Краткое описание основных функций Web-интерфейса управления контроллеров ПЛК2xx и СПК1xx

Руководство пользователя

Редакция 3.1.0 Draft

Код документа: TN-UG-OWRT-LUCI-R3
Дата сборки: 21 марта 2021 г.
Страниц в документе: 227

http://owen.ua

Документ выполнен в системе разработки документации TanoDoc 0.9.1-26

Содержание

Список иллюстраций

Перечень сокращений и условных обозначений

ARP	Address Resolution Protocol	52
ASCII	American Standard Code for Information Interchange	84, 149, 150
BPDU	Bridge Protocol Data Unit	127, 129, 132, 133
CA	Certification Authority	118, 216
CPU	Central Processing Unit	11, 201
CSV	Comma-Separated Values	56, 110
DDNS	Dynamic DNS	3, 5, 8, 9, 11, 14, 113–124, 214–218
DHCP	Dynamic Host Configuration Protocol	4, 10, 14, 23, 24, 30, 31, 50, 62, 155, 158–161, 166, 168, 170, 171
DNS	Domain Name System	3, 5, 12, 14, 31, 113, 115, 121, 158, 161, 166, 168, 170, 194, 196, 218
F2FS	Flash-Friendly File System	70
FAT	File Allocation Table	12, 13
FAT32	File Allocation Table 32	73
FIFO	First In First Out	67
FQDN	Fully Qualified Domain Name	198
FTP	File Transfer Protocol	2, 4–6, 11, 14, 17, 41–43, 147–150, 211–213, 227
HTTP	HyperText Transfer Protocol	14, 15, 42, 43, 89, 145, 146
HTTPS	HyperText Transfer Protocol Secure	15, 42, 43, 89, 118, 119, 145, 146, 179, 216
ICMP	Internet Control Message Protocol	11, 100, 181, 185, 187, 190, 205
IGMP	Internet Group Management Protocol	156, 185
IP	Internet Protocol	5, 8, 9, 11, 24, 30, 31, 34–37, 52, 59, 81, 100, 101, 104, 105, 107, 113, 115, 116, 118–122, 145, 147, 158, 161–163, 168, 170–172, 176, 178, 181, 182, 186, 187, 189, 190, 194, 196, 207, 211, 216–218, 224
IPv4	Internet Protocol version 4	31, 50, 52, 115, 121, 153, 158, 160, 173, 178, 187, 194, 195, 214
IPv6	Internet Protocol version 6	10, 52, 115, 121, 152, 153, 155, 158, 159, 161, 173, 178, 187, 194, 195
JSON	Java Script Object Notation	56
LAN	Local Area Network	24–27, 29–31, 207, 211
MAC	Media Access Control	48, 50, 52, 126, 127, 153, 158, 159, 182, 187
MMC	MultiMedia Card	71
MSS	Maximum Segment Size	177
MTU	Maximum Transmission Unit	158, 159
NAT	Network Address Translation	5, 10, 163, 175, 182, 189–192
NDP	Neighbor Discovery Protocol	161

NTFS	New Technology File System	73
NTP	Network Time Protocol	14, 17, 22, 23, 61, 62
OPC	Open Platform Communications	13
OPC UA	OPC Unified Architecture	42, 43
PID	Process IDentifier	116, 136, 198
PPP	Point-to-Point Protocol	48
RA	Router Advertisement	161
RNDIS	Remote Network Driver Interface Specification	32, 48, 95
RSS	Resident Set Size	11, 201, 202
RSTP	Rapid Spanning Tree Protocol	9, 14, 31, 125–128, 130–132, 156, 227
SFTP	SSH File Transfer Protocol	63
SSH	Secure SHell	2, 3, 5–7, 11, 13, 14, 17, 35, 39, 40, 42, 43, 63–65, 101, 103, 207, 208, 227
SSL	Secure Sockets Layer	3, 7, 8, 82, 84, 85, 89–92
STP	Spanning Tree Protocol	9, 14, 31, 125–128, 130–132, 156, 227
TCN	Topology Change Notification	129, 133
TCP	Transmission Control Protocol	11, 39, 42, 43, 53, 59, 63, 64, 84, 89, 121, 179, 181, 182, 185, 186, 190, 205, 206, 219
TTL	Time To Live	205
UDP	User Datagram Protocol	42, 53, 59, 121, 162, 170, 181, 182, 185, 186, 190, 219
ULA	Unique Local Address	152
URL	Uniform Resource Locator	116, 118, 120, 216, 217
USB	Universal Serial Bus	6, 32, 45, 46, 48, 71, 95
UTC	Universal Time Coordinated	188, 191
UTP	Unshielded Twisted Pair	207, 211
UUID	Universally Unique IDentifier	71
VFAT	Virtual File Allocation Table	70, 73
VPN	Virtual Private Network	11, 48, 138, 219, 220, 222
VSZ	Virtual Set siZe	11, 201, 203
WAN	Wide Area Network	24–27, 30, 31, 42
ПЛК	Программируемый Логический Контроллер	34, 35, 37, 40, 88

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 TanoWrt[1].

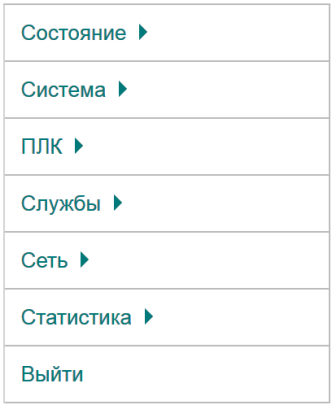


Рис. 1-1: Главное меню Web-интерфейса управления LuCI

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 3.5.2), журнала ядра (раздел 3.5.1), и страницы для просмотра графиков в реальном времени для некоторых системных параметров (раздел 3.4).

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 5.6) 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://github.com/tano-systems/meta-tanowrt

1.1 Поддерживаемые контроллеры

В данном руководстве описан веб-интерфейс управления следующими контроллерами производства компании ОВЕН:

- ПЛК200 — контроллер для средних и малых систем автоматизации;
- ПЛК210 — контроллер для средних и распределённых систем автоматизации;
- СПК107 — контроллер с сенсорным экраном 7” для локальных систем;
- СПК110 — контроллер с сенсорным экраном 10.2” для локальных систем.

1.2 Поддерживаемые браузеры

Веб-интерфейс управления LuCI рассчитан на работу со следующими браузерами:

- Google Chrome (версия 85.0.4183.102 или выше);
- Mozilla Firefox (версия 80.0.1 или выше);
- Opera (версия 70.0.3728.178 или выше);
- Microsoft Edge (версия 87.0.664.66 или выше);
- Microsoft Internet Explorer (версия 11.0.9600.18817 или выше).

Работа веб-интерфейса на других браузерах (или на перечисленных, но с более низкими версиями) возможна, но полная функциональность не гарантируется.

Веб-интерфейс управления контроллерами имеет адаптивный интерфейс и поддерживает работу на мобильных устройствах (мобильные телефоны, планшеты) с разрешением экрана не менее 400 x 600 точек. Мобильная версия веб-интерфейса отличается от настольной лишь расположением и размером некоторых элементов. В связи с этим мобильная версия веб-интерфейса в документе отдельно не рассматривается, а описана только работа с веб-интерфейсом через браузер с использованием обычного настольного персонального компьютера.

Все представленные в данном документе скриншоты веб-интерфейса выполнены с использованием браузера Mozilla Firefox, запущенного в операционной системе Microsoft Windows 10 (x64).

1.3 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.

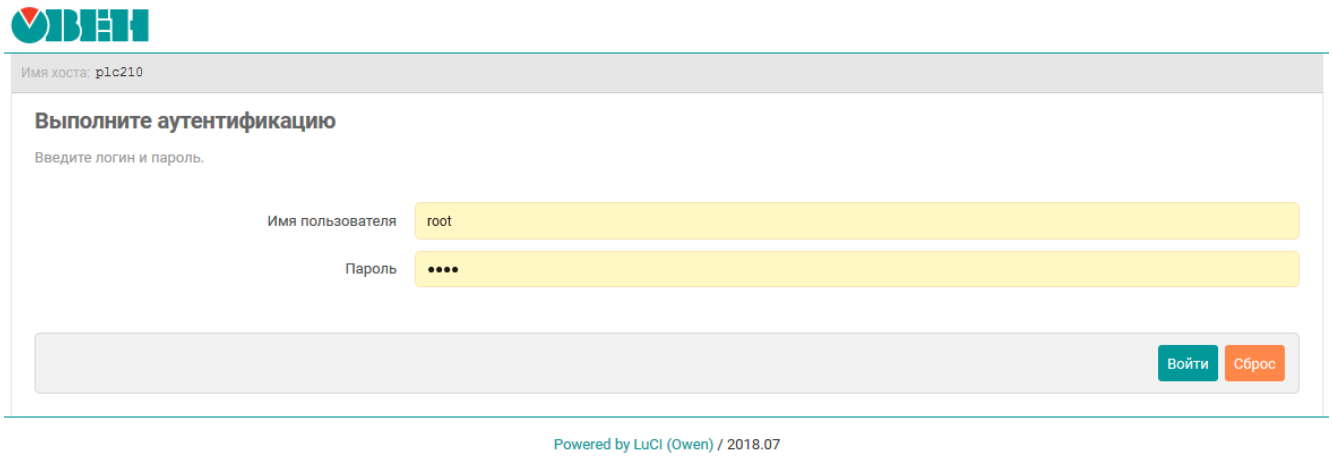


Рис. 1-2: Страница аутентификации

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.

1.4 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 в верхней части 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

Мастер настройки 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 1.3), будет автоматически отображено всплывающее окно мастера настройки, как показано на рисунке 2-1.

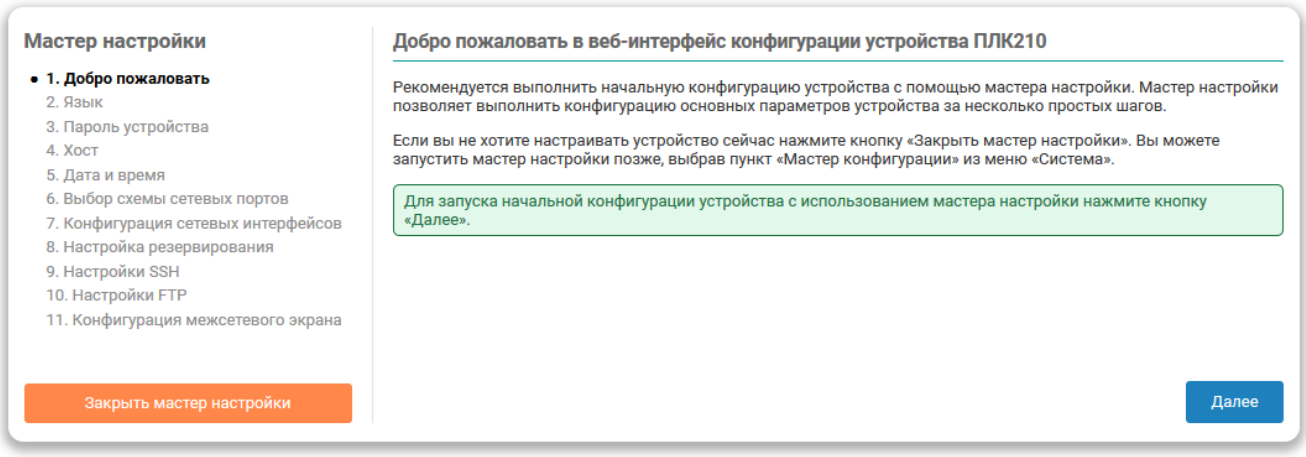


Рис. 2-1: Запуск «Мастера настройки» при первом включении устройства

Для продолжения работы мастера настройки необходимо нажать кнопку «Далее».

