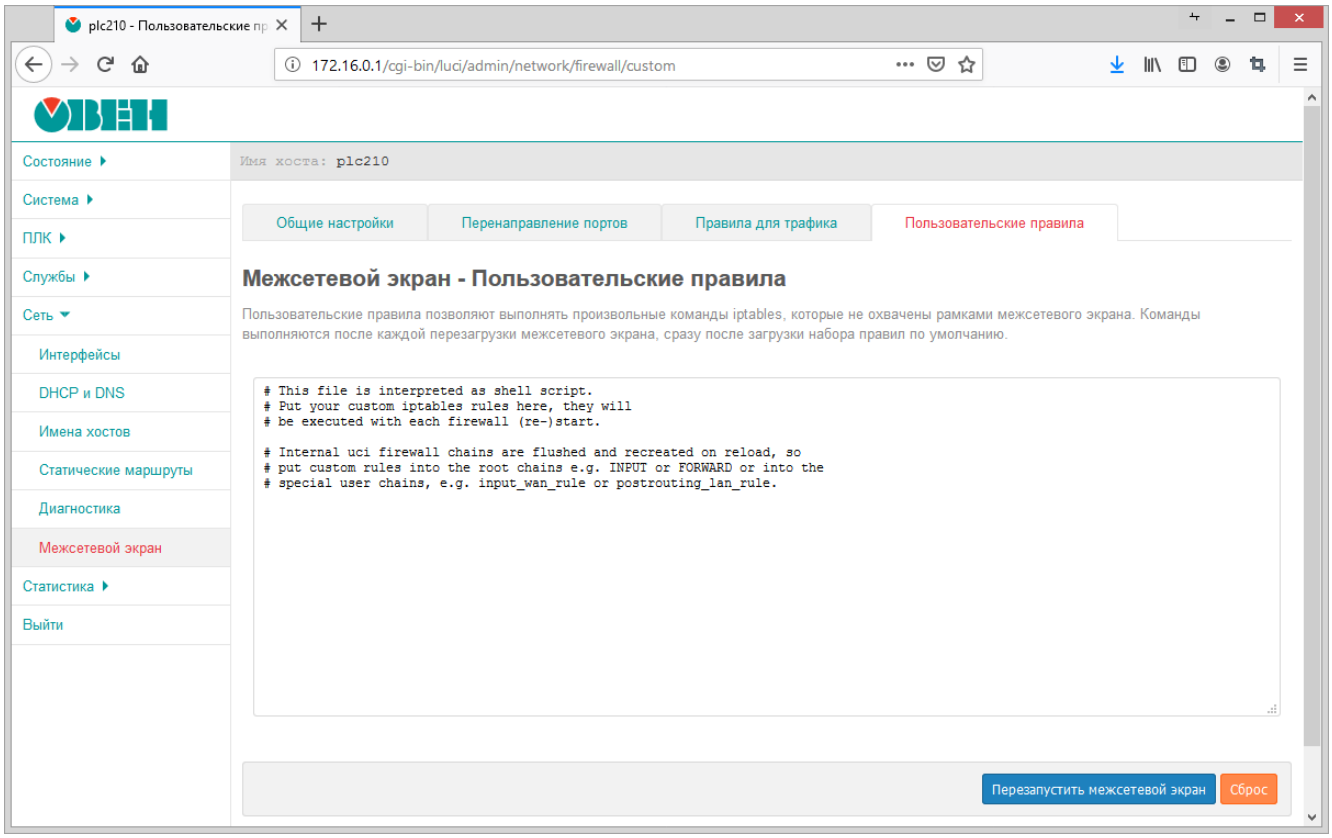


Рис. 7-43: Пользовательские правила межсетевого экрана

Здесь же имеется кнопка «Перезапустить межсетевой экран», позволяющая выполнить перезапуск службы межсетевого экрана с применением пользовательских правил.

7.6 Диагностика

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

- «Пинг-запрос» (см. раздел 7.6.1) — выполнение пинг-запроса указанного IPv4 или IPv6-адреса (IP-адрес или доменное имя).
- «Трассировка» (см. раздел 7.6.2) — выполнение IPv4 или IPv6 трассировки указанного адреса (IP-адрес или доменное имя).
- «DNS-запрос» (см. раздел 7.6.3) — выполнение DNS-запроса указанного адреса (IP-адрес или доменное имя).

Внешний вид страницы «Диагностика» показан на рисунке 7-44.

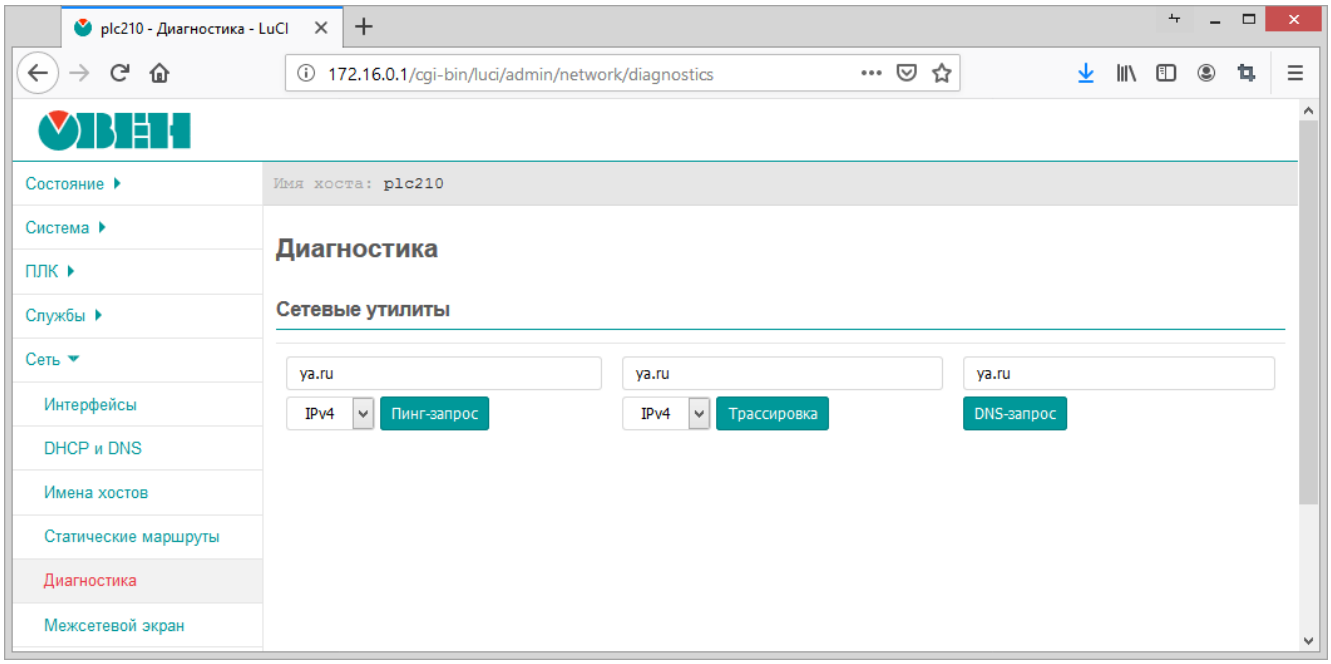


Рис. 7-44: Страница «Диагностика»

При выполнении какой-либо из диагностик, результат будет выведен в текстовом виде, как показано на рисунке 7-45.

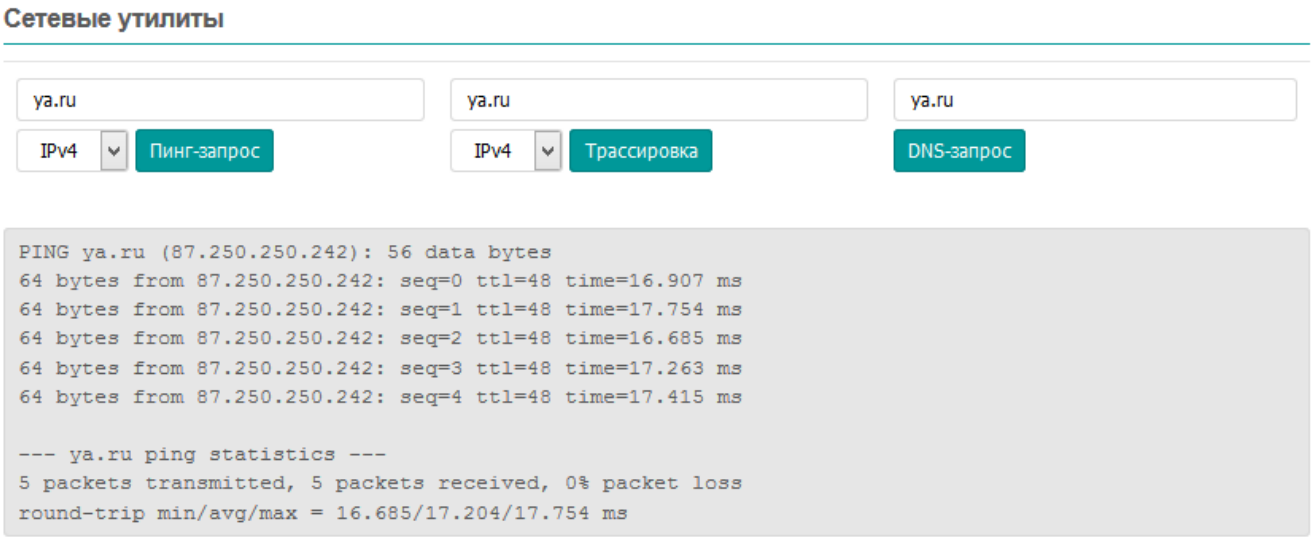


Рис. 7-45: Страница «Диагностика». Вывод результата диагностики

7.6.1 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>
```

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
```

7.6.2 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>
```

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
```

7.6.3 DNS-запрос

Выполнение DNS-запроса адреса соответствует выполнению команды:

```
nslookup <адрес>
```