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:

- выбор языка интерфейса (раздел 2.1);
- установка пароля доступа к устройству (раздел 2.2);
- конфигурация параметров хоста (раздел 2.3);
- настройка даты и времени, включая конфигурацию клиента и сервера NTP (раздел 2.4);
- выбор схемы сетевых портов (раздел 2.5);
- настройка сетевых интерфейсов (раздел 2.6);
- настройка функции резервирования ПЛК (разедл 2.7);
- настройка службы SSH (раздел 2.8);
- настройка службы FTP (раздел 2.9);
- настройка правил межсетевого экрана (раздел 2.10).

В зависимости от используемого контроллера количество и состав настроек шагов мастера настройки может отличаться.

В левой части окна 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).

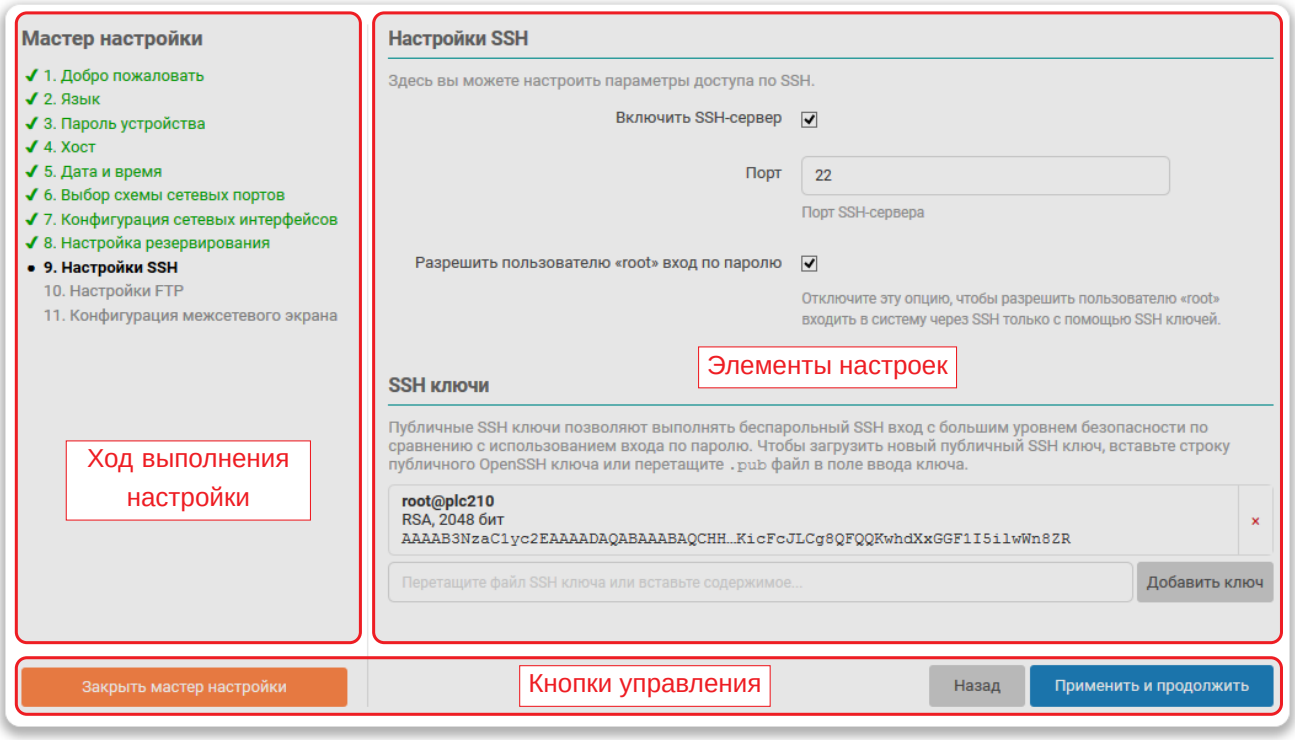


Рис. 2-2: Мастер настройки. Элементы управления

В нижней части страницы мастера настроек расположены кнопки управления (см. рисунок 2-2).

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

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 «Применить и продолжить» (или «Завершить» для последнего шага).

В правой части окна мастера настройки расположены 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 Язык

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

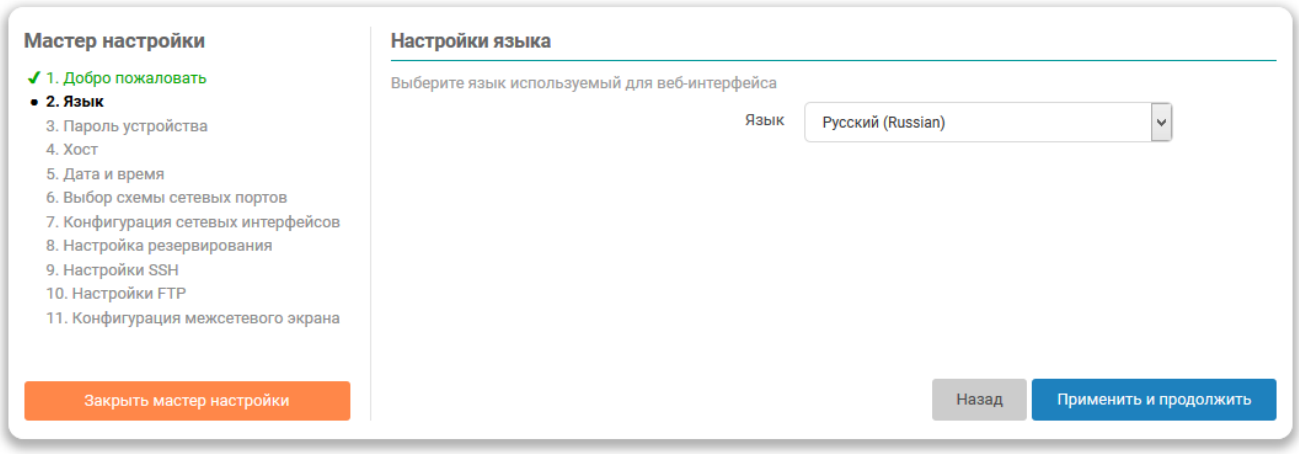


Рис. 2-3: Мастер настройки. Настройки языка интерфейса

В выпадающем списке «Язык» помимо списка языков 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 Пароль устройства

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

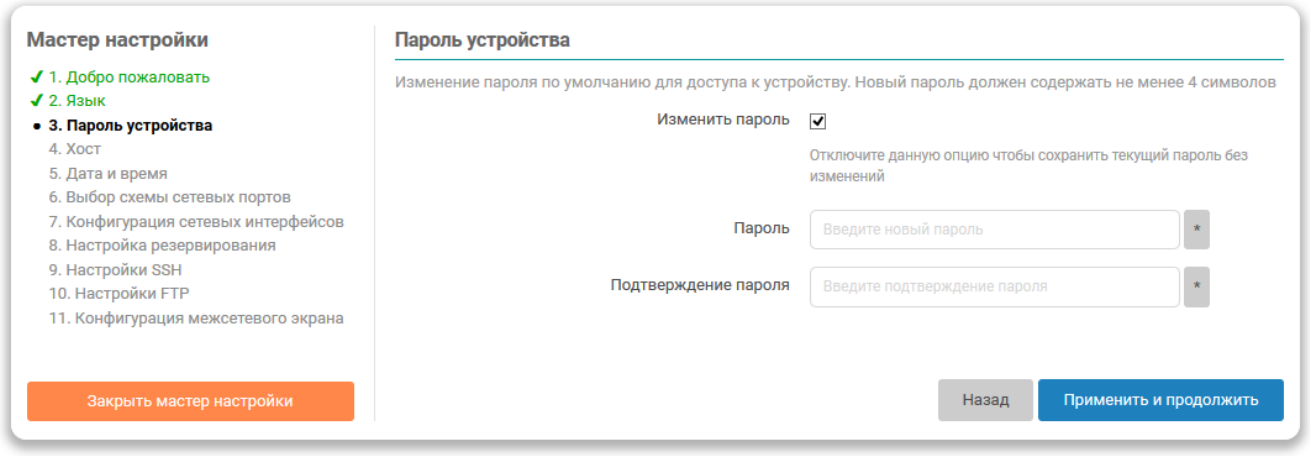


Рис. 2-4: Мастер настройки. Установка пароля устройства

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), то 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 Хост

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

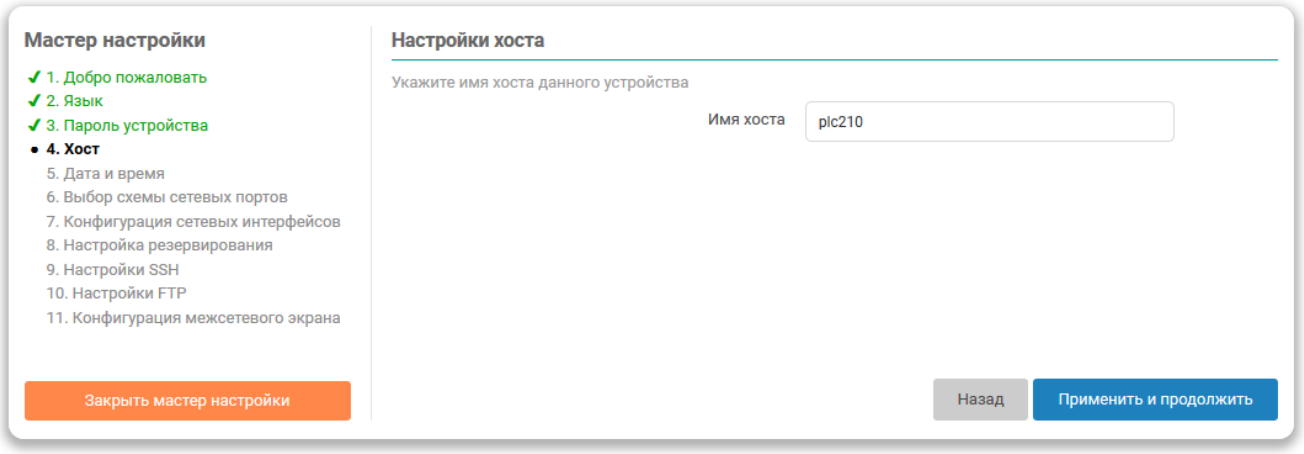


Рис. 2-5: Мастер настройки. Настройка параметров хоста

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 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).

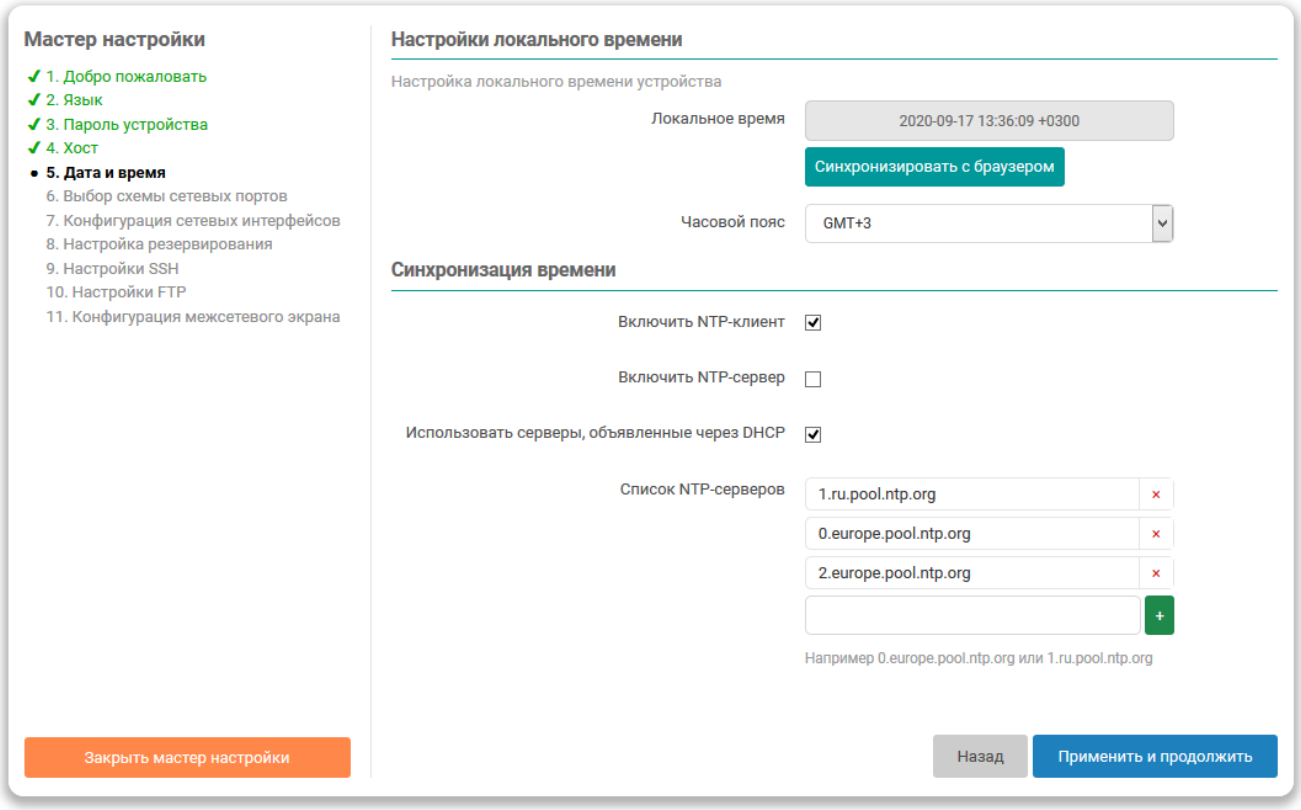


Рис. 2-6: Мастер настройки. Настройка даты и времени

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.

При включении опции «Использовать серверы, объявленные через DHCP» для синхронизации времени будут использованы серверы, объявленные DHCP сервером (опция 42), который выдал устройству параметры конфигурации сети.

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

2.5 Выбор схемы сетевых портов

На данном шаге мастера настройки выполняется выбор схемы сетевых портов устройства. Схема сетевых портов определяет роль каждого из физических сетевых портов устройства, а также количество и назначение сетевых интерфейсов в системе.

В зависимости от используемого контроллера набор доступных схем сетевых портов отличается.

2.5.1 Выбор схемы сетевых портов ПЛК200

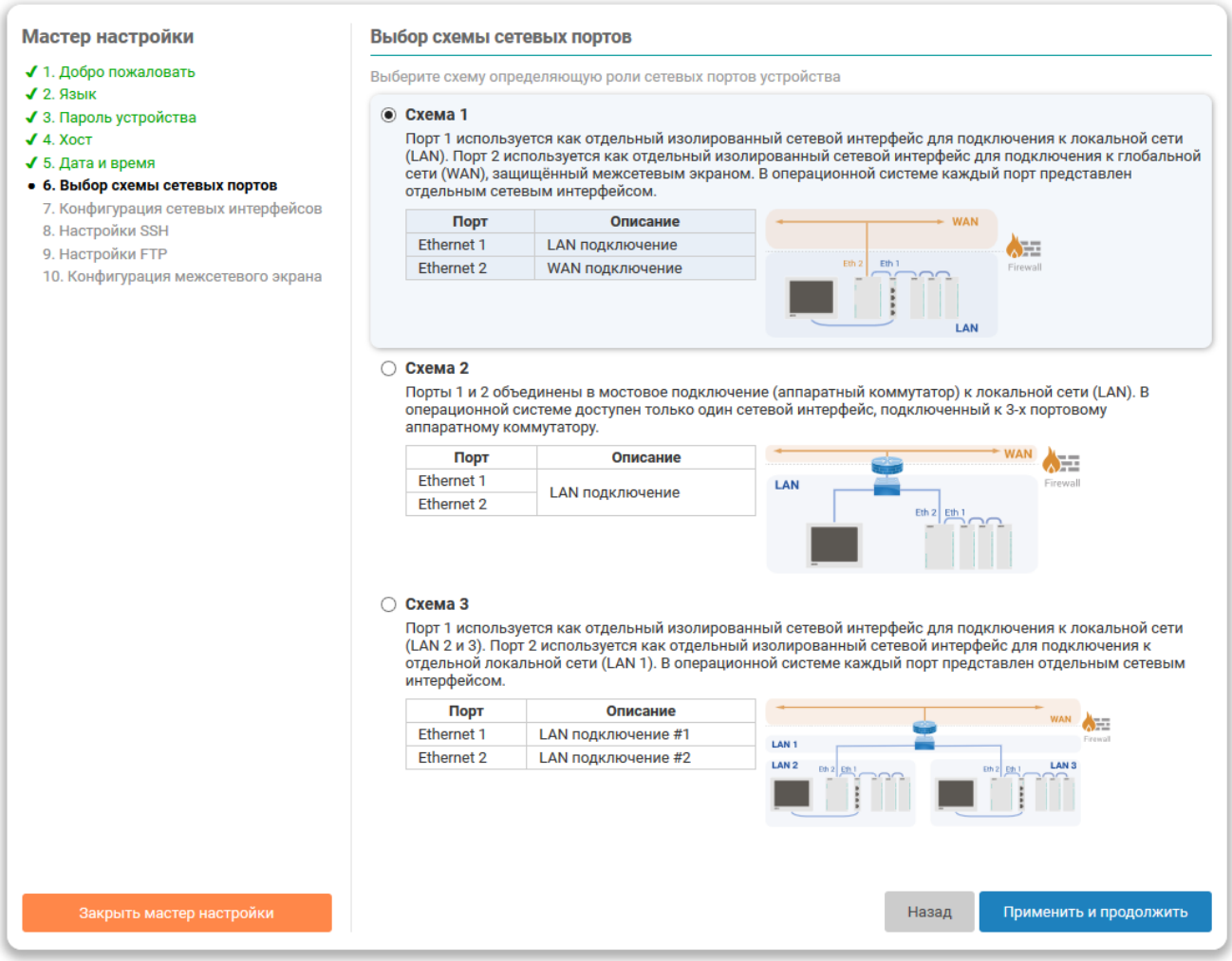


Рис. 2-7: Мастер настройки. Выбор схемы сетевых портов для контроллера ПЛК200

Для контроллера ПЛК200 доступны три схемы сетевых портов (см. рисунок 2-7):

- Схема №1 (см. рисунок 2-8):

  Порт Ethernet 1 используется как отдельный изолированный сетевой интерфейс для подключения 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.

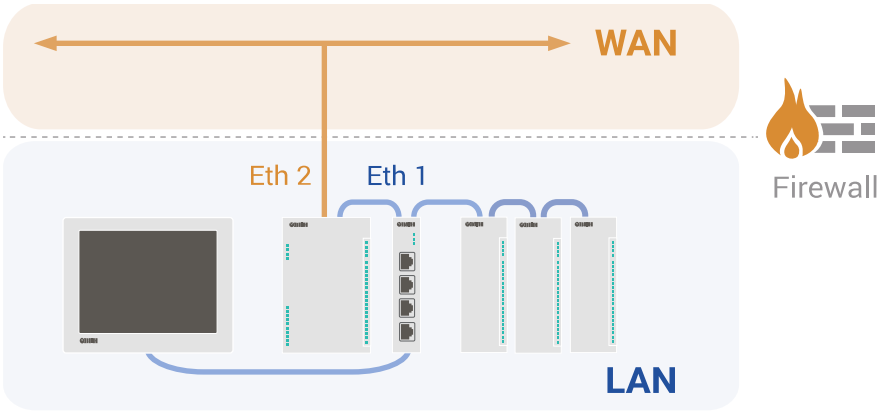


Рис. 2-8: Схема №1 сетевых портов контроллера ПЛК200

- Схема №2 (см. рисунок 2-9):

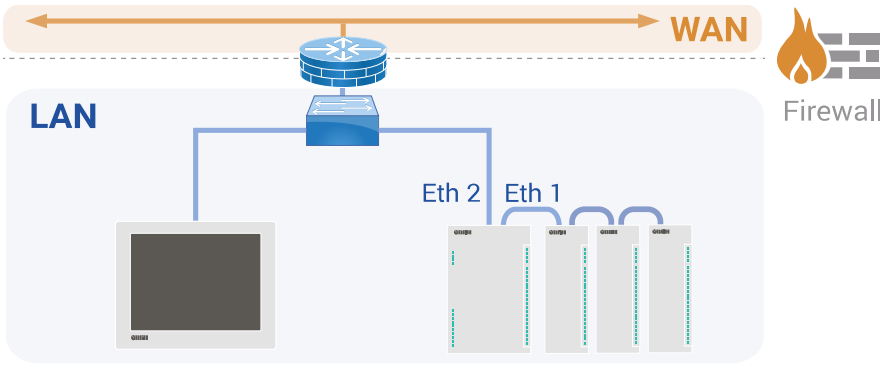


Рис. 2-9: Схема №2 сетевых портов контроллера ПЛК200

Порты Ethernet 1 и Ethernet 2 объединены в мостовое подключение к локальной сети (LAN) в режиме аппаратного коммутатора (см. раздел 3.1.4.1). При выборе данной схемы в системе будет доступен лишь один сетевой интерфейс, подключенный к аппаратному 3-х портовому коммутатору.

- Схема №3 (см. рисунок 2-10):

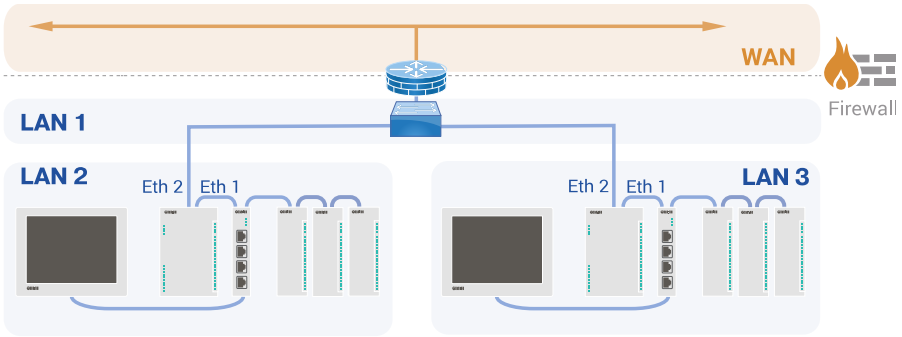


Рис. 2-10: Схема №3 сетевых портов контроллера ПЛК200

Порт Ethernet 1 используется как отдельный изолированный сетевой интерфейс для подключения к локальной сети (LAN 1).