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
```

8 Статистика

В разделе главного меню «Статистика» содержатся страницы управления и просмотра графиков статистики, полученных при помощи службы collectd [21].

Collectd — это небольшая служба, которая с заданным интервалом собирает статистику об использовании ресурсов системы. Объём собираемых данных определяется набором плагинов (подключаемых модулей).

На рисунке 8-1 приведена страница просмотра графиков статистики. Просмотр графиков осуществляется в разделе «Графики» раздела «Статистика» главного меню.

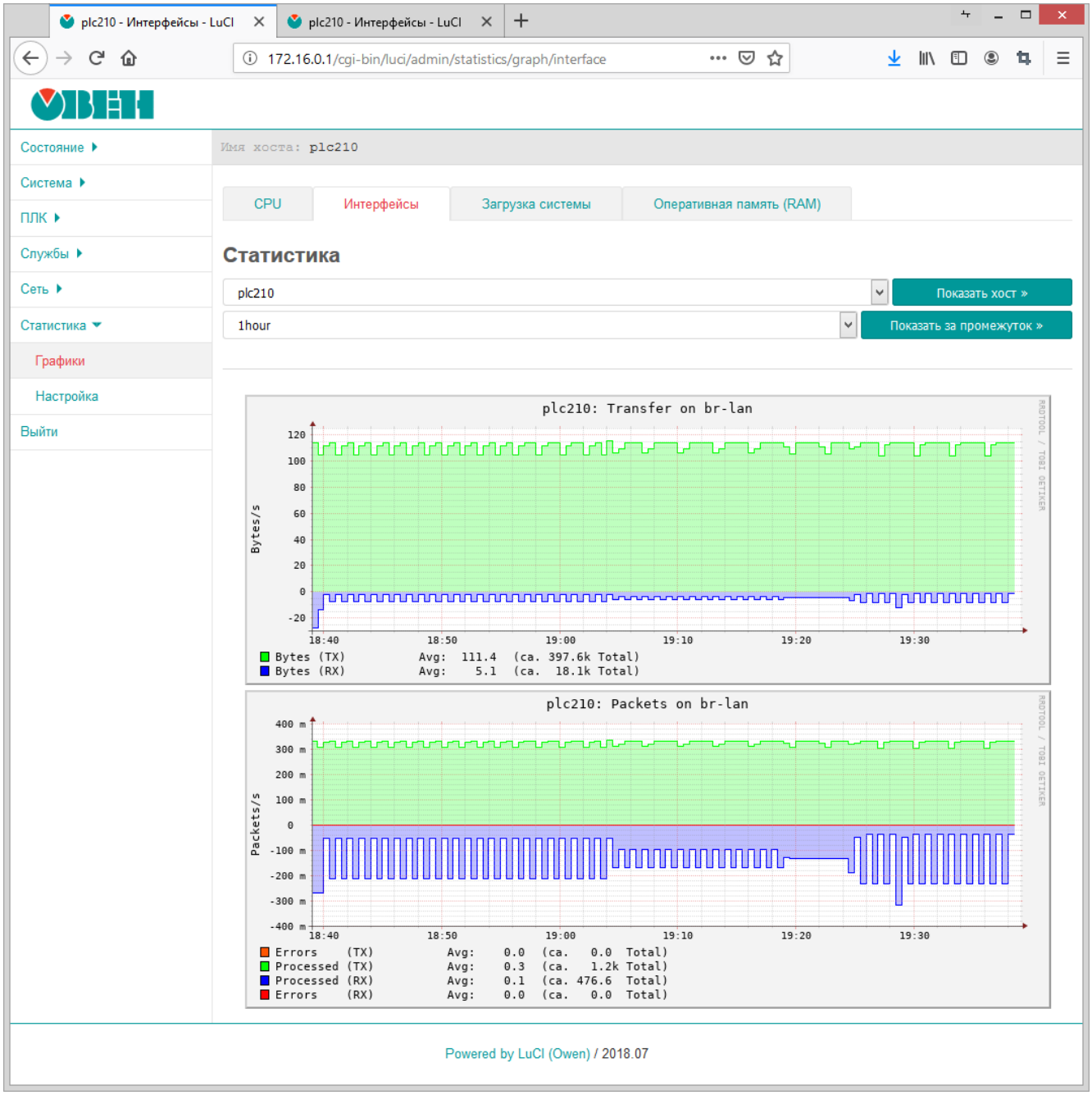


Рис. 8-1: Страница просмотра графиков статистики

8.1 Настройки сбора и отображения статистики

Страница настроек сбора и отображения статистики расположена в подразделе «Настройка» раздела «Статистика» главного меню (см. рисунок 8-2).

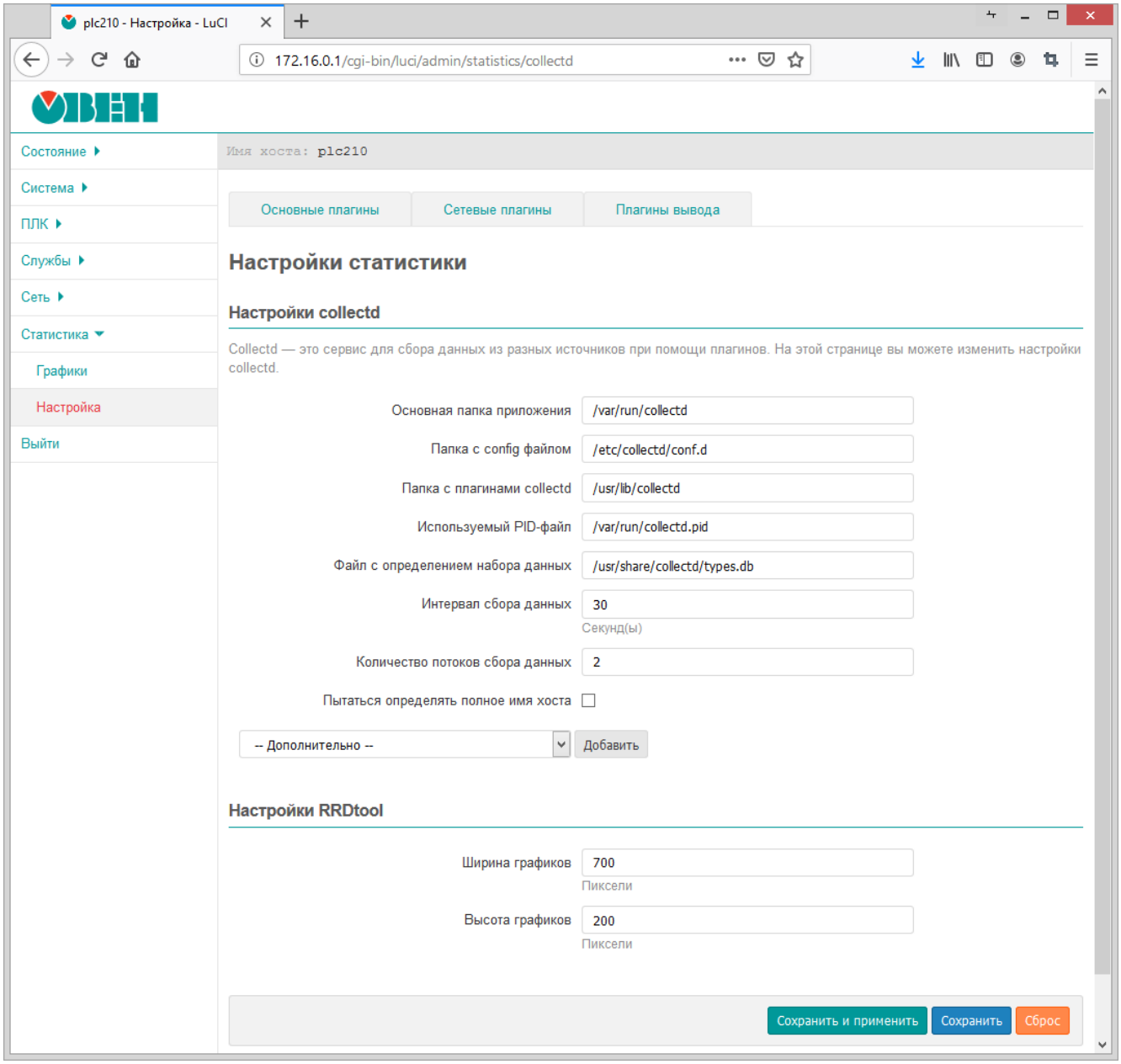


Рис. 8-2: Настройки сбора и отображения статистики

На данной странице расположены следующие настройки сбора и отображения статистики службы collectd:

- «Основная папка приложения» — путь к основной рабочей папке службы collectd;
- «Папка с config файлом» — путь к папке конфигурационных файлов службы collectd;
- «Папка с плагинами collectd» — путь к папке с плагинами службы collectd;
- «Используемый PID-файл» — путь к PID-файлу службы collectd;
- «Файл с определением набора данных» — путь к файлу определений наборов данных службы collectd [22];
- «Интервал сбора данных» — интервал сбора данных службой collectd (в секундах);
- «Количество потоков сбора данных» — количество одновременно работающих потоков сбора данных;
- «Имя хоста» — имя данного хоста. Если не задано, имя хоста будет определено автоматически.
- «Пытаться определять полное имя хоста» — настройка указывающая требуется ли пытаться определить полное имя хоста (FQDN) или использовать короткое. Данная настройка доступна только если не задано значение параметру «Имя хоста».

Дополнительно в подразделе «Настройки RRDtool» возможно указать размеры в пикселях (ширина и высота) отображаемых графиков.

8.2 Плагины (подключаемые модули)

В самом верху страницы настроек (см. раздел 8.1) расположены вкладки управления плагинами (подключаемыми модулями) службы collectd.

Большинство плагинов возможно только включить, либо выключить. Но некоторые из плагинов имеют свои собственные дополнительные настройки, влияющие на сбор и отображение данных. Если у плагина имеются такие дополнительные настройки, их описание приводится в разделе соответствующего плагина.

8.2.1 Основные плагины

8.2.1.1 Переключения контекста

Данный плагин собирает статистику о количестве переключений контекста процессора.

Пример графика данных, полученных при помощи данного плагина, показан на рисунке 8-3.

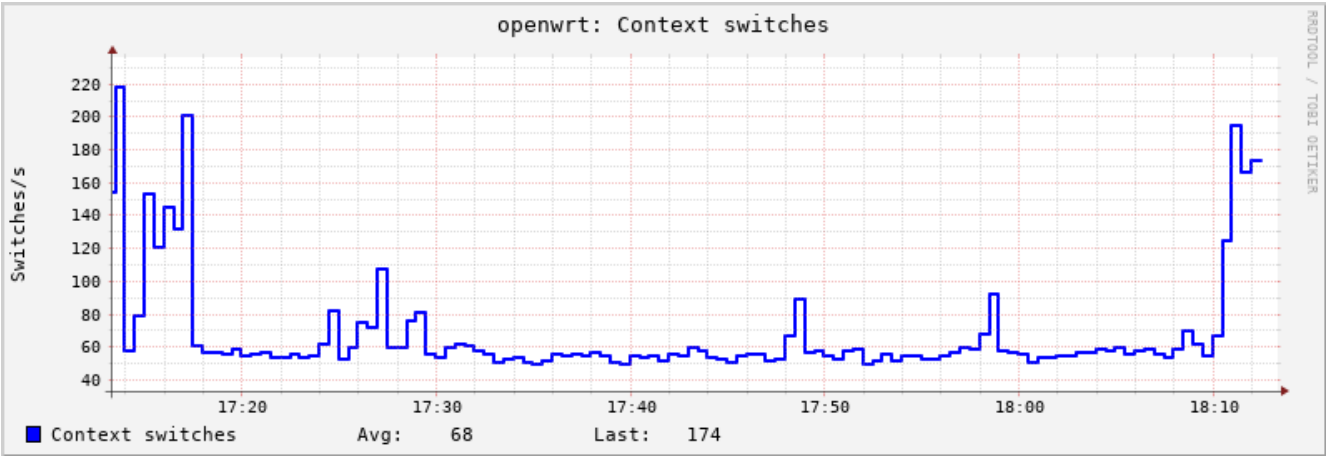


Рис. 8-3: Статистика. График переключений контекста процессора

8.2.1.2 CPU

Плагин «CPU» собирает статистику об использовании процессора.

Пример графика данных, полученных при помощи данного плагина, показан на рисунке 8-4.

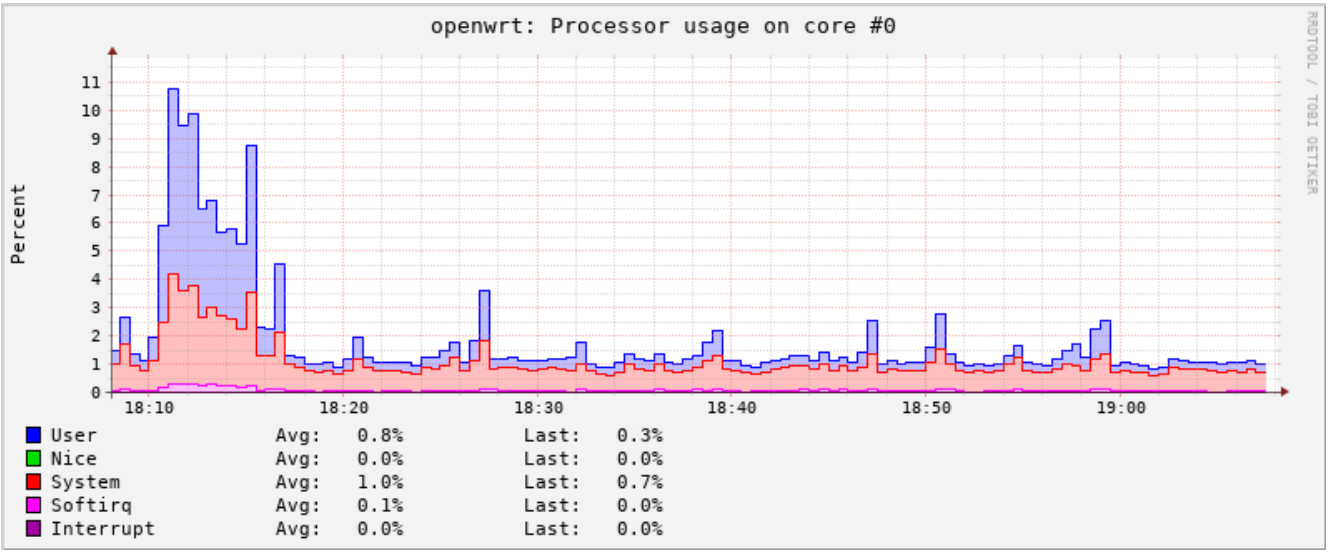


Рис. 8-4: Статистика. График использования процессора

8.2.1.3 Entropy

Плагин «Entropy» собирает статистику о доступной энтропии.

Пример графика данных, полученных при помощи данного плагина, показан на рисунке 8-5.

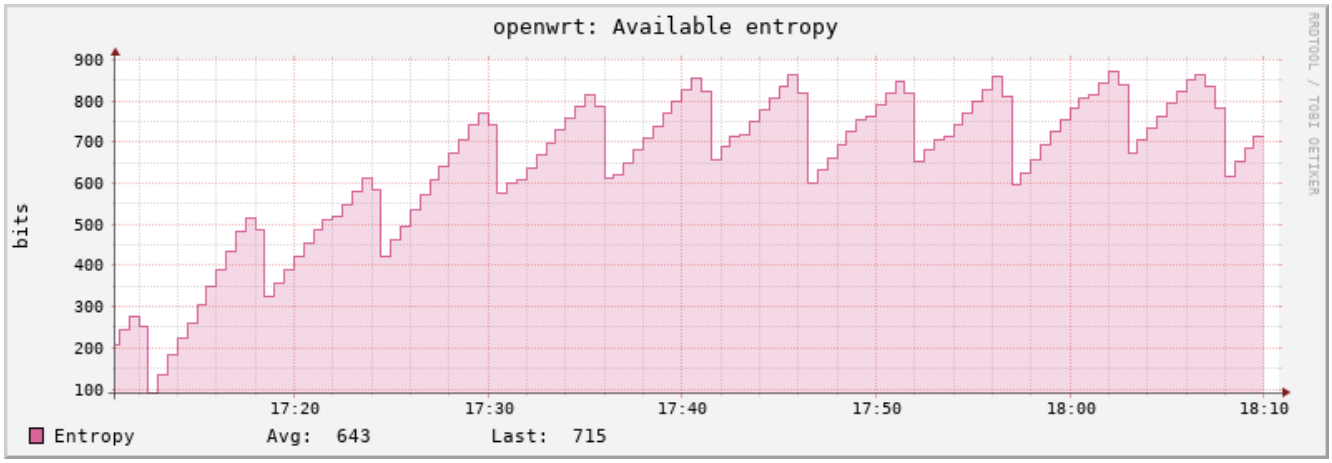


Рис. 8-5: Статистика. График доступной энтропии

8.2.1.4 Прерывания

Плагин «Прерывания» собирает статистику по выбранным прерываниям.

Плагин имеет дополнительные настройки:

- «Мониторить прерывания» — список номеров прерываний (разделённых символом пробела), для которых требуется собирать статистику. Если ни одно прерывание не указано, сбор статистики будет проводиться по всем прерываниям.
- «Собирать статистику со всех кроме указанных» — если опция включена, то сбор статистики будет производиться только для прерываний, номера которых не указаны в списке «Мониторить прерывания».

8.2.1.5 Загрузка системы

Плагин «Загрузка системы» собирает статистику о средней загрузке системы за 1, 5 и 15 минут [3].

Пример графика данных, полученных при помощи данного плагина, показан на рисунке 8-6.

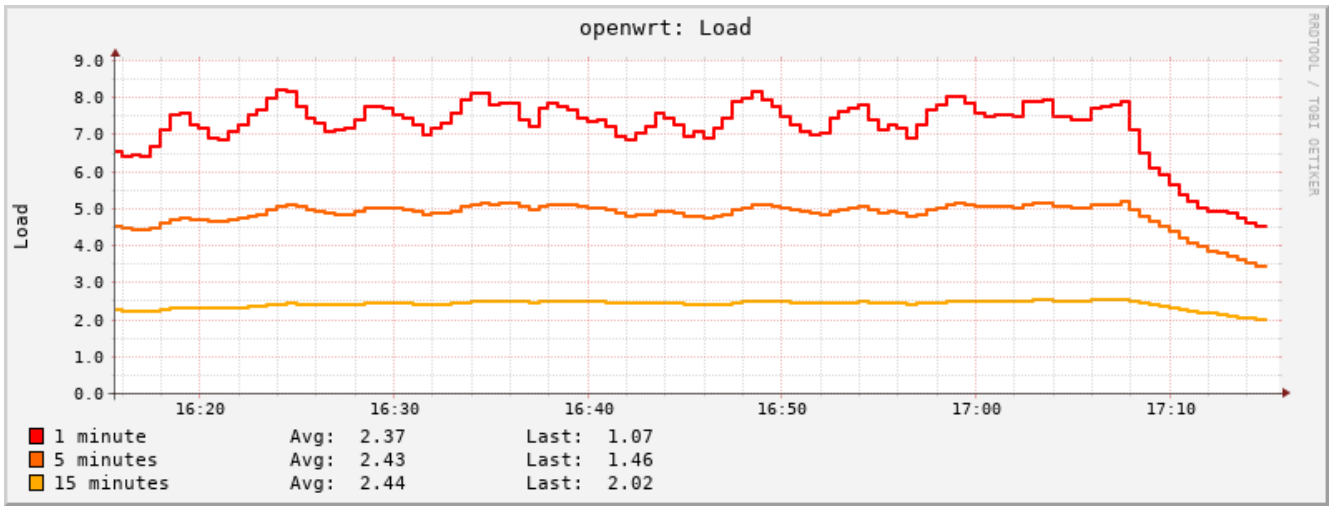


Рис. 8-6: Статистика. График средней загрузки системы

8.2.1.6 Оперативная память (RAM)

Плагин «Оперативная память (RAM)» собирает статистику об использовании памяти.

Пример графика данных, полученных при помощи данного плагина, показан на рисунке 8-7.

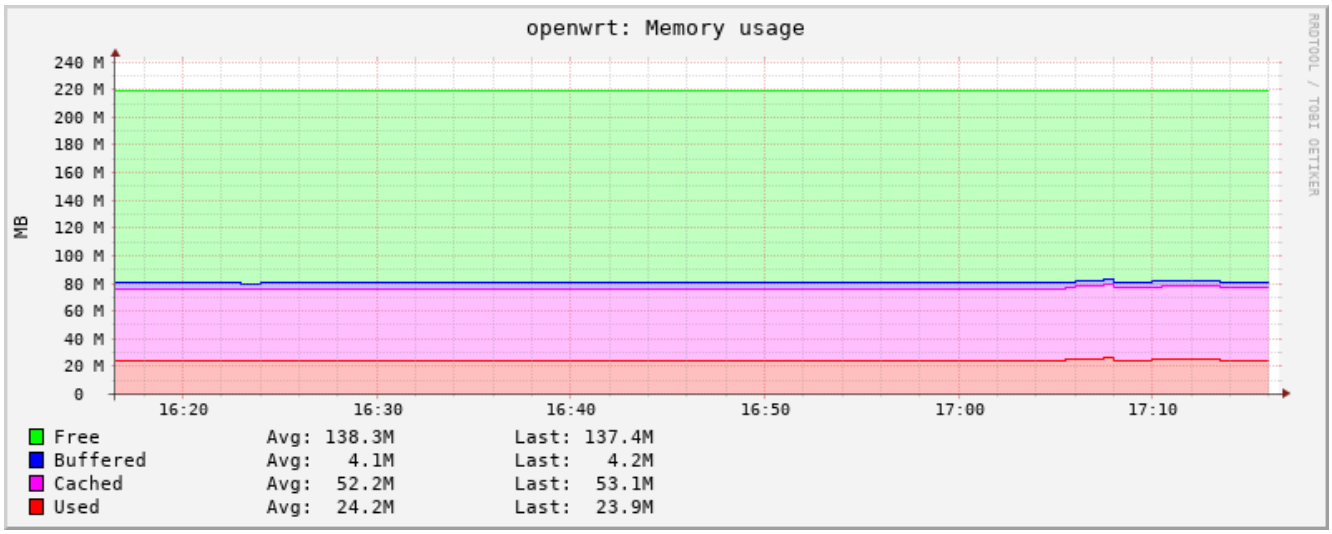


Рис. 8-7: Статистика. График использования оперативной памяти

8.2.1.7 Процессы

Плагин «Процессы» собирает информацию, такую как время CPU, ошибки страницы и использование памяти для выбранных процессов.

Плагин имеет настройку «Мониторить процессы», которая представляет собой список процессов (разделённых символом пробела), для которых требуется собирать статистику.

Для каждого выбранного процесса строится несколько графиков:

- время CPU отведённое выбранному процессу. Пример графика приведён на рисунке 8-8;
- потоки и дочерние процессы принадлежащие выбранному процессу. Пример графика приведён на рисунке 8-9;
- ошибки страниц (page faults) выбранного процесса. Пример графика приведён на рисунке 8-10;
- размер страниц памяти, выделенных процессу операционной системой и в настоящее время находящихся в оперативной памяти (RSS). Пример графика приведён на рисунке 8-11;
- размер виртуальных страниц памяти, выделенных процессу операционной системой (VSZ). Пример графика приведён на рисунке 8-12.

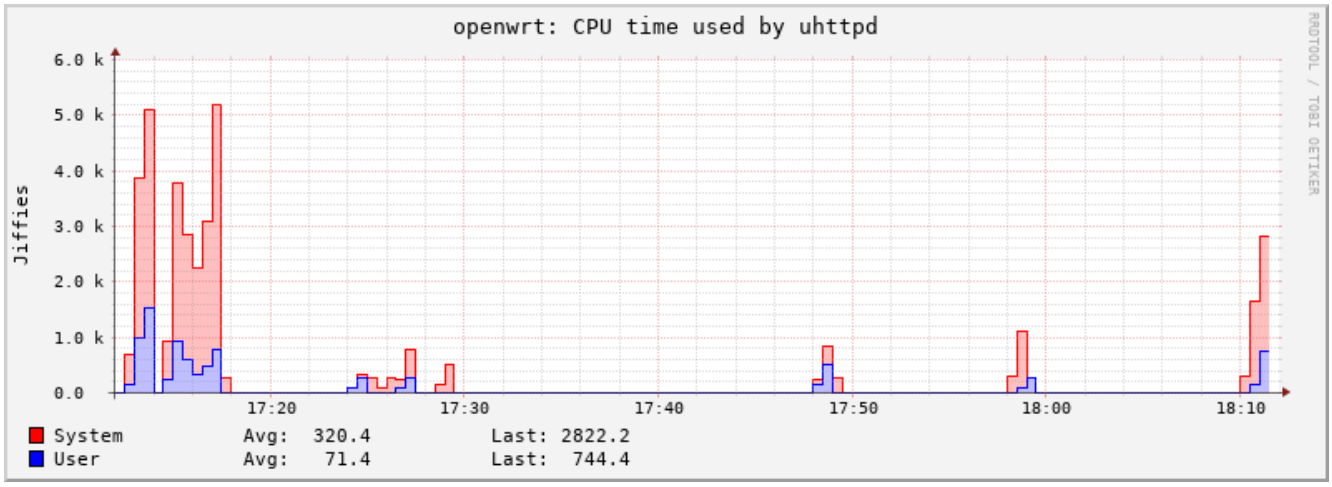


Рис. 8-8: Статистика. График времени CPU для процесса

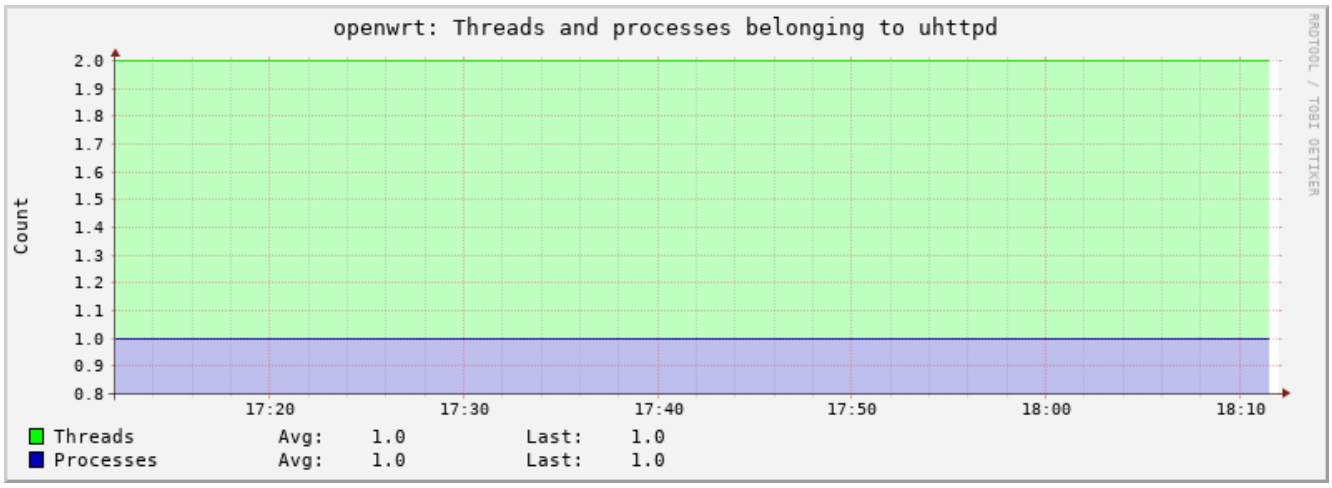


Рис. 8-9: Статистика. График потоков процесса

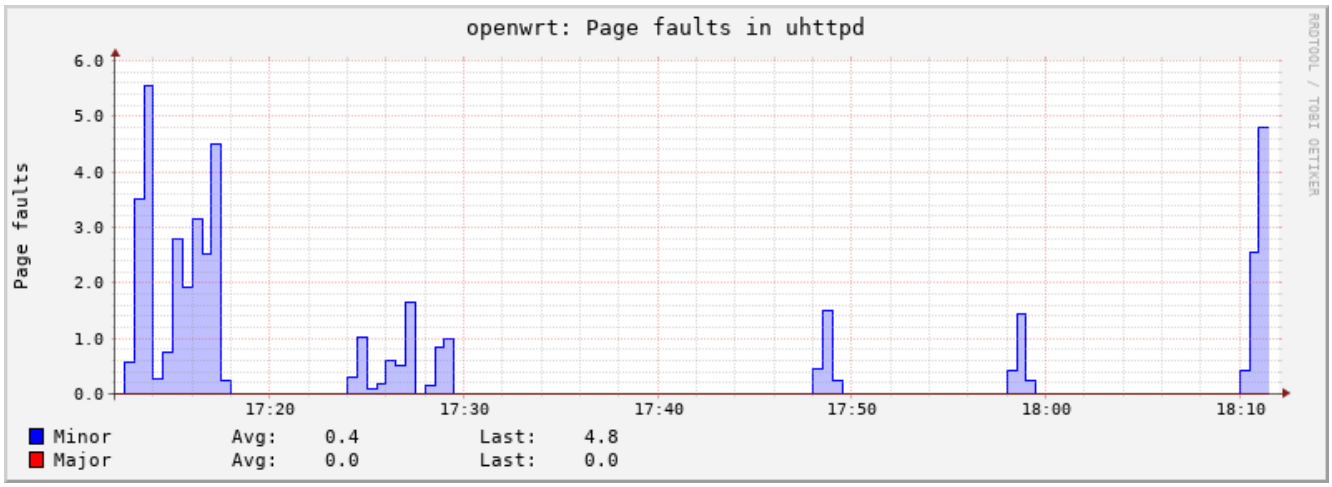


Рис. 8-10: Статистика. График ошибок страниц процесса

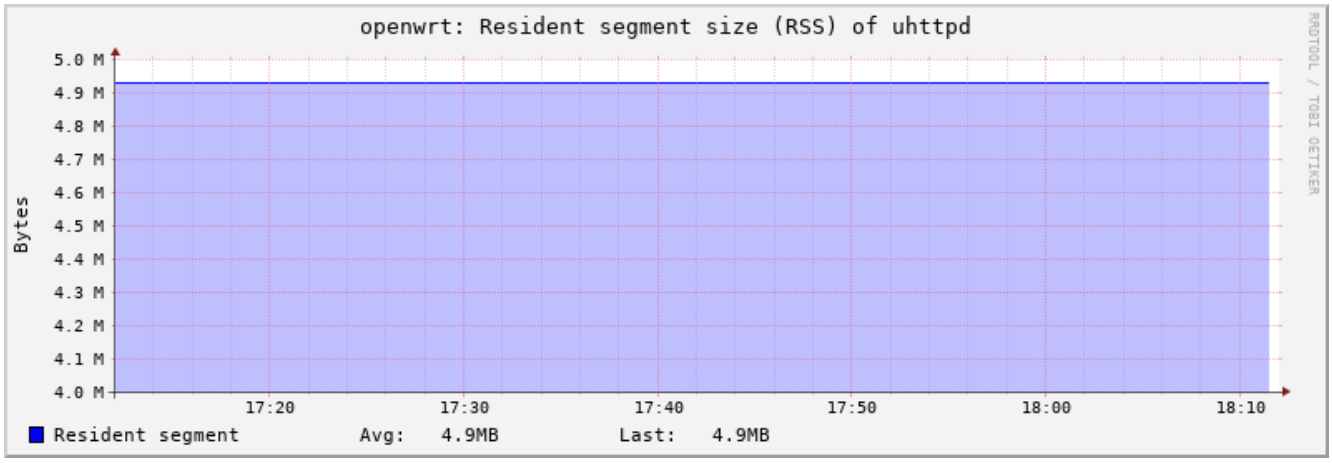


Рис. 8-11: Статистика. График RSS процесса

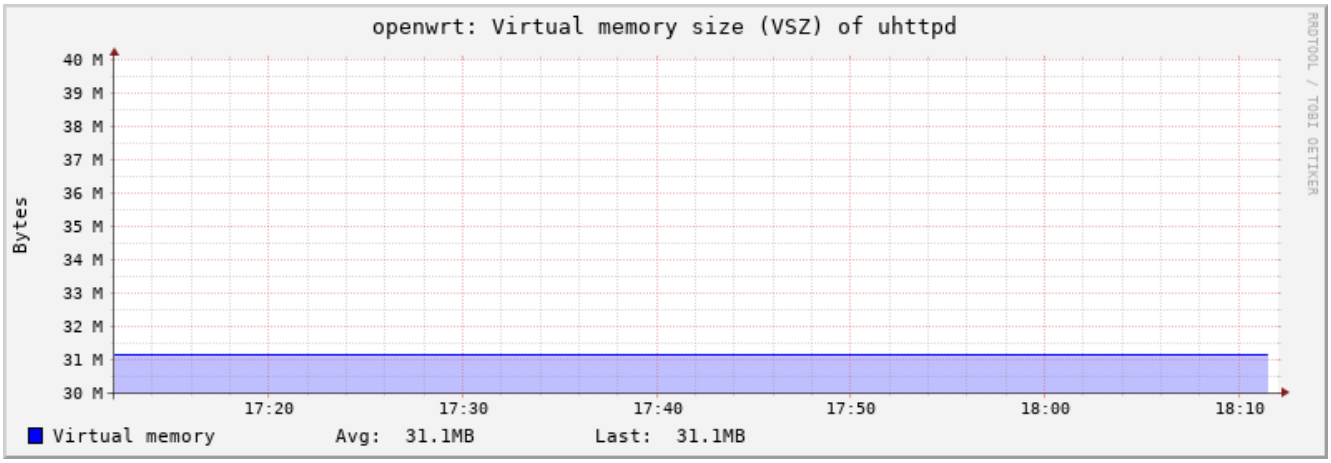


Рис. 8-12: Статистика. График VSZ процесса

8.2.1.8 Время работы

Плагин «Время работы» собирает статистику о времени работы системы.

Пример графика данных, полученных при помощи данного плагина, показан на рисунке 8-13.

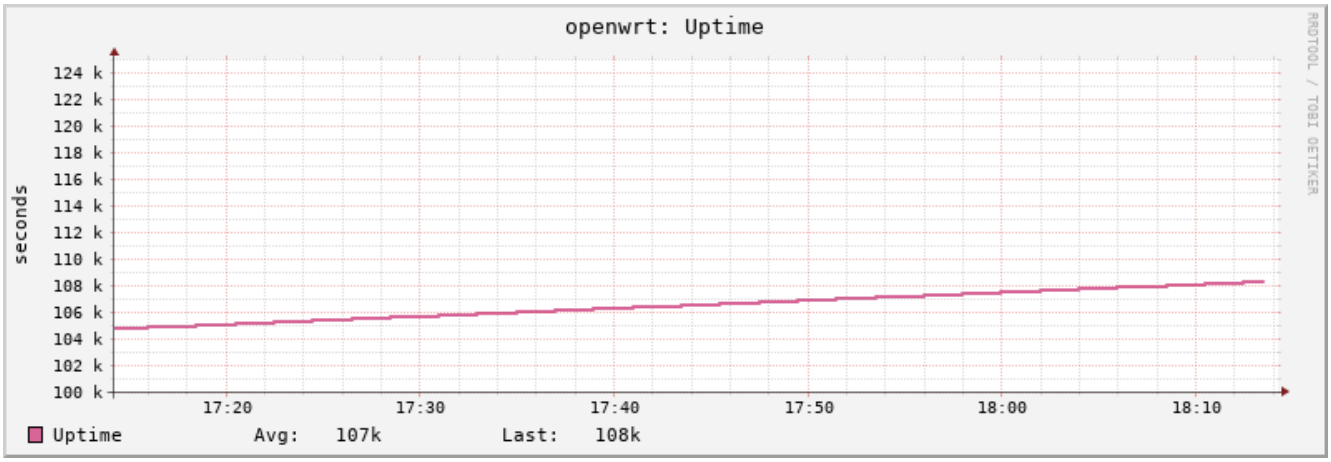


Рис. 8-13: Статистика. График времени работы

8.2.2 Сетевые плагины

8.2.2.1 Отслеживание подключений (Conntrack)

Плагин «Отслеживание подключений (Conntrack)» собирает статистику о количестве отслеживаемых соединений.

Пример графика данных, полученных при помощи данного плагина, показан на рисунке 8-14.

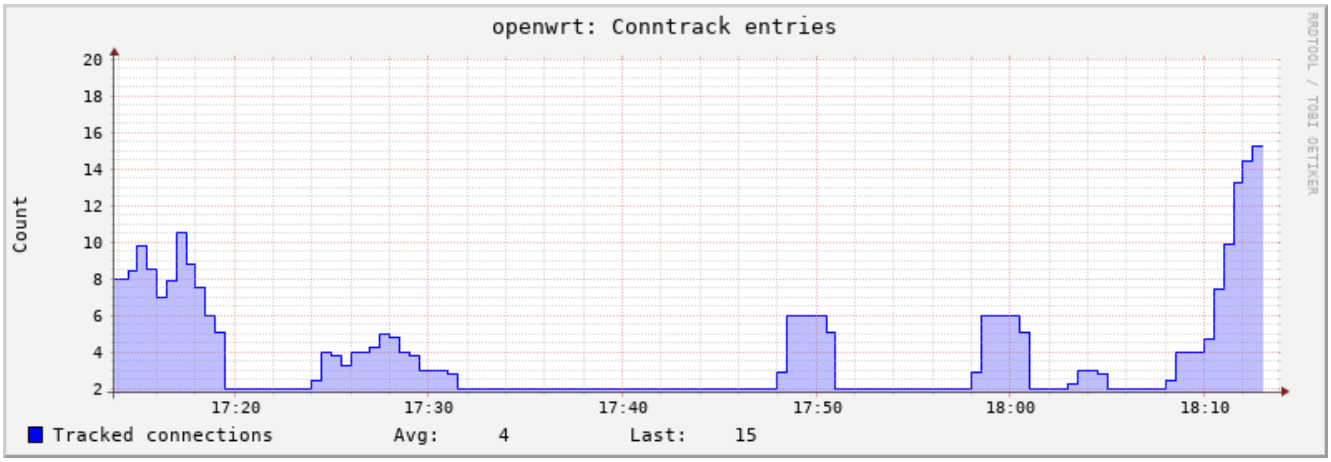


Рис. 8-14: Статистика. График отслеживаемых подключений (conntrack)

8.2.2.2 Интерфейсы

Плагин «Интерфейсы» собирает статистику выбранных сетевых интерфейсов.

Плагин имеет дополнительные настройки:

- «Мониторить интерфейсы» — список интерфейсов, для которых требуется собирать статистику.
- «Собирать статистику со всех кроме указанных» — если опция включена, то сбор статистики будет производиться только для интерфейсов, которые не указаны в списке «Мониторить интерфейсы».

Для каждого выбранного интерфейса строится два графика:

- количество принятых и отправленных данных (байт/с). Пример графика приведён на рисунке 8-15;
- количество принятых и отправленных пакетов, включая ошибки приёма и отправки (пакетов/с). Пример графика приведён на рисунке 8-16.

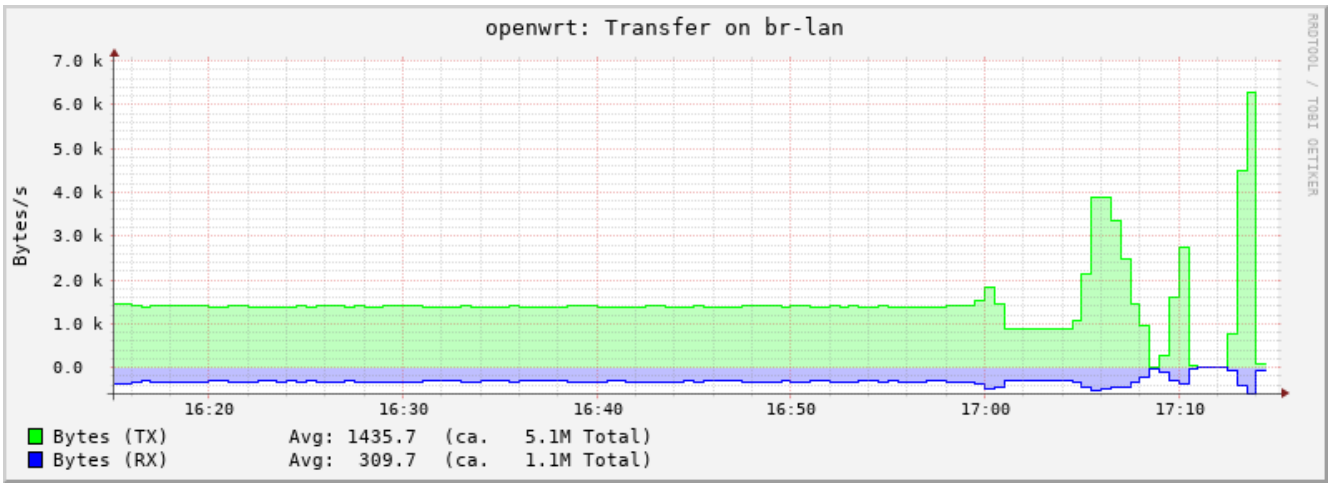


Рис. 8-15: Статистика. График приёма и отправки данных через сетевой интерфейс (байт/с)

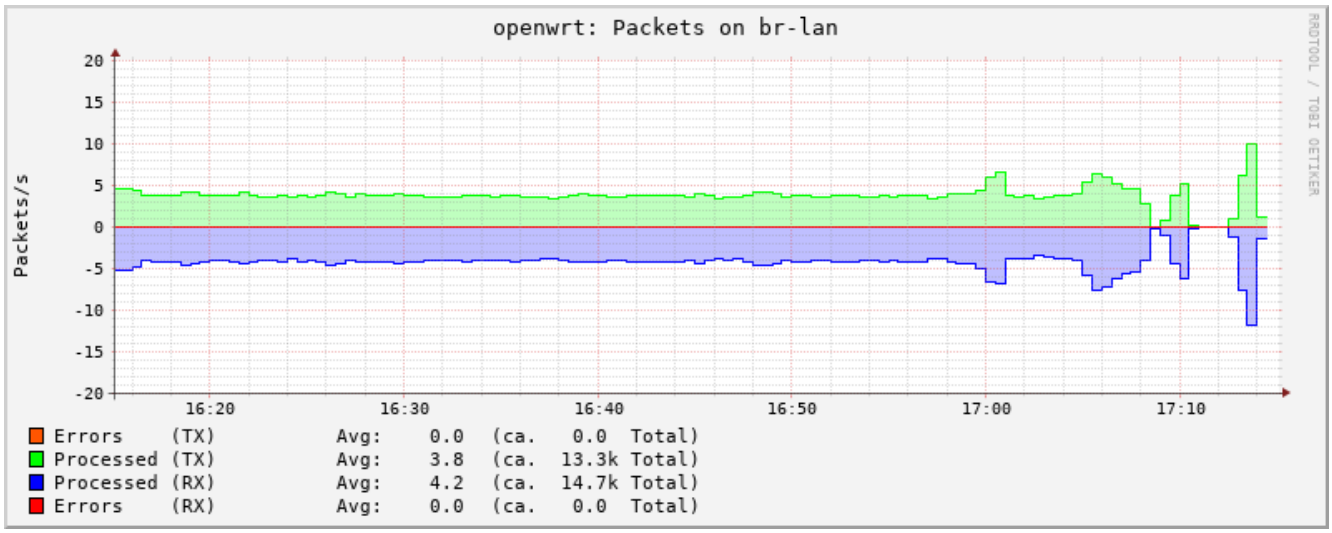


Рис. 8-16: Статистика. График приёма и отправки данных через сетевой интерфейс (пакетов/с)

8.2.2.3 Межсетевой экран

Плагин «Межсетевой экран» собирает статистику с определённых правил межсетевого экрана.

8.2.2.4 Пинг-запрос

Плагин «Пинг-запрос» посылает ICMP-запросы выбранным хостам и измеряет время отклика.

Плагин имеет дополнительные настройки:

- «Мониторить хосты» — список хостов (разделённых символом пробела), для которых требуется собирать статистику ICMP-запросов;
- «TTL для ping-пакетов» — значение TTL для пакетов ICMP-запросов;
- «Интервал для ping-запросов» — интервал (в секундах) отправки ICMP-запросов выбранным хостам.

Пример графика данных, полученных при помощи данного плагина, показан на рисунке 8-17.

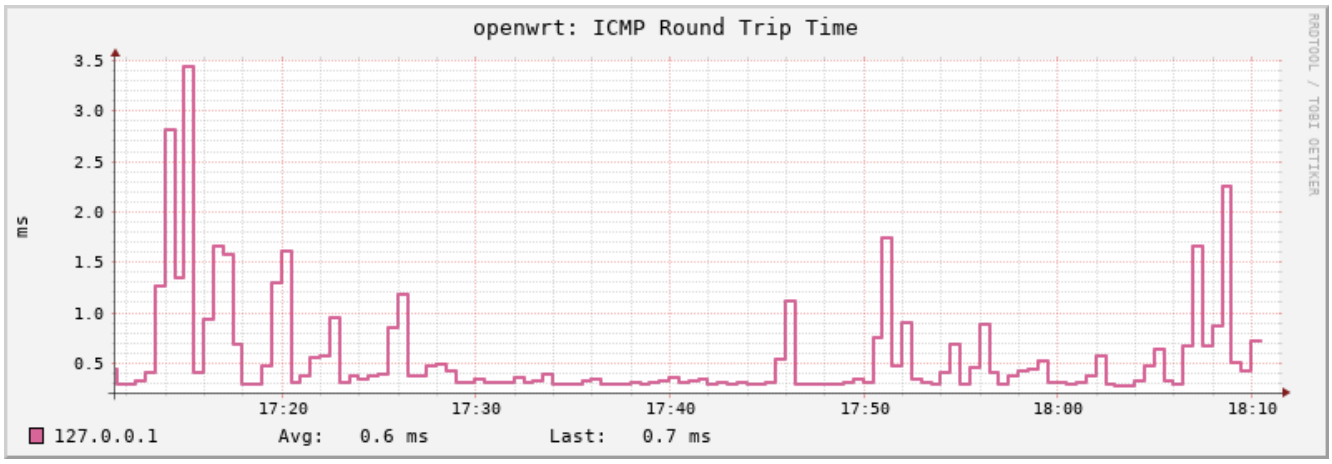


Рис. 8-17: Статистика. График времени отклика ICMP-запроса

8.2.2.5 TCPConns

Плагин «TCPConns» собирает информацию об открытых TCP соединениях на выбранных портах.

Плагин имеет дополнительные настройки:

- «Мониторить локальные порты» — список номеров портов (разделённых символом пробела), для которых требуется собирать статистику TCP соединений;

- «Собирать статистику со всех портов для входящих соединений» — при включении данной опции, статистика будет собираться со всех портов для входящих подключений;

Пример графика данных, полученных при помощи данного плагина, показан на рисунке 8-18.

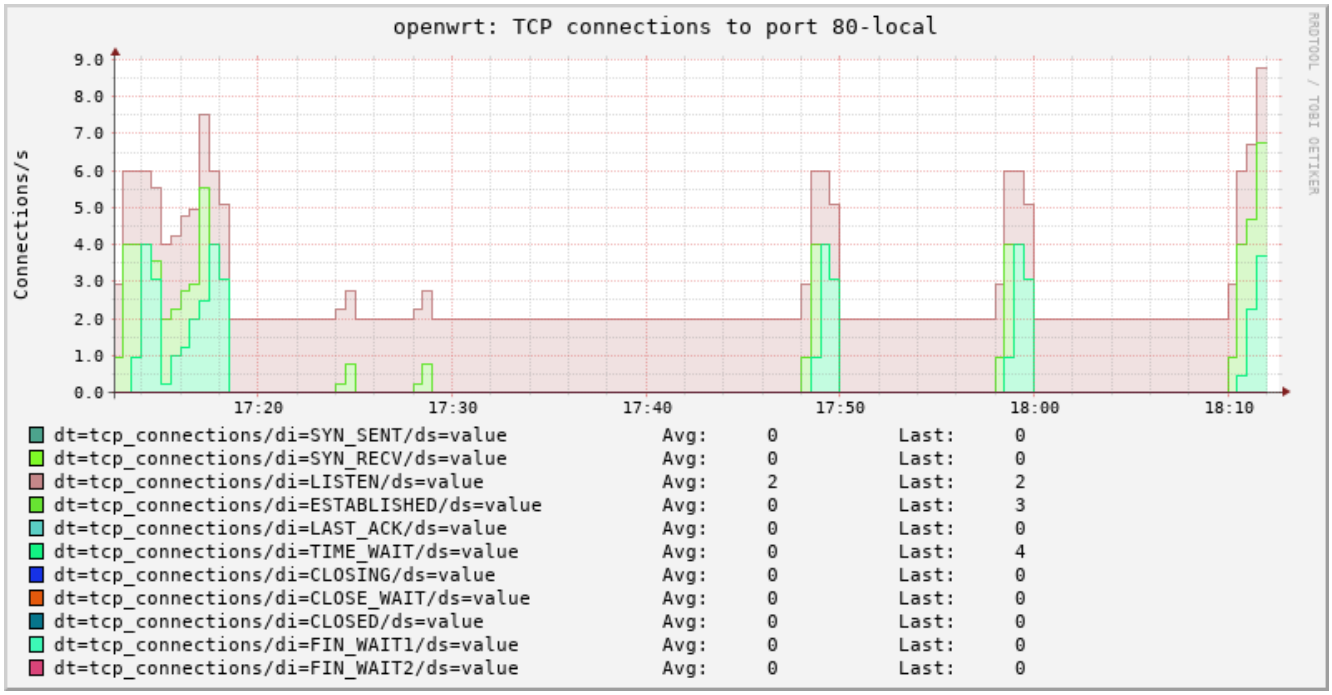


Рис. 8-18: Статистика. График открытых соединений для TCP порта

Приложение А Проверка доступа к консоли устройства ПЛК210 по протоколу SSH

Проверка доступа будет осуществляться с инструментального компьютера с установленной операционной системой Ubuntu 16.04.4 LTS при помощи утилит ssh, scp и sftp пакета OpenSSH версии 7.2.

К конфигурации инструментального компьютера, кроме наличия сетевой карты с поддержкой подключения на скорости 100 Мбит/с и полным дуплексом, дополнительных требований не предъявляется.

Предполагается, что для данной проверки ПЛК210 сконфигурирован с использованием мастера настройки (см. раздел 2) и при конфигурации была выбрана схема сетевых портов №1 (см. раздел 2.5). Мостовому LAN подключению ПЛК210 назначен статический IP-адрес 192.168.0.58 и маска подсети 255.255.255.0.

Инструментальному компьютеру назначен IP-адрес из той же подсети (255.255.255.0).

Вывод команды «`lsb_release -a`» на инструментальном компьютере выглядит следующим образом:

```
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.4 LTS
Release:        16.04
Codename:       xenial
```

Вывод команды «`apt-cache policy openssh-client`» на инструментальном компьютере выглядит следующим образом:

```
openssh-client:
  Installed: 1:7.2p2-4ubuntu2.4
  Candidate: 1:7.2p2-4ubuntu2.4
  Version table:
 *** 1:7.2p2-4ubuntu2.4 500
        500 http://ru.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages
        500 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages
        100 /var/lib/dpkg/status
     1:7.2p2-4 500
        500 http://ru.archive.ubuntu.com/ubuntu xenial/main amd64 Packages
```

Схема подключения инструментального компьютера и устройства ПЛК210 показана на рисунке А-1.

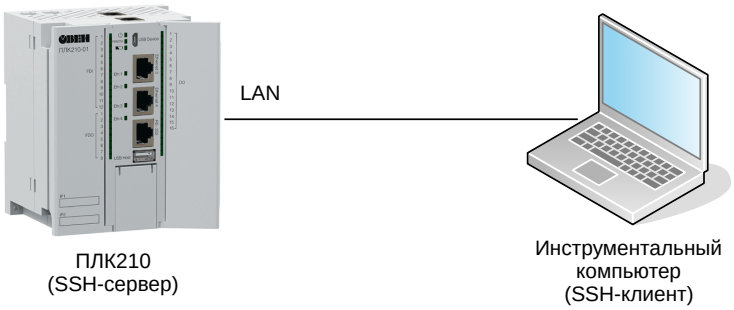


Рис. А-1: Схема подключения проверки доступа к консоли устройства ПЛК210 по протоколу SSH

Инструментальный компьютер подключён напрямую в любой из 3-х портов (порты Ethernet 1, 2 и 3) мостового LAN подключения при помощи стандартного 4-х парного UTP патч-корда категории 5е прямого обжима с коннекторами RJ-45 на обоих концах.

А.1 Доступ к консоли устройства при помощи утилиты ssh

Для доступа к консоли устройства ПЛК210 при помощи утилиты ssh на инструментальном компьютере необходимо выполнить в терминале команду:

```
ssh root@192.168.0.58
```

В том случае, если ранее не выполнялось подключение по SSH протоколу к данному устройству с данного инструментального компьютера, будет выведено сообщение о необходимости подтверждения получения и сохранения ключа с выводом отпечатка (fingerprint):

```
The authenticity of host '192.168.0.58 (192.168.0.58)' can't be established.
RSA key fingerprint is SHA256:r47nRb5cjz741ePHp7AVMsdL0ndGfZS7lsYA/hTOSN8.
Are you sure you want to continue connecting (yes/no)?
```

В случае возникновения подобного запроса, необходимо подтвердить получение ключа. Для этого необходимо ввести «yes».

Далее будет выведен запрос пароля для пользователя root на устройстве, к которому выполняется подключение:

```
root@192.168.0.58's password:
```

В случае ввода правильного пароля (по умолчанию установлен пароль «owen») будет выведено приглашение командной строки устройства ПЛК210 как показано на рисунке A-2.

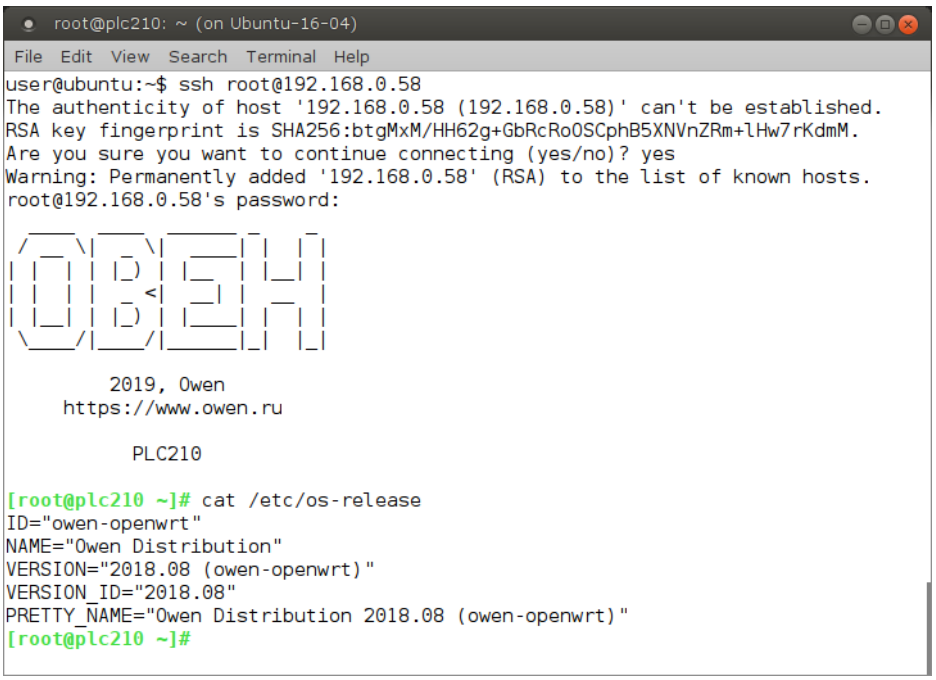


Рис. A-2: Доступ к консоли устройства ПЛК210 при помощи утилиты ssh

Для того чтобы убедится в том, что подключение выполнено именно к устройству ПЛК210, можно выполнить вывод содержимого файла «/etc/os-release», введя команду:

```
cat /etc/os-release
```

Пример вывода содержимого файла «/etc/os-release» также приведён на рисунке A-2.

A.2 Доступ к файловой системе устройства при помощи утилиты scp

В данной проверке выполняется копирование файла «/etc/os-release» с файловой системы удалённого устройства в домашнюю папку пользователя на инструментальном компьютере при помощи утилиты scp.

Для этого необходимо выполнить в терминале инструментального компьютера команду:

```
scp root@192.168.0.58:/etc/os-release ~/os-release
```

При подключении будет выведен запрос пароля для пользователя root на устройстве, к которому выполняется подключение:

```
root@192.168.0.58's password:
```

В случае ввода правильного пароля будет выведена информация о скопированной информации:

```
os-release                                    100%  539     0.5KB/s   00:00
```

После того, как файл был успешно скопирован в домашнюю папку пользователя на инструментальном компьютере, для его просмотра необходимо выполнить команду:

```
cat ~/os-release
```

Пример вывода данной команды приведён на рисунке А-3.

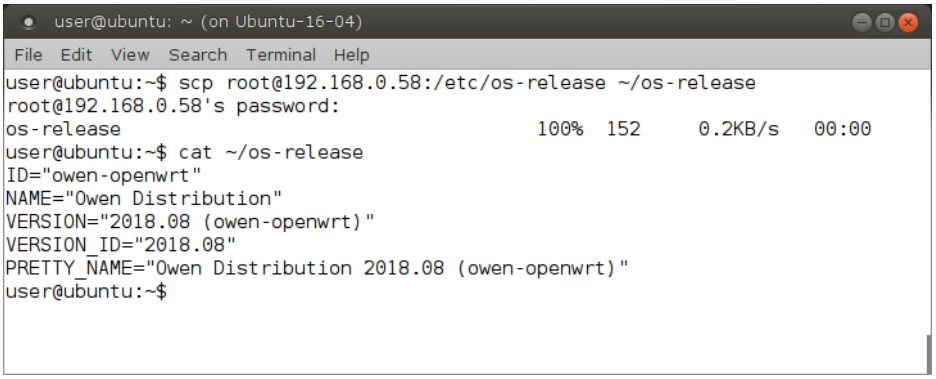


Рис. А-3: Доступ к файловой системе устройства ПЛК210 при помощи утилиты scp

А.3 Доступ к файловой системе устройства при помощи утилиты sftp

В данной проверке выполняется просмотр листинга корня удалённой файловой системы устройства при помощи утилиты sftp.

Для этого необходимо выполнить в терминале инструментального компьютера команду:

```
sftp root@192.168.0.58
```

При подключении будет выведен запрос пароля для пользователя root на устройстве, к которому выполняется подключение:

```
root@192.168.0.58's password:
```

В случае ввода правильного пароля будет выведена информация об успешном подключении и приглашение для ввода команд утилиты sftp:

```
Connected to 192.168.0.58.
sftp>
```

Для вывода листинга корня удалённой файловой системы необходимо выполнить команду:

```
ls -l /
```

Пример вывода данной команды приведён на рисунке А-4.

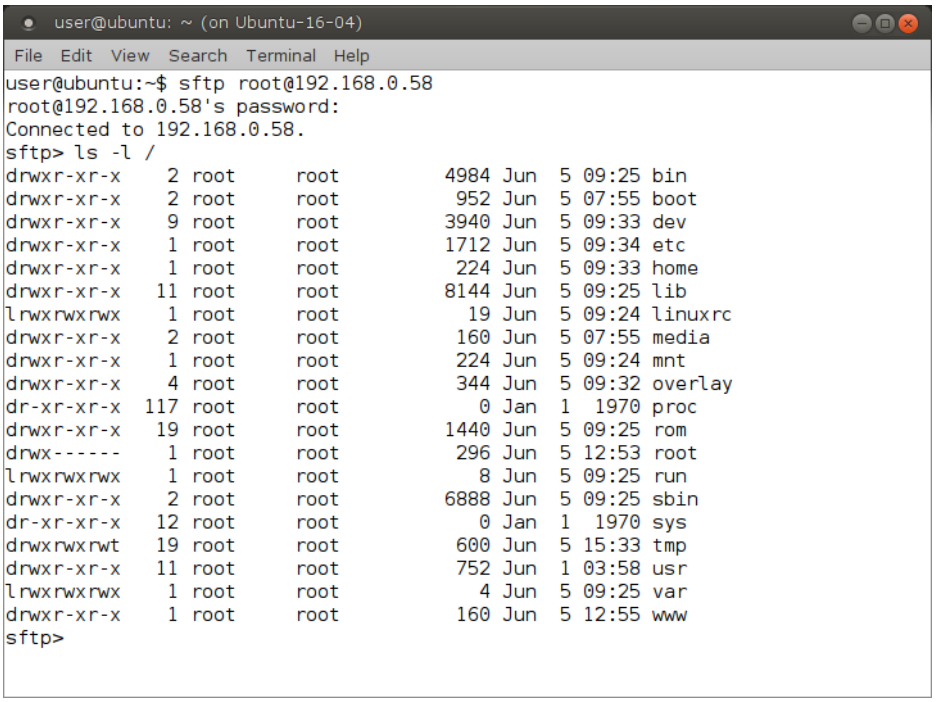


Рис. А-4: Доступ к файловой системе устройства ПЛК210 при помощи утилиты sftp

Приложение Б Проверка доступа к содержимому FTP-сервера на устройстве ПЛК210

Проверка доступа будет осуществляться с инструментального компьютера с установленной операционной системой Ubuntu 16.04.4 LTS при помощи утилиты ftp версии 0.17.

К конфигурации инструментального компьютера, кроме наличия сетевой карты с поддержкой подключения на скорости 100 Мбит/с и полным дуплексом, дополнительных требований не предъявляется.

Предполагается, что для данной проверки ПЛК210 сконфигурирован с использованием мастера настройки (см. раздел 2) и при конфигурации была выбрана схема сетевых портов №1 (см. раздел 2.5). Мостовому LAN подключению ПЛК210 назначен статический IP-адрес 192.168.0.58 и маска подсети 255.255.255.0.

Инструментальному компьютеру назначен IP-адрес из той же подсети (255.255.255.0).

Вывод команды «`lsb_release -a`» на инструментальном компьютере выглядит следующим образом:

```
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.4 LTS
Release:        16.04
Codename:       xenial
```

Вывод команды «`apt-cache policy ftp`» на инструментальном компьютере выглядит следующим образом:

```
ftp:
  Installed: 0.17-33
  Candidate: 0.17-33
  Version table:
 *** 0.17-33 500
        500 http://ru.archive.ubuntu.com/ubuntu xenial/main amd64 Packages
        100 /var/lib/dpkg/status
```

Схема подключения инструментального компьютера и устройства ПЛК210 показана на рисунке Б-1.

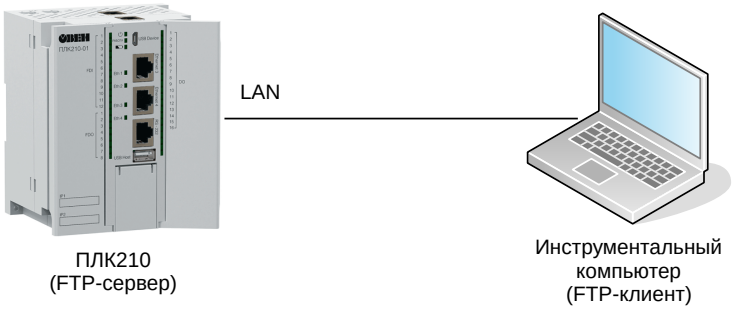


Рис. Б-1: Схема подключения проверки доступа к содержимому FTP-сервера устройства ПЛК210

Инструментальный компьютер подключён напрямую в любой из 3-х портов (порты Ethernet 1, 2 и 3) мостового LAN подключения при помощи стандартного 4-х парного UTP патч-корда категории 5e прямого обжима с коннекторами RJ-45 на обоих концах.

Б.1 Подготовка

Для тестирования передачи файлов по протоколу FTP необходимо подготовить файл с тестовыми данными. Для этого, на инструментальном компьютере выполним команду:

```
# dd if=/dev/urandom of=/tmp/data.bin bs=1024 count=1024
1024+0 records in
1024+0 records out
1048576 bytes (1,0 MB, 1,0 MiB) copied, 0,00610422 s, 172 MB/s
```

Данная команда создаст файл «/tmp/data.bin» размером 1 МиБ (1048576 байт) со случайными данными.

Подсчитаем и запомним контрольную сумму (MD5) данных этого файла:

```
# md5sum /tmp/data.bin
25853ed8e4d3518e72f310feb0f86c4d  /tmp/data.bin
```

Далее, это значение будет использоваться для проверки корректности передачи данных по протоколу FTP.

Контрольная сумма для каждого вновь сгенерированного файла данных будет отличаться от приведённой в данном документе.

Б.2 Подключение к FTP-серверу

На инструментальном компьютере, для запуска FTP-клиента, необходимо выполнить в терминале команду:

```
# ftp 192.168.0.58
```

Будет отображено сообщение об успешном подключении и запрос имени пользователя:

```
Connected to 192.168.0.58.
220 (vsFTPd 3.0.3)
Name (192.168.0.58:user): ftp
```

Необходимо ввести имя пользователя «ftp», после чего последует запрос пароля:

```
331 Please specify the password.
Password:
```

Если в мастере настройки пароль доступа к FTP не менялся (раздел 2.8), то пароль по умолчанию установлен в значение «ftp». В противном случае следует ввести установленный пароль. В случае ввода правильного пароля, будет отображено сообщение об успешной авторизации и приглашение для ввода команд:

```
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Б.3 Загрузка (upload) файла на FTP-сервер

Подготовьте файл данных согласно инструкции, приведённой в разделе Б.1, затем выполните подключение к устройству ПЛК210 согласно инструкции, приведённой в разделе Б.2.

В FTP-клиенте выполните команду:

```
ftp> put /tmp/data.bin data.bin
```

где:

- `/tmp/data.bin` — путь к передаваемому файлу на локальной файловой системе (инструментальный компьютер);
- `data.bin` — путь к файлу на FTP-сервере относительно корня FTP-сервера (ПЛК210).

В случае успешной передачи файла на FTP-сервер будут отображены следующие сообщения:

```
local: /tmp/data.bin remote: data.bin
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
1048576 bytes sent in 0.09 secs (11.6982 MB/s)
```

Таким образом, переданный файл должен быть сохранен в корневой папке FTP-сервера под именем «data.bin». Так как по умолчанию корнем FTP-сервера является папка «/mnt/ufs/home/ftp», то полный путь к файлу на файловой системе устройства ПЛК210 будет «/mnt/ufs/home/ftp/data.bin». Контрольная сумма данного файла должна совпадать с контрольной суммой исходного сгенерированного файла (см. раздел Б.1):

```
[root@plc210 ~]# md5sum /mnt/ufs/home/ftp/data.bin
25853ed8e4d3518e72f310feb0f86c4d  /mnt/ufs/home/ftp/data.bin
```

Б.4 Скачивание (download) файла с FTP-сервера

Выполним скачивание файла с данными с FTP-сервера, который был туда загружен в разделе Б.3.

В FTP-клиенте выполните команду:

```
ftp> get data.bin /tmp/data-received.bin
```

где:

- `data.bin` — путь к файлу на FTP-сервере относительно корня FTP-сервера (ПЛК210);
- `/tmp/data-received.bin` путь к скачиваемому файлу на локальной файловой системе (инструментальный компьютер).

```
local: /tmp/data-received.bin remote: data.bin
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for data.bin (1048576 bytes).
226 Transfer complete.
1048576 bytes received in 0.17 secs (5.7856 MB/s)
```

Таким образом, скачанные данные будут сохранены в файле «/tmp/data-received.bin». Контрольные суммы исходного сгенерированного файла «/tmp/data.bin» и скачанного файла «/tmp/data-received.bin» должны совпадать:

```
# md5sum /tmp/data.bin /tmp/data-received.bin
25853ed8e4d3518e72f310feb0f86c4d  /tmp/data.bin
25853ed8e4d3518e72f310feb0f86c4d  /tmp/data-received.bin
```

Приложение В Пример настройки службы DDNS для провайдера no-ip.com

B.1 Регистрация домена в панели управления DDNS провайдера

B.1.1 Перейдите на сайт DDNS провайдера no-ip.com по ссылке https://noip.com и выполните вход с систему с использованием логина и пароля.

В данном документе не рассматривается вопрос создания и настройки учётной записи DDNS провайдера no-ip.com. Данную информацию можно найти по адресу https://www.noip.com/support/

B.1.2 Перейдите в меню «Dynamic DNS» (см. рисунок B-1).

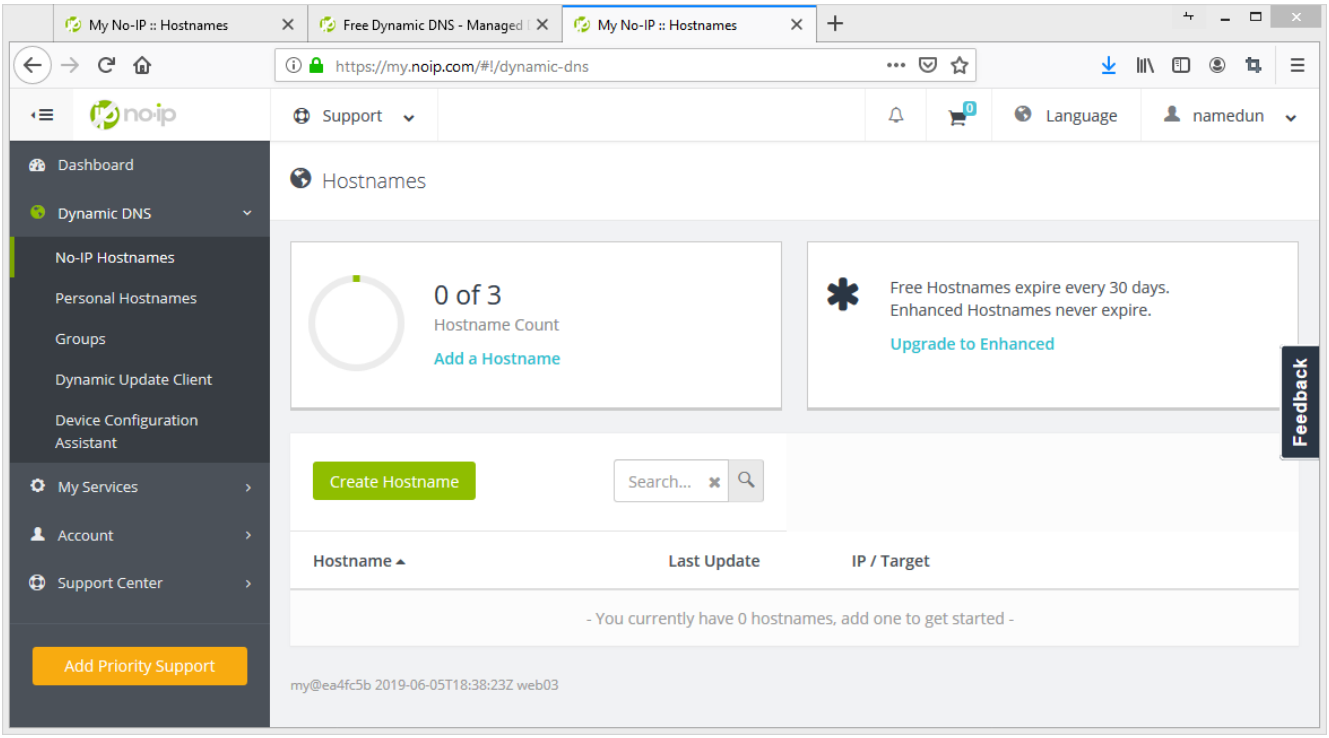


Рис. B-1: Раздел «Dynamic DNS» панели управления DDNS провайдера no-ip.com

B.1.3 Нажмите кнопку «Create Hostname». В открывшемся окне (см. рисунок B-2) выберите произвольное имя домена (в данном примере выбрано имя myplctest.ddns.net).