Порт Ethernet 2 используется как отдельный изолированный сетевой интерфейс для подключения к отдельной локальной сети (LAN 2 и LAN 3).

Схема не имеет защищённого межсетевым экраном подключения к глобальной сети (WAN). В случае необходимости подключения к глобальной сети (WAN) рекомендуется использовать промышленный маршрутизатор с поддержкой функции межсетевого экрана.

2.5.2 Выбор схемы сетевых портов ПЛК210

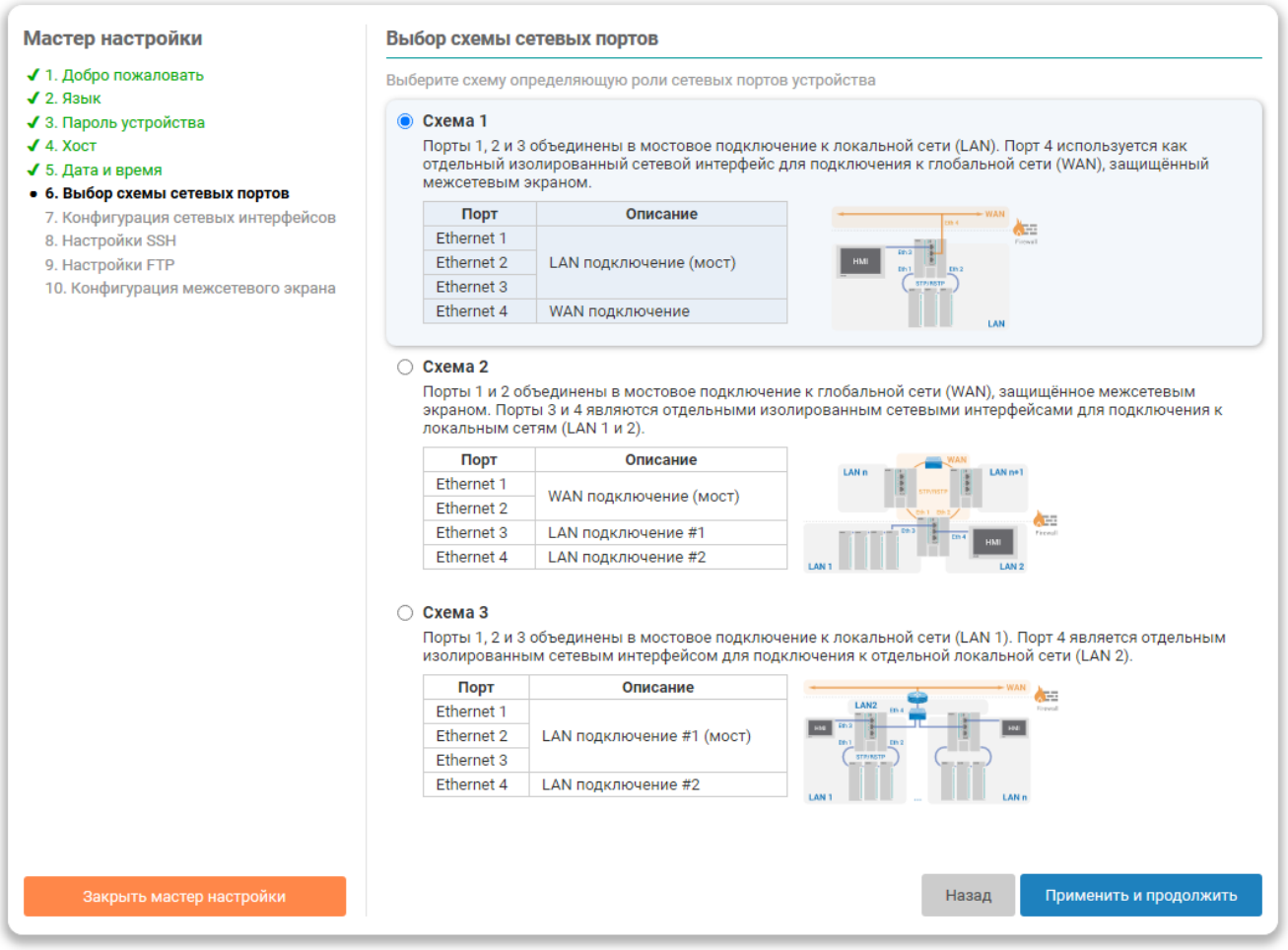


Рис. 2-11: Мастер настройки. Выбор схемы сетевых портов для контроллера ПЛК210

Для контроллера ПЛК210 доступны три схемы сетевых портов (см. рисунок 2-11):

- Схема №1 (см. рисунок 2-12):

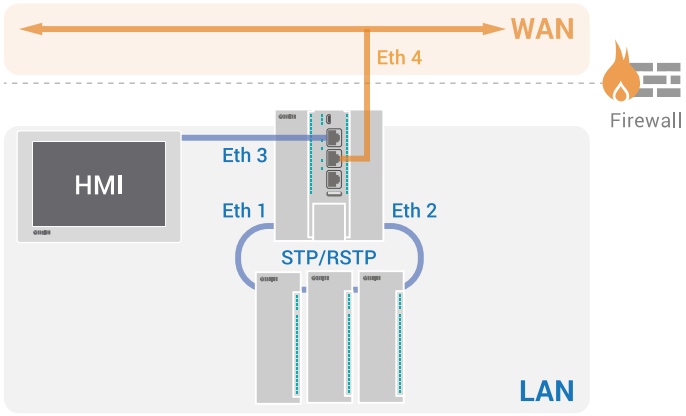


Рис. 2-12: Схема №1 сетевых портов контроллера ПЛК210

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.

- Схема №2 (см. рисунок 2-13):

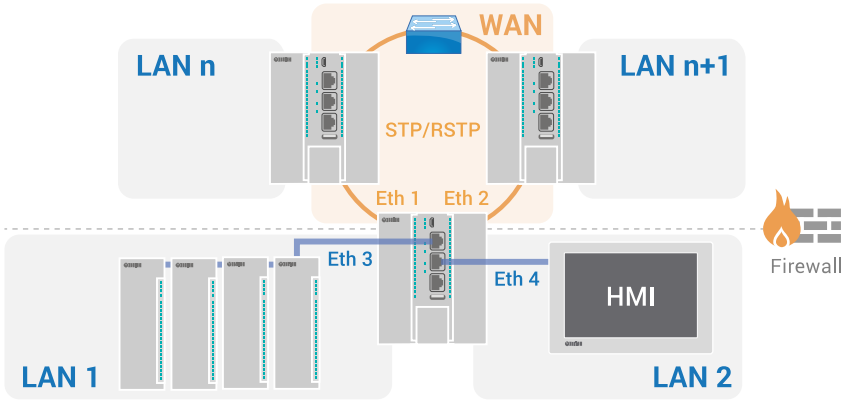


Рис. 2-13: Схема №2 сетевых портов контроллера ПЛК210

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).

- Схема №3 (см. рисунок 2-14):

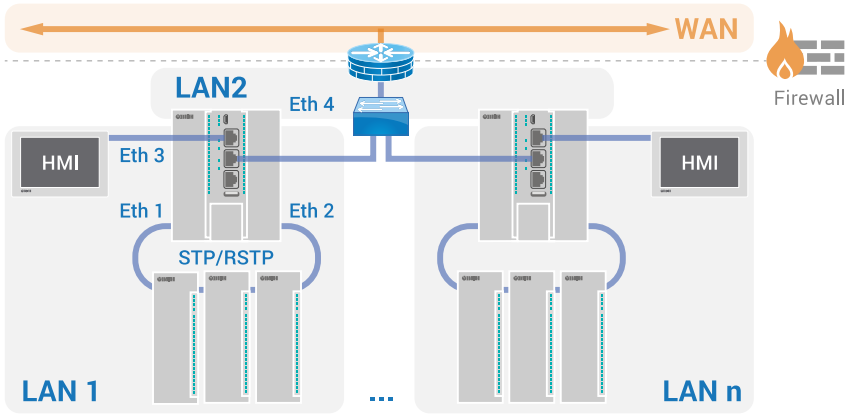


Рис. 2-14: Схема №3 сетевых портов контроллера ПЛК210

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 не имеет защищённого межсетевым экраном подключения к глобальной сети (WAN). В случае необходимости подключения к глобальной сети (WAN) рекомендуется использовать промышленный маршрутизатор с поддержкой функции межсетевого экрана.

В том случае, если используемый контроллер ПЛК210 имеет поддержку резервирования ПЛК, будут доступны для выбора дополнительные схемы сетевых портов. При этом все доступные схемы сетевых портов будут разеделены на две вкладки (см. рисунок 2-15):

- «Без резервирования» — схемы сетевых портов без поддержки функции резервирования, описанные выше. Данные схемы доступны для всех контроллеров ПЛК210 (как с поддержкой функции резервирования так и без неё);
- «С резервированием» — дополнительные схемы сетевых портов с поддержкой функции резервирования. Данные схемы доступны только на контроллерах ПЛК210 с поддержкой функции резервирования.

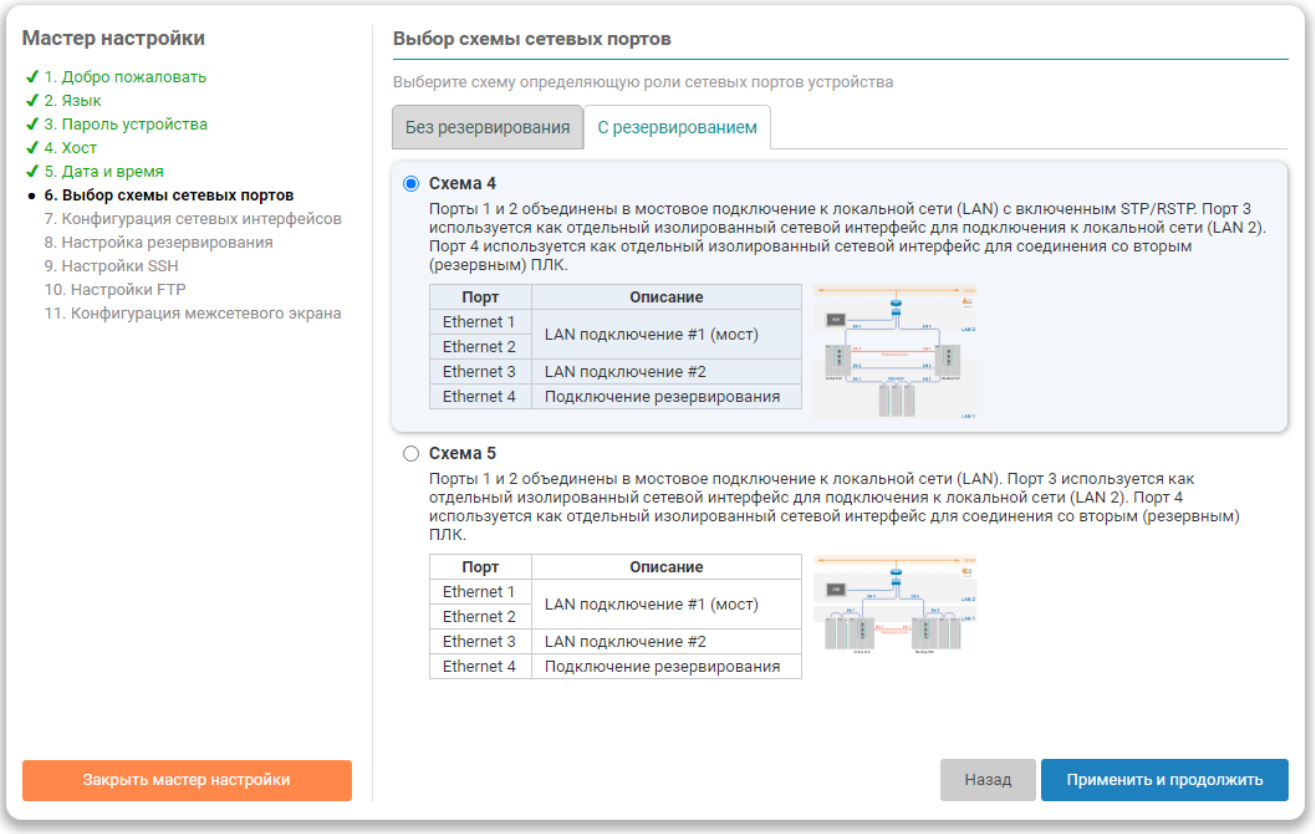


Рис. 2-15: Мастер настройки. Дополнительные схемы сетевых портов для контроллера ПЛК210 с функцией резервирования

Для контроллера ПЛК210 с поддержкой функции резервирования доступны следующие дополнительные схемы сетевых портов (см. рисунок 2-15):

- Схема №4 (см. рисунок 2-16):

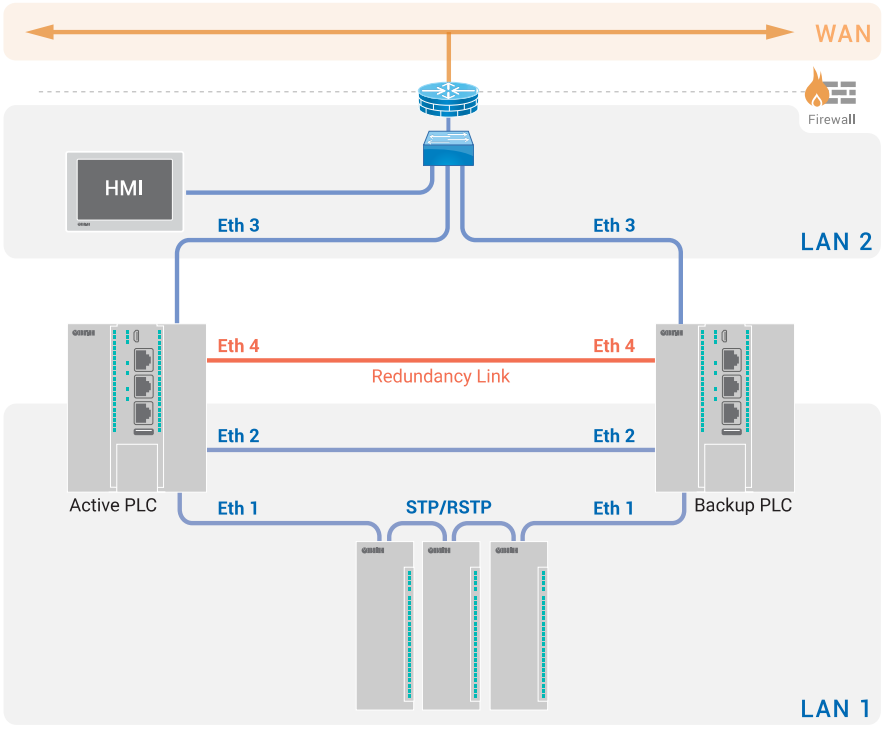


Рис. 2-16: Схема №4 сетевых портов контроллера ПЛК210 с поддержкой функции резервирования

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

Порт Ethernet 3 используется как отдельный изолированный сетевой интерфейс для подключения к локальной сети (LAN 2)

Порт Ethernet 4 используется как отдельный изолированный сетевой интерфейс для соединения со вторым (резервным) ПЛК.

- Схема №5 (см. рисунок 2-17):

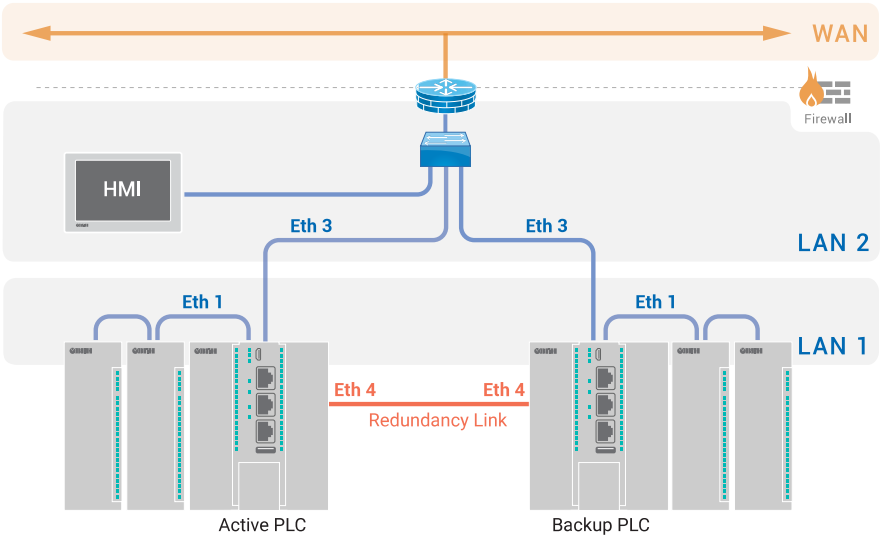


Рис. 2-17: Схема №5 сетевых портов контроллера ПЛК210 с поддержкой функции резервирования

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

Порт Ethernet 3 используется как отдельный изолированный сетевой интерфейс для подключения к локальной сети (LAN 2)

Порт Ethernet 4 используется как отдельный изолированный сетевой интерфейс резервирования для подключения второго (резервного) ПЛК.

2.6 Конфигурация сетевых интерфейсов

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

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

Настройки каждого сетевого интерфейса расположены в отдельной вкладке (см. рисунок 2-18).

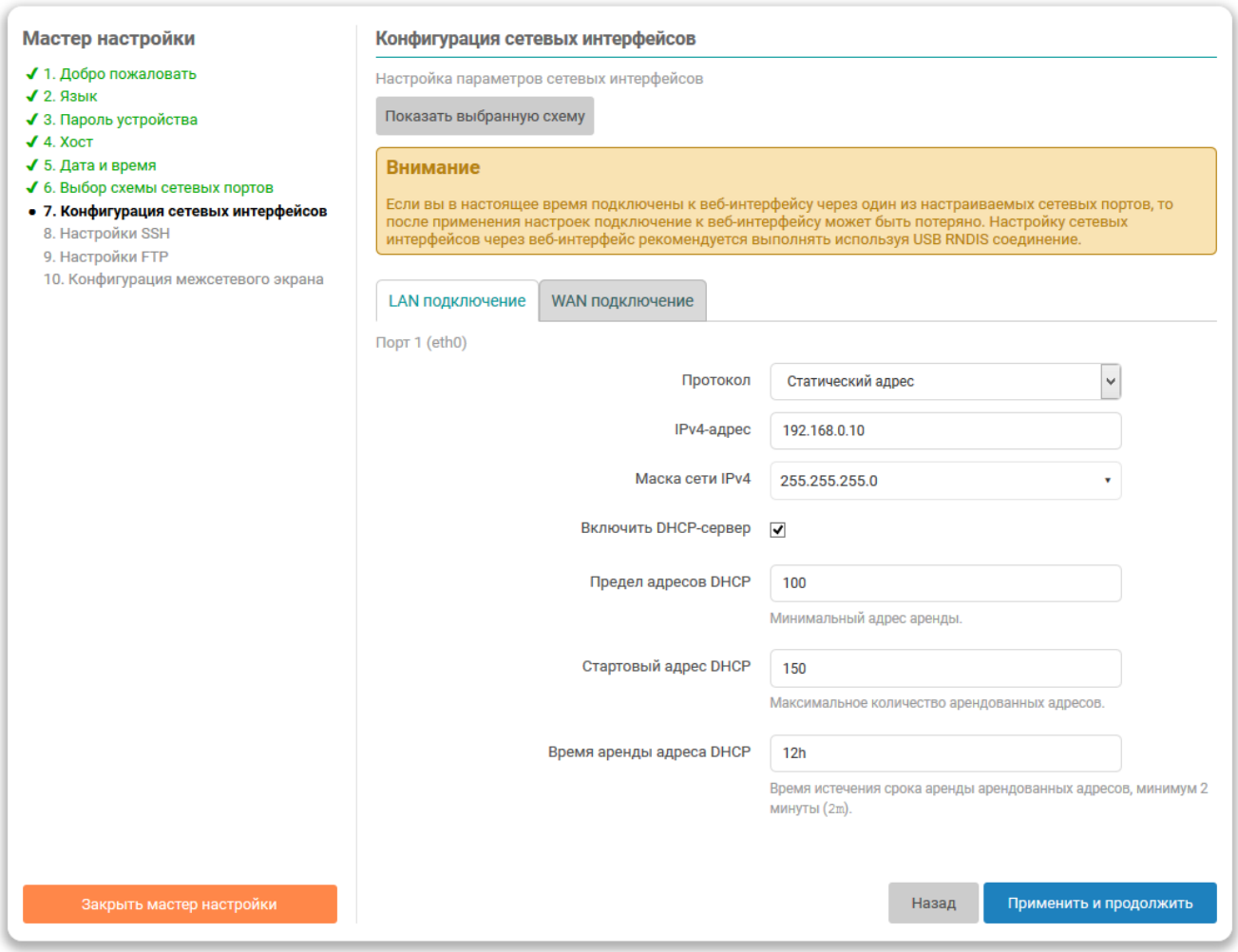


Рис. 2-18: Мастер настройки. Настройки сетевых интерфейсов

Над вкладками настроек интрфейсов расположена кнопка «Показать выбранную схему», при нажатии на которую будет отображено всплывающее окно (см. рисунок 2-19) с информацией о текущей выбранной схеме сетевых портов (см. раздел 2.5).

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. Возможность выбора протокола «Клиент DHCP» отсутствует для интерфейсов резервирования.