B.1.4 Введите любой произвольный IPv4-адрес для данного домена (в данном примере домену был присвоен адрес 8.8.8.8). Необходимо ввести заведомо неверный IPv4-адрес с целью последующей проверки обновления адреса с устройства ПЛК210.

B.1.5 Нажмите кнопку «Create Hostname». В разделе «Hostnames» страницы «Dynamic DNS» будет отображён вновь созданный домен, как показано на рисунке B-3.

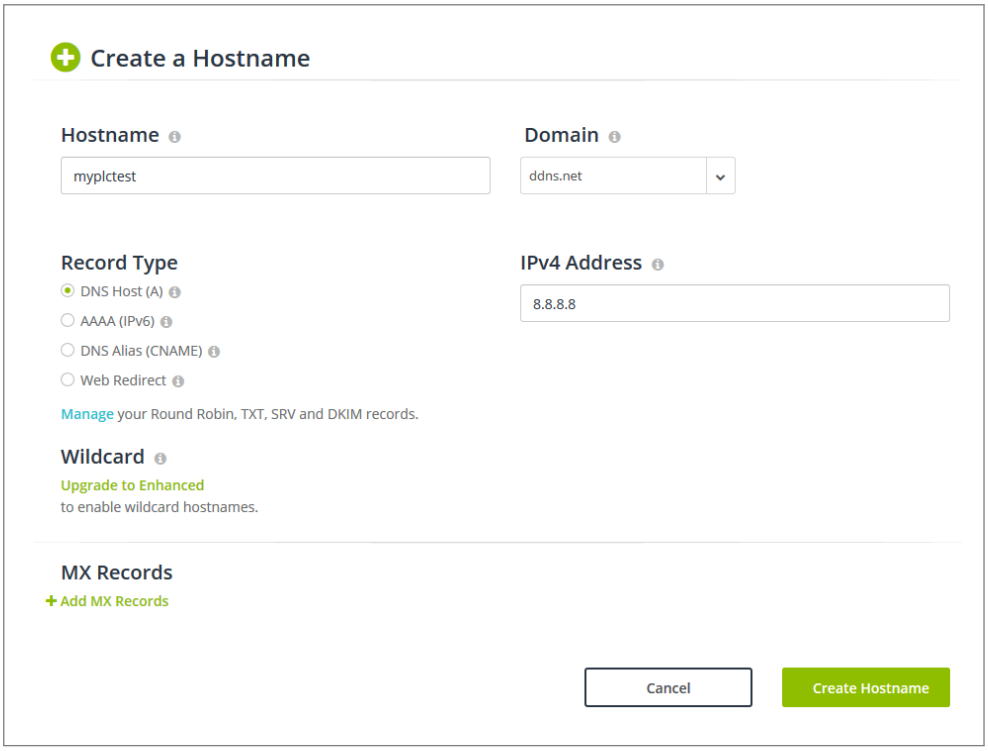


Рис. B-2: Создание Hostname в панели управления DDNS провайдера no-ip.com

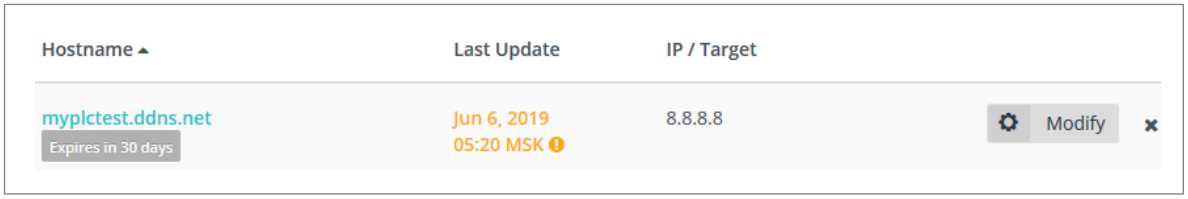


Рис. B-3: Таблица «Hostnames» в панели управления DDNS провайдера no-ip.com

B.2 Настройка службы DDNS на ПЛК210

B.2.1 Перейдите в веб-интерфейс управления ПЛК210 и выполните вход в систему.

B.2.2 Перейдите на страницу «DDNS» раздела «Службы» главного меню.

B.2.3 На странице «DDNS» введите имя новой DDNS записи (в данном примере «myplctest») в текстовое поле слева от кнопки «Добавить» и нажмите кнопку «Добавить» (см. рисунок B-4).

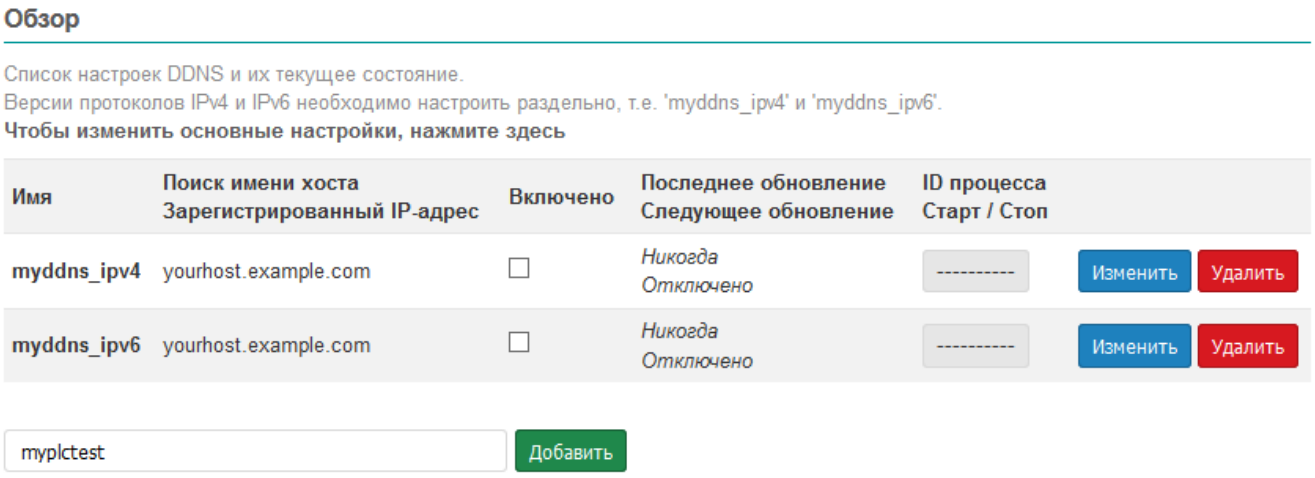


Рис. B-4: Добавление новой DDNS записи

B.2.4 На открывшейся странице редактирования настроек новой DDNS записи, на вкладке «Основные настройки», в выпадающем списке «Провайдер службы DDNS» выберите пункт «no-ip.com» и нажмите кнопку «Сменить провайдера» (см. рисунок B-5).

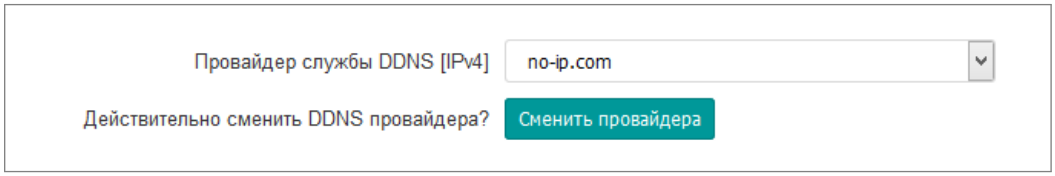


Рис. B-5: Редактирование новой DDNS записи. Выбор DDNS провайдера

На вкладке «Основные настройки» установите следующие настройки (см. рисунок B-6):

- «Включено» — да;
- «Поиск имени хоста» — выбранное имя домена (в данном примере — myplctest.ddns.net);
- «Домен» — выбранное имя домена (в данном примере myplctest.ddns.net);
- «Имя пользователя» — имя пользователя учётной записи DDNS провайдера no-ip.com;
- «Пароль» — пароль учётной записи DDNS провайдера no-ip.com;
- «Использовать HTTPS» — да;
- «Путь к CA-сертификату» — /etc/ssl/certs.

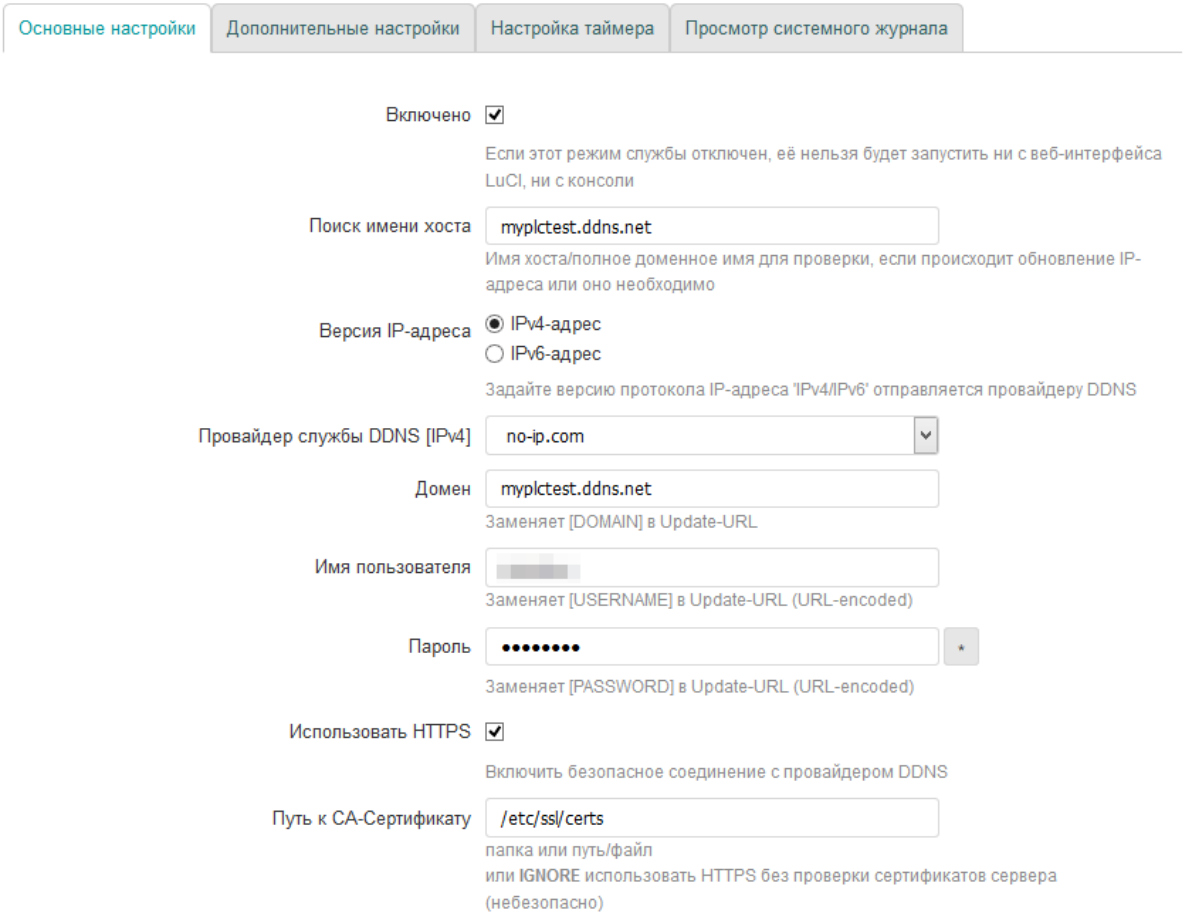


Рис. B-6: Основные настройки новой DDNS записи

B.2.5 На вкладке «Дополнительные настройки» установите следующие настройки:

- «IP-адрес источника» — URL;
- «URL для обнаружения» — http://checkip.dyndns.com;

Все прочие настройки следует оставить со значениями по умолчанию.

В.2.6 Нажмите кнопку «Сохранить и применить». На основной странице «DDNS» в таблице DDNS записей должна отображаться новая DDNS запись, как показано на рисунке В-7.