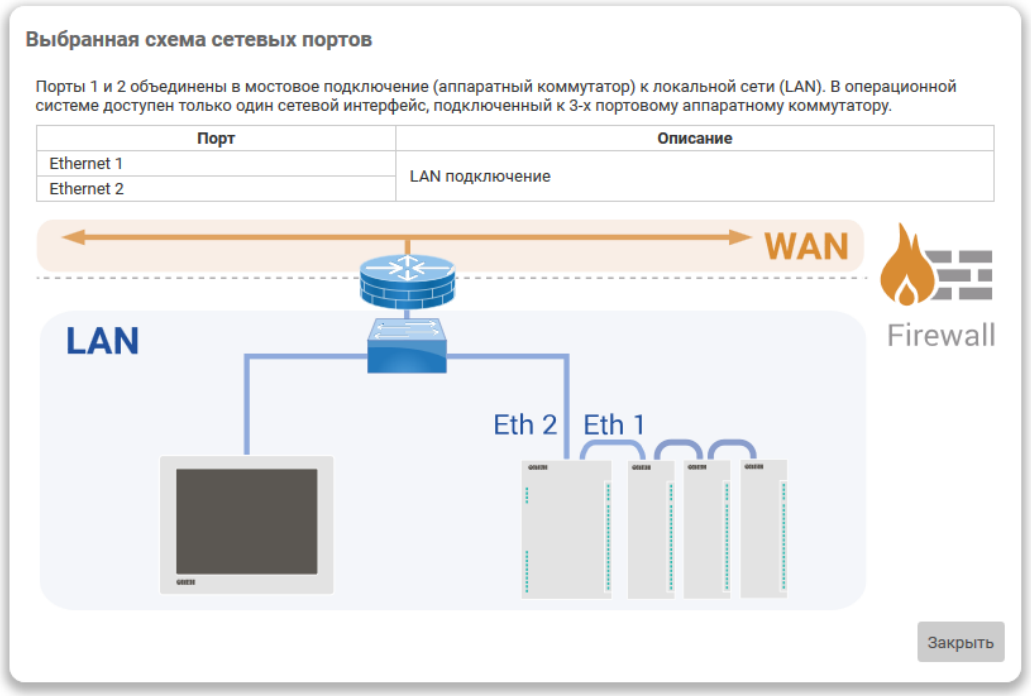


Рис. 2-19: Мастер настройки. Окно с информацией о выбранной схеме сетевых портов

- «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».

Для интерфейсов мостовых подключений (мостовое LAN или 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.

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».

Если подключение к Web-интерфейсу выполняется через один из настраиваемых сетевых портов, то после нажатия кнопки «Применить и продолжить» подключение к Web-интерфейсу может быть потеряно. Настройку сетевых интерфейсов через Web-интерфейс рекомендуется выполнять используя USB RNDIS подключение.

2.6.1 Переключение режима работы аппаратного коммутатора на контроллере ПЛК200

На контроллере ПЛК200 доступен режим аппаратного коммутатора (см. разделы 2.5.1 и 3.1.4.1). В том случае если выбрана схема сетевых портов, предполагающая переключение текущего режима работы аппаратного коммутатора, то на шаге настройки сетевых интерфейсов будет выведено соответствующее предупредление о необходимости перезагрузки устройства, как показано на рисунке 2-20.

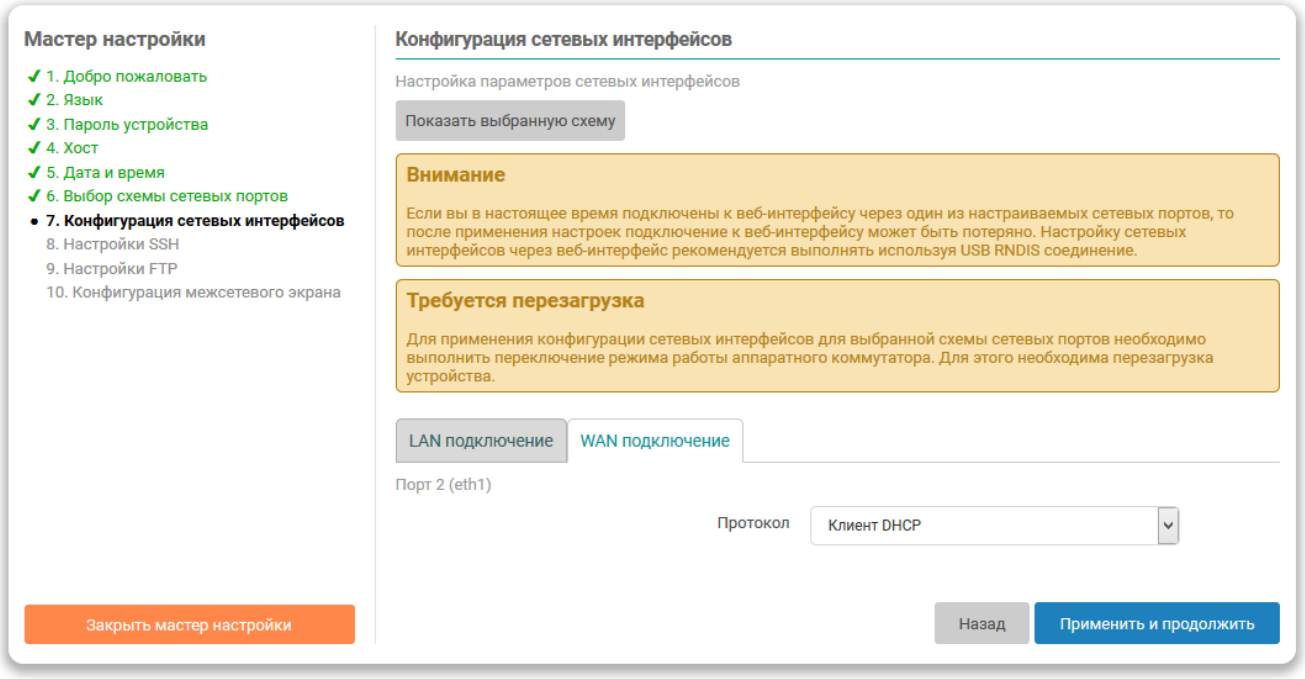


Рис. 2-20: Мастер настройки. Предупреждение о необходимости перезагрузки для переключения режима работы аппаратного коммутатора на контроллере ПЛК200

В этом случае, после нажатия кнопки «Применить и продолжить», будет отображено всплывающее окно с запросом подтверждения перезагрузки устройства, как показано на рисунке 2-21.

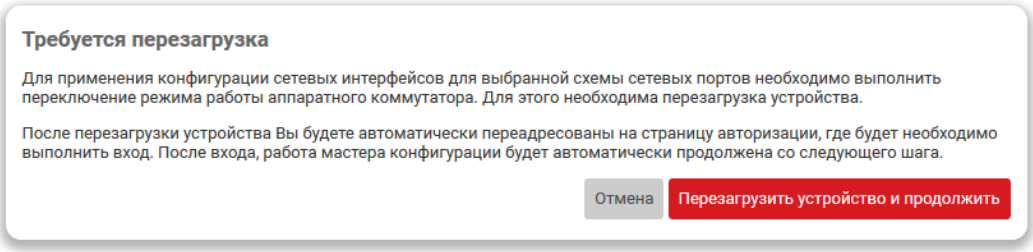


Рис. 2-21: Мастер настройки. Подтверждение перезагрузки для переключения режима работы аппаратного коммутатора на контроллере ПЛК200

Нажатие кнопки «Перезагрузить устройство и продолжить» приведёт к перезагрузке устройства, переключению режима работы аппаратного коммутатора в соответствии с выбранной схемой сетевых портов и при-

менению настроек сетевых интерфейсов. После выполнения перезагрузки устройства будет выполнена автоматическая переадресация на страницу авторизации (см. раздел 1.3), где необходимо ввести учётные данные для входа в систему. После успешного входа в систему будет автоматически запущен мастер настройки на шаге следующим за шагом конфигурации сетевых интерфейсов для продолжения конфигурирования устройства.

2.7 Настройки резервирования

Данный шаг мастера настройки присутствует только в Web-интерфейсе управления контроллеров ПЛК210 с поддержкой функции резервирования.

Если ранее, на шаге выбора схемы сетевых портов, была выбрана схема без резервирования (см. раздел 2.5.2), то настройки резервирования будут не доступны. В этом случае область настроек данного шага будет выглядеть так, как показано на рисунке 2-22.

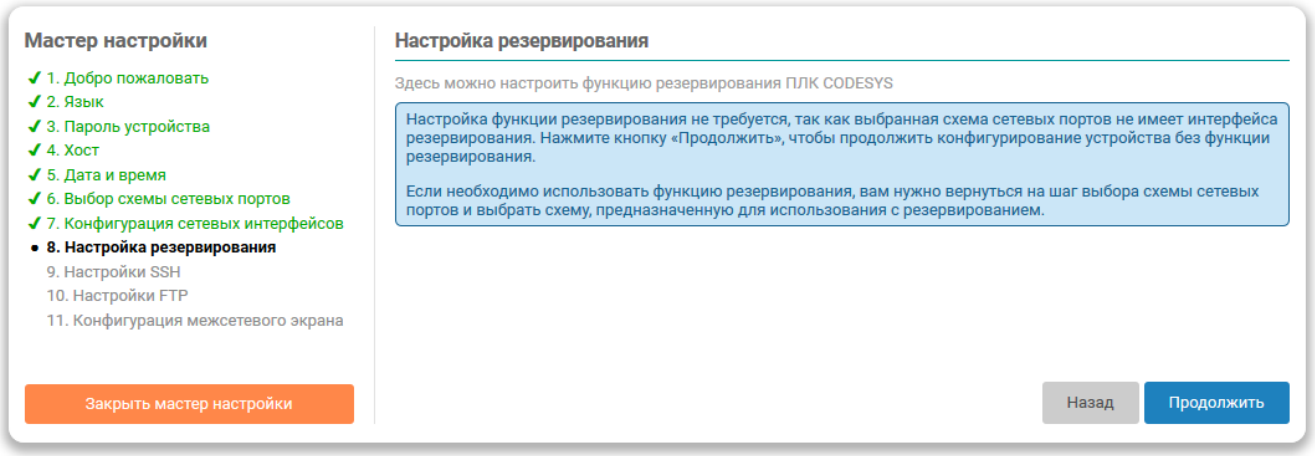


Рис. 2-22: Мастер настройки. Настройка резервирования не требуется

Настройки для схемы сетевых портов с поддержкой резервирования на данном шаге будут выглядеть так, как показано на рисунке 2-23.

Настройка резервирования предполагает одновременный запуск мастера настройки сразу на двух устройствах. В первую очередь, на каждом из устройств необходимо выбрать режим конфигурирования. На одном из устройств выбирается режим конфигурирования «ПЛК 1», а на другом — «ПЛК 2».

Далее по тексту устройство с выбранным режимом конфигурирования «ПЛК 1» будет обозначаться просто как устройство ПЛК 1, а устройство с выбранным режимом конфигурирования «ПЛК 2» — устройство ПЛК 2.

Далее в разделах 2.7.1 и 2.7.2 приводится детальное описание конфигурирования в режимах «ПЛК 1» и «ПЛК 2» соответственно.

В дальнейшем настройка функций резервирования ПЛК может быть произведена на странице «Резервирование» пункта главного меню «ПЛК» (см. раздел 5.5).

2.7.1 Настройка в режиме конфигурирования «ПЛК 1»

Устройство с выбранным режимом конфигурирования «ПЛК 1» является основным и осуществляет конфигурирование как своих собственных параметров резервирования, так и удалённого второго устройства (на котором выбран режим конфигурирования «ПЛК 2»).

При выборе режима конфигурирования «ПЛК 1» доступны следующие настройки (см. рисунок 2-23):

- «IP-адрес подключенного ПЛК» — IP-адрес подключенного ПЛК (устройство ПЛК 1) на интерфейсе резервирования. На данном шаге настройка доступна только для чтения.

  Если IP-адрес требуется изменить, необходимо вернуться к шагу конфигурации сетевых интерфейсов (см. раздел 2.6) и выполнить требуемые изменения.

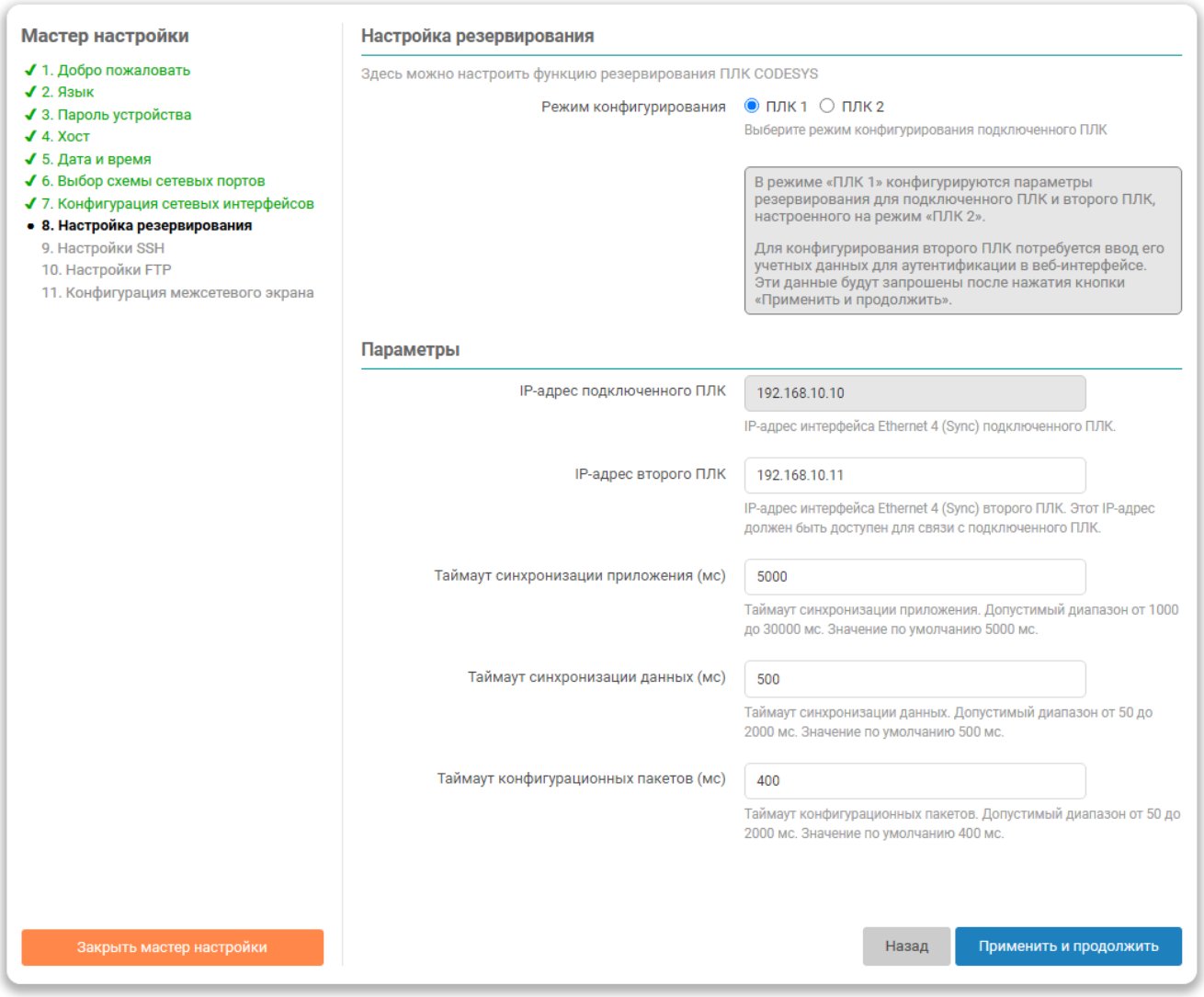


Рис. 2-23: Мастер настройки. Настройки резервирования в режиме конфигурирования «ПЛК 1»

- «IP-адрес второго ПЛК» — IP-адрес второго ПЛК (устройство ПЛК 2). Данный IP-адрес должен быть в той же подсети, что и IP-адрес подключенного ПЛК 1.
- «Таймаут синхронизации приложения (мс)» — таймаут синхронизации приложения. Допустимый диапазон от 1000 до 30000 мс (1–30 с). Значение по умолчанию 5000 мс (5 с). Значение данного параметра будет синхронизировано на устройство ПЛК 2.
- «Таймаут синхронизации данных (мс)» — таймаут синхронизации данных. Допустимый диапазон от 50 до 2000 мс. Значение по умолчанию 500 мс. Значение данного параметра будет синхронизировано на устройство ПЛК 2.
- «Таймаут конфигурационных пакетов (мс)» — таймаут конфигурационных пакетов. Допустимый диапазон от 50 до 2000 мс. Значение по умолчанию 400 мс. Значение данного параметра будет синхронизировано на устройство ПЛК 2.

При нажатии кнопки «Применить и продолжить» будет отображено всплывающее окно с запросом имени пользователя и пароля для аутентификации на устройстве ПЛК 2, как показано на рисунке 2-24. Эти данные требуются, так как конфигурирование устройства ПЛК 2 осуществляется по сети через сетевой интерфейс резервирования с использованием протокола SSH.

Нажатие кнопки «Сконфигурировать» приведёт к запуску процесса конфигурирования функции резервирования на устройствах ПЛК 1 и ПЛК 2. Перед запуском процесса конфигурирования необходимо убедиться, что выполнены следующие основные условия:

- на обоих устройствах, на шаге выбора схемы сетевых портов, выбрана схема с резервированием (см. раздел 2.5.2);

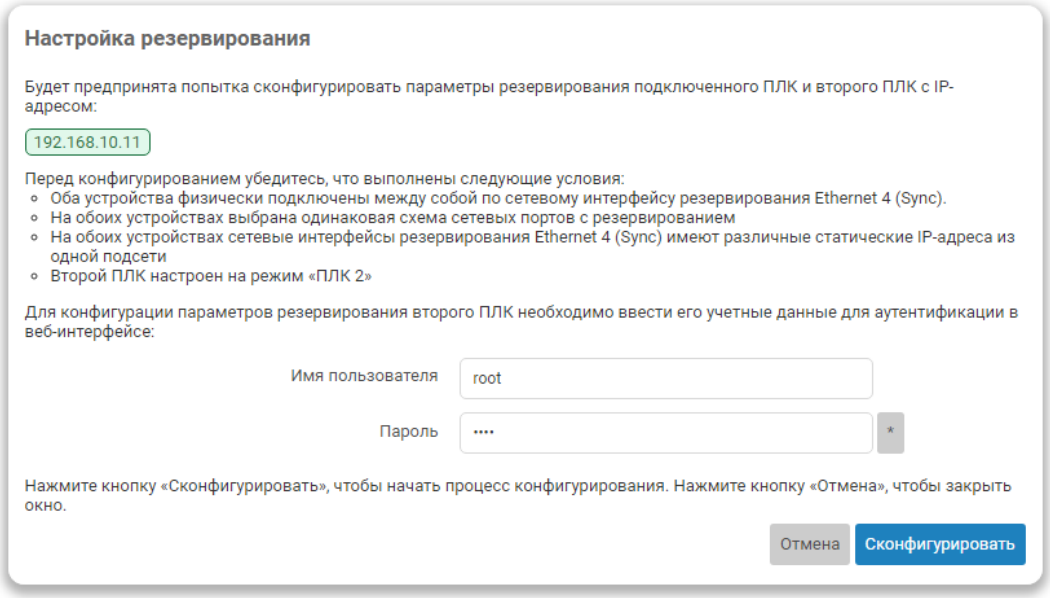


Рис. 2-24: Мастер настройки. Запрос имени пользователя и пароля для аутентификации на устройстве ПЛК 2

- на обоих устройствах сетевые интерфейсы резервирования имеют различные статические IP-адреса из одной подсети;
- оба устройства физически подключены между собой через сетевые интерфейсы резервирования;
- на устройстве ПЛК 2 запущен процесс ожидания окончания конфигурирования устройства (см. раздел 2.7.2).

Во время процесса конфигурирования будет отображаться окно, показанное на рисунке 2-25.

Рис. 2-25: Мастер настройки. Процесс конфигурирования резервирования

Если в процессе конфигурирования произойдёт ошибка, то будет отображено окно с информацией об ошибке, показанное на рисунке 2-26.

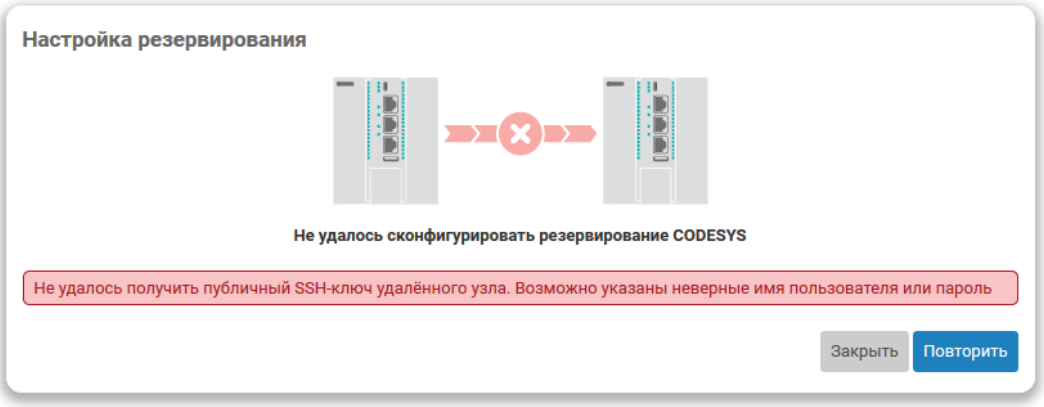


Рис. 2-26: Мастер настройки. Ошибка конфигурирования резервирования

Кнопка «Повторить» позволяет выполнить повторную попытку конфигурирования с теми же параметрами. Нажатие кнопки «Закрыть» приведёт к закрытию всплывающего окна, после чего можно выполнить изменение параметров резервирования и повторить процедуру конфигурирования.

В случае успешного завершения конфигурирования будет отображено окно, показанное на рисунке 2-27.

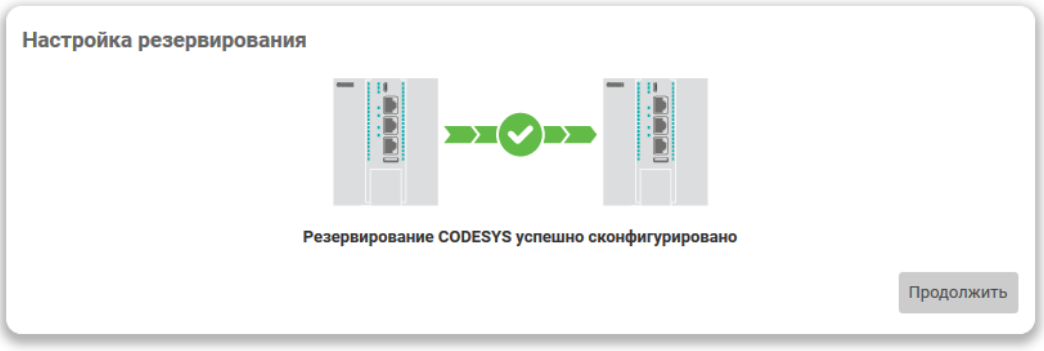


Рис. 2-27: Мастер настройки. Успешное завершение конфигурирования резервирования

Нажатие кнопки «Продолжить» приведёт к переходу на следующий шаг мастера настройки.