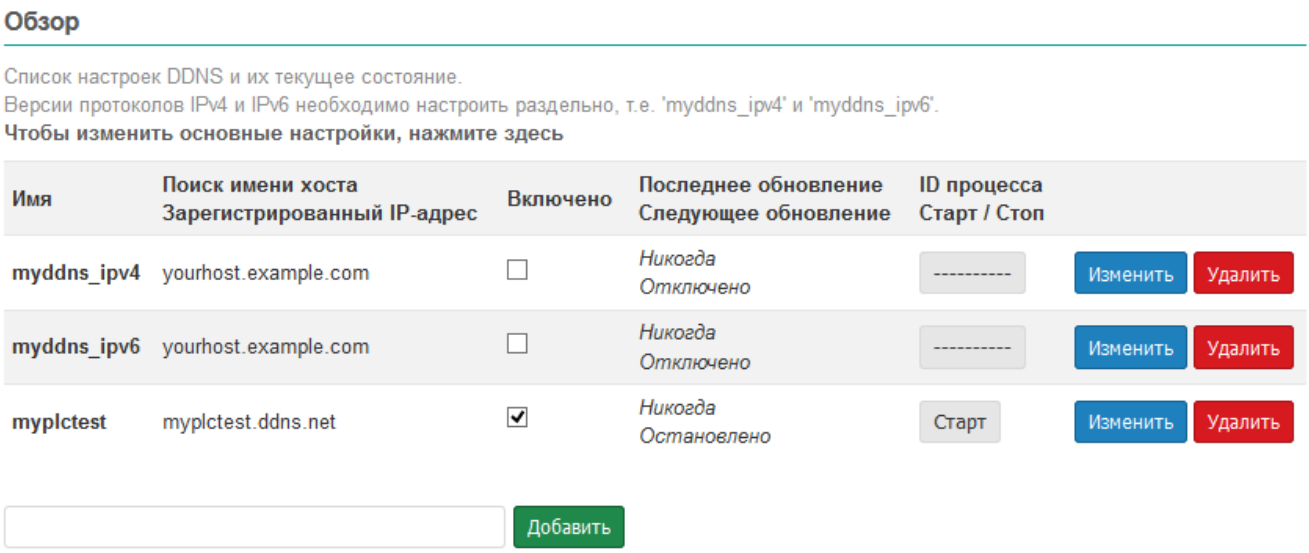


Рис. В-7: Созданная DDNS запись

В.2.7 Нажмите кнопку «Старт» и подождите некоторое время (не более 1 минуты). Строка DDNS записи в таблице должна измениться, как показано на рисунке В-8.

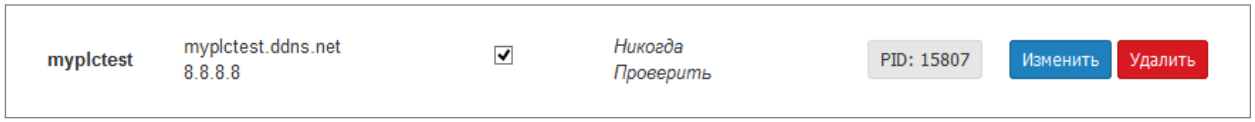
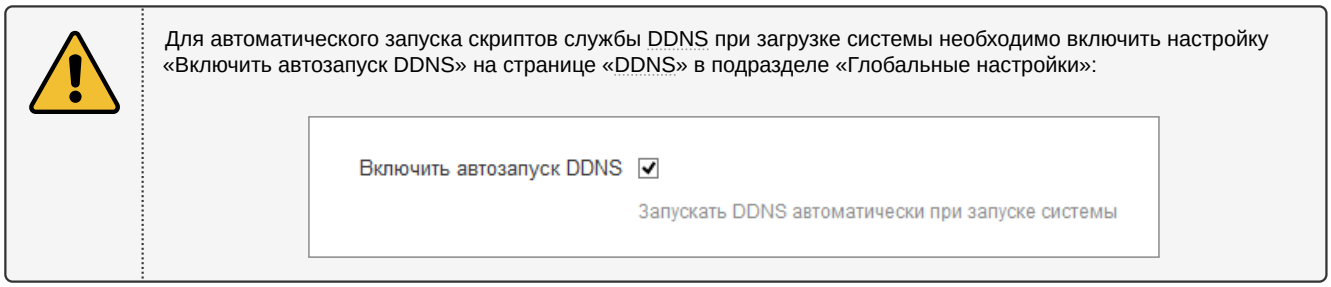


Рис. В-8: Созданная DDNS запись с запущенным скриптом



Как видно на рисунке В-8, при последней проверке был определён IP-адрес 8.8.8.8 (именно этот адрес указывался при регистрации домена в панели управления DDNS провайдера) для домена myplctest.ddns.net.

В настройках DDNS записи для определения IP-адреса был указан URL http://checkip.dyndns.com. В результате, при выполнении скрипта для DDNS записи полученный текущий адрес для домена (8.8.8.8) и адрес, определённый страницей http://checkip.dyndns.com были проверены, и так как они не совпадают, провайдеру DDNS была отправлена информация с новым IP-адресом, который был возвращён страницей http://checkip.dyndns.com.

В таблице DDNS записей на странице «DDNS» новый IP-адрес будет отображён (см. рисунок В-9) только при выполнении следующей плановой проверки (по умолчанию, проверка выполняется раз в 10 минут).

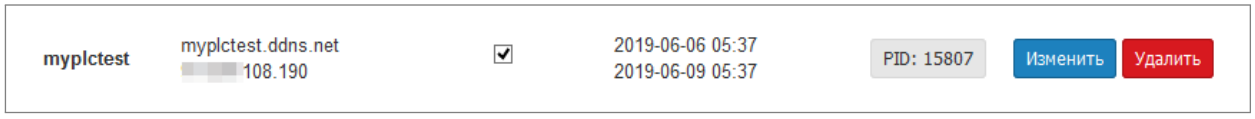


Рис. В-9: Созданная DDNS запись с обновлённым IP-адресом

B.3 Дополнительные проверки

B.3.1 Проверить правильность обновления IP-адреса для домена DDNS записи можно следующими дополнительными способами:

1) В системном журнале DDNS записи на устройстве ПЛК210 (см. раздел 6.1.1.4) должны присутствовать записи, подобные приведённым:

```
 053637  info : Starting main loop at 2019-06-06 05:36
 053639       : Detect local IP on 'web'
 053640       : #> /usr/bin/curl -RsS -o /var/run/ddns/myplctest.dat --stderr /var/run/ddns/myplctest.
    ← err --capath /etc/ssl/certs --noproxy '*' 'http://checkip.dyndns.com'
 053645       : Local IP 'XXX.XXX.108.190' detected on web at 'http://checkip.dyndns.com'
 053647       : Update needed - L: 'XXX.XXX.108.190' <> R: '8.8.8.8'
 053649       : parsing script '/usr/lib/ddns/update_no-ip_com.sh'
 053650       : sending dummy IP to 'no-ip.com'
 053652       : #> /usr/bin/curl -RsS -o /var/run/ddns/myplctest.dat --stderr /var/run/ddns/myplctest.
    ← err --capath /etc/ssl/certs --noproxy '*' 'https://***USERNAME***:***PW***@dynupdate.no-ip.com/
    ← nic/update?hostname=myplctest.ddns.net&myip=127.0.0.1'
 053659       : 'no-ip.com' answered:
good 127.0.0.1
 053702       : sending real IP to 'no-ip.com'
 053703       : #> /usr/bin/curl -RsS -o /var/run/ddns/myplctest.dat --stderr /var/run/ddns/myplctest.
    ← err --capath /etc/ssl/certs --noproxy '*' 'https://***USERNAME***:***PW***@dynupdate.no-ip.com/
    ← nic/update?hostname=myplctest.ddns.net&myip=XXX.XXX.108.190'
 053710       : 'no-ip.com' answered:
good XXX.XXX.108.190
 053712  info : Update successful - IP 'XXX.XXX.108.190' send
 053713  info : Forced update successful - IP: 'XXX.XXX.108.190' send
 053715       : Waiting 600 seconds (Check Interval)
```

В листинге реальный публичный IP-адрес заменён на `XXX.XXX.108.190`.

2) В панели управления DDNS провайдера должен отображаться обновлённый IP-адрес, как показано на рисунке B-10.

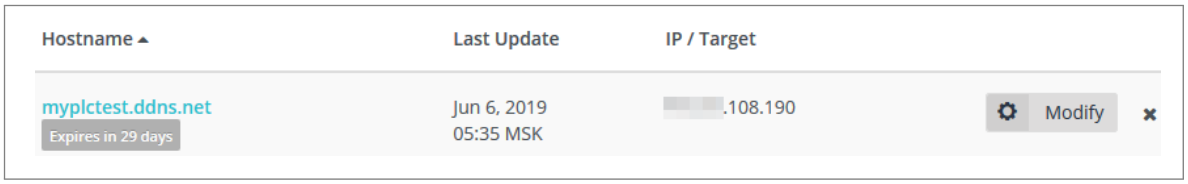


Рис. B-10: Таблица «Hostnames» с обновлённым IP-адресом домена в панели управления DDNS провайдера no-ip.com

3) DNS запрос с любого компьютера должен вернуть новый обновлённый IP-адрес:

```
# nslookup myplctest.ddns.net
Server:     127.0.1.1
Address:    127.0.1.1#53

Non-authoritative answer:
Name:   myplctest.ddns.net
Address: XXX.XXX.108.190
```

В листинге реальный публичный IP-адрес заменён на XXX.XXX.108.190.

Список литературы

1. Формирование системного решения по применению технологии управления топологией связей в сети Ethernet на базе протоколов STP/RSTP для устройства ПЛК210. Справочное руководство. TN-RG-KSZ8895-RSTP. ОВЕН (цит. на с. 22, 89).
2. Использование устройства ПЛК210 в сетях Ethernet с поддержкой протоколов STP/RSTP. Руководство пользователя. TN-UG-KSZ8895-RSTP. ОВЕН (цит. на с. 22, 89).
3. Load Average. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Load_Average (цит. на с. 29, 37, 144).
4. Netfilter. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Netfilter (цит. на с. 33).
5. Iptables. Викиучебник. Открытые книги для открытого мира. URL: https://ru.wikibooks.org/wiki/Iptables (цит. на с. 33, 138).
6. sched — overview of CPU scheduling. Linux man page. URL: http://man7.org/linux/man-pages/man7/sched.7.html (цит. на с. 48).
7. mount — mount a filesystem. Linux man page. URL: http://man7.org/linux/man-pages/man8/mount.8.html (цит. на с. 51, 53).
8. Bell character. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Bell_character (цит. на с. 62).
9. CSV. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/CSV (цит. на с. 77).
10. Y. Rekhter и др. Address Allocation for Private Internets. RFC 1918 (Best Current Practice). Updated by RFC 6761. Internet Engineering Task Force, февр. 1996. URL: http://www.ietf.org/rfc/rfc1918.txt (цит. на с. 97, 119).
11. Сетевой мост. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BC%D0%BE%D1%81%D1%82 (цит. на с. 108).
12. Spanning Tree Protocol. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/STP (цит. на с. 108).
13. IGMP snooping. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/IGMP_snooping (цит. на с. 108).
14. BOOTP / DHCP options. RFC Sourcebook. URL: http://www.networksorcery.com/enp/protocol/bootp/options.htm (цит. на с. 113).
15. DNS rebinding. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/DNS_rebinding (цит. на с. 119).
16. resolv.conf — resolver configuration file. Linux man page. URL: http://man7.org/linux/man-pages/man5/resolv.conf.5.html (цит. на с. 121).
17. hosts — static table lookup for hostnames. Linux man page. URL: http://man7.org/linux/man-pages/man5/hosts.5.html (цит. на с. 121).
18. ethers — Ethernet address to IP number database. Linux man page. URL: http://man7.org/linux/man-pages/man5/ethers.5.html (цит. на с. 121).
19. SYN-flood. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/SYN-%D1%84%D0%BB%D1%83%D0%B4 (цит. на с. 127).
20. NAT loopback. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/NAT#NAT_loopback (цит. на с. 133).
21. collectd – The system statistics collection daemon. Official site. URL: https://collectd.org/ (цит. на с. 141).
22. types.db - Data-set specifications for the system statistics collection daemon collectd. Official site. URL: https://collectd.org/documentation/manpages/types.db.5.shtml (цит. на с. 142).

История редакций

Редакция	Дата	Изменения
2.2.0	05.05.2020	Текст документа адаптирован для применения на устройствах ПЛК200, ПЛК210 и СПК1xx. В раздел 2 добавлена информация о схемах сетевых портов для ПЛК200. Добавлен рисунок 2-8. В раздел 5 добавлено описание кнопок «Загрузить...», «Очистить retain память...», «Перезапустить CODESYS» и «Удалить проект». Заменены рисунки 5-22, 5-3 и 5-4. В раздел 7.1.2 добавлен подраздел 7.1.2.3 с описанием протокола «WireGuard VPN». Добавлены рисунки 7-16, 7-17 и 7-18. Заменен рисунок 7-5.
2.1.6	10.12.2019	Исправлен раздел 7.1.2. Заменены рисунки 5-22 и 7-5.
2.1.5	11.10.2019	Обновлён текст раздела 4.7. Заменены рисунки 4-20 и 4-21.
2.1.4	01.10.2019	Добавлена информация по генерации SSL сертификата для веб визуализации CODESYS (разделы 5.2.1 и 5.2.2). Заменены рисунки 5-3 и 5-22.
2.1.3	25.07.2019	Добавлен раздел 4.3.4 с описанием настроек последовательного порта RS232. Заменены рисунки 4-7, 4-8 и 4-9 В настройках FTP (раздел 6.4.1) опция «Порт FTP» переименована в «Порт для входящих соединений». Заменены рисунки 6-30 и 6-31. Документация приведена в соответствие с прошивкой 1.0.0725.1525.
2.1.2	02.07.2019	Исправлены опечатки. Заменены рисунки 6-18 и 6-19.
2.1.1	01.07.2019	Исправлены опечатки. Документация приведена в соответствие с прошивкой 1.0.0624.1806. Добавлено описание режимов автоконфигурации DHCPv6 (раздел 7.1.2.2.1). Добавлено описание параметров моста «Порт последнего изменения топологии» и «Количество изменений топологии» в раздел 6.2.1. Заменены рисунки 1-1, 7-35 и 7-36.
2.1.0	09.06.2019	Добавлено описание дополнительных разделов. Документация приведена в соответствие с прошивкой 1.0.0605.1931.
2.0	25.11.2018	Использование скриншотов с темой оформления ОВЕН.
1.0	30.10.2018	Начальная редакция.