2.7.2 Настройка в режиме конфигурирования «ПЛК 2»

Устройство с выбранным режимом конфигурирования «ПЛК 2» является ведомым по отношению к устройству ПЛК 1 и осуществляет лишь ожидание окончания конфигурирования параметров резервирования устройством ПЛК 1.

При выборе режима конфигурирования «ПЛК 2» окно мастера настройки будет выглядеть так, как показано на рисунке 2-28.

В окне будет отображаться лишь значение IP-адреса данного ПЛК, сконфигурированного на сетевом интерфейсе резервирования. Данное значение IP-адреса должно быть введено в качестве значения параметра «IP-адрес второго ПЛК» на устройстве ПЛК 1 (см. раздел 2.7.1).

Для изменения IP-адреса сетевого интерфейса резервирования необходимо вернуться к шагу конфигурации сетевых интерфейсов (см. раздел 2.6).

После нажатия кнопки «Применить и продолжить» выполняется переход к следующему шагу.

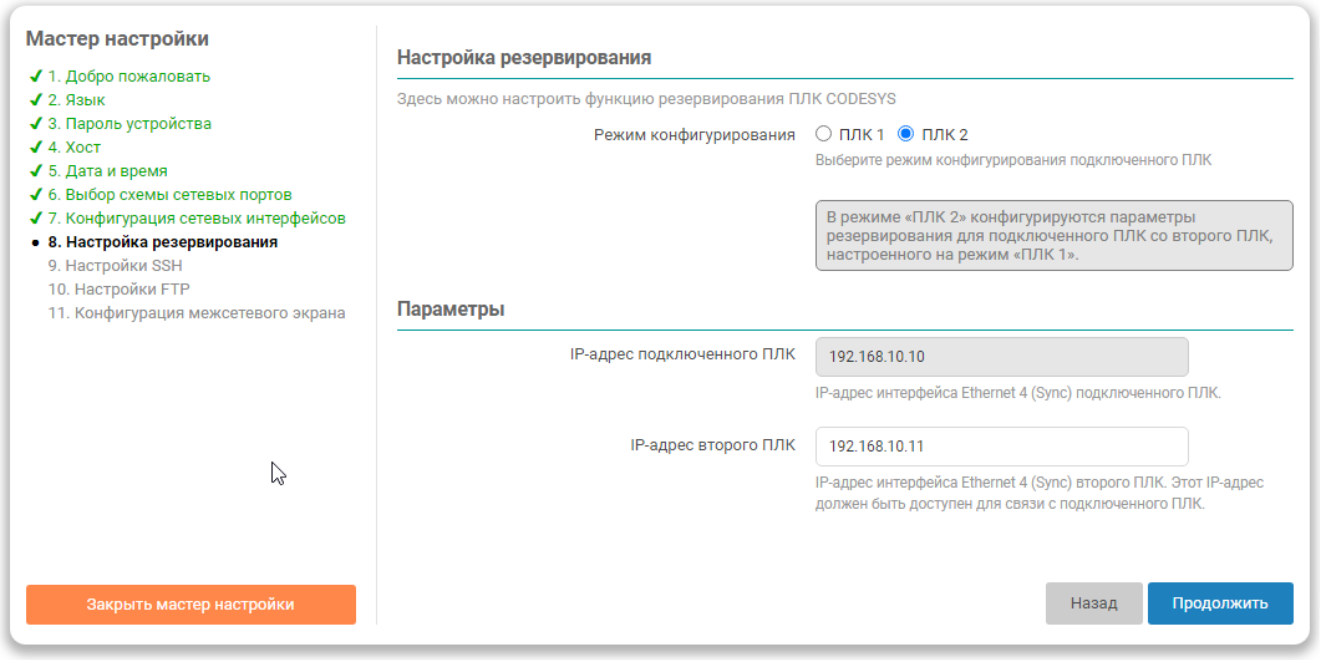


Рис. 2-28: Мастер настройки. Настройки резервирования в режиме конфигурирования «ПЛК 2»

2.8 Настройки SSH

На данном шаге мастера настройки выполняется настройка параметров доступа к устройству с использованием SSH-протокола (см. рисунок 2-29).

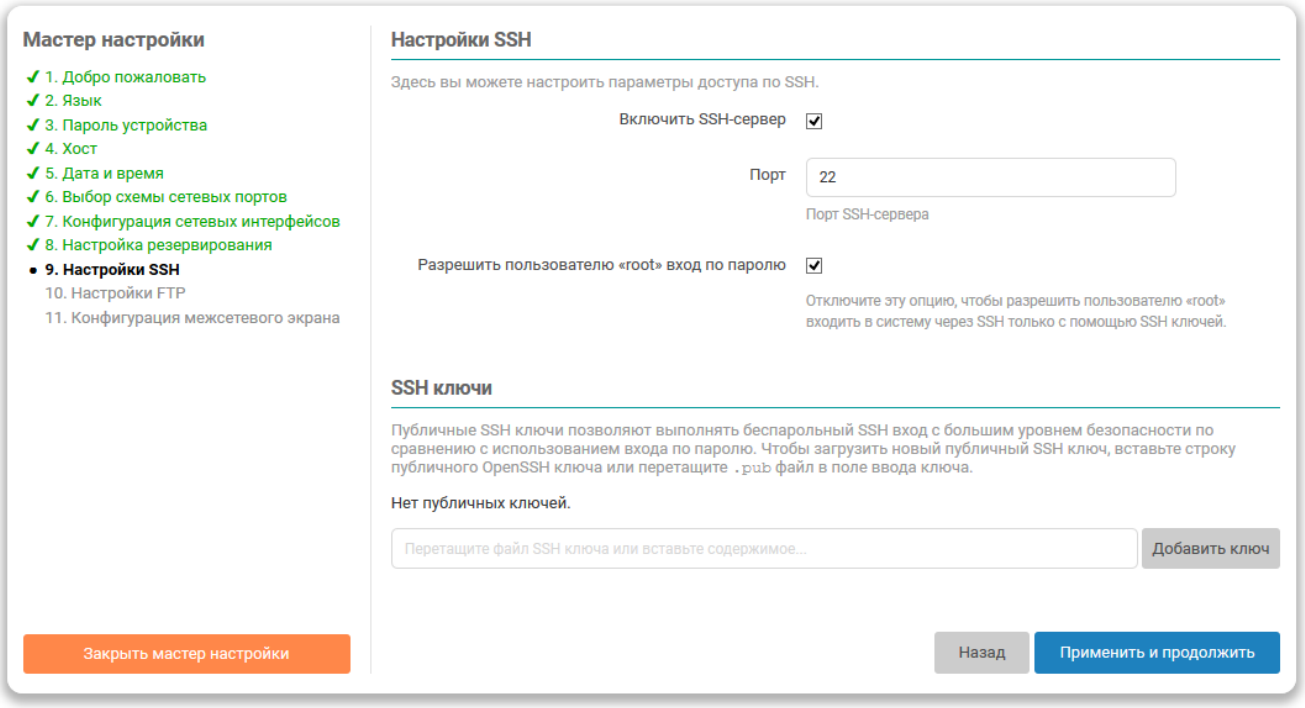


Рис. 2-29: Мастер настройки. Настройка SSH

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

Отключение службы SSH-сервера невозможно в случае выбора схемы сетевых портов с поддержкой функции резервирования на контроллере ПЛК210.

При необходимости отключения службы SSH-сервера рекомендуется выполнить ручную настройку сервера Dropbear (см. раздел 4.3.2), оставив в списке интерфейсов только сетевой интерфейс резервирования.

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 с использованием SSH-протокола. 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 2.8.1).

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.

2.8.1 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 2-30.

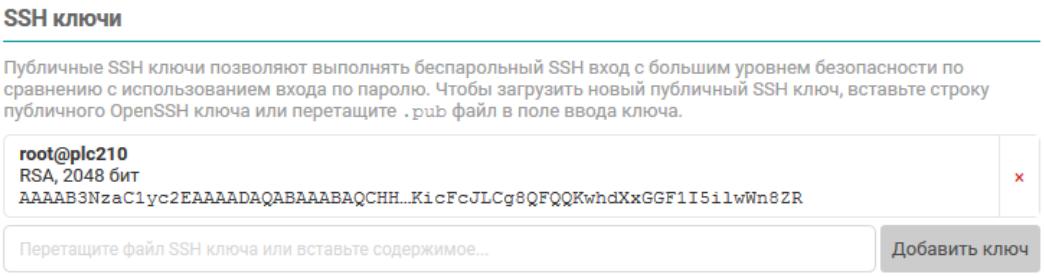


Рис. 2-30: Мастер настройки. Добавленный SSH ключ

На контроллере ПЛК210 с использованием схемы сетевых портов с поддержкой функции резервирования во время конфигурирования резервирования (см. раздел 2.7) автоматически выполняется добавление публичного SSH ключа второго (резервного) ПЛК. Удаление этого ключа может привести к нарушению некоторых функций резервирования, описанных в разделе 5.5 данного руководства.

Для удаления добавленного ключа необходимо нажать кнопку с красным крестиком справа от информации о ключе. При этом будет отображено всплывающее окно с запросом подтверждения удаления ключа, как показано на рисунке 2-31.

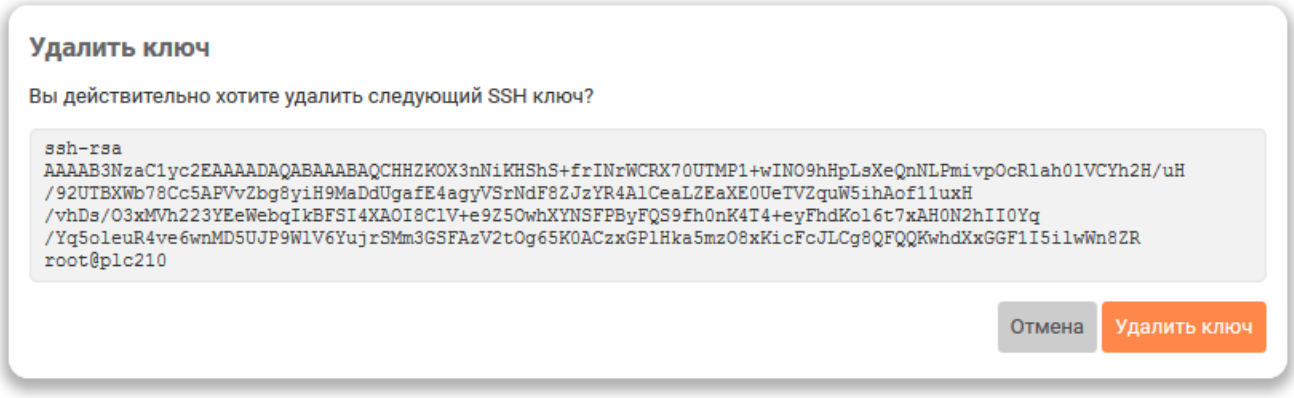


Рис. 2-31: Мастер настройки. Подтверждение удаления SSH ключа

2.9 Настройки FTP

На данном шаге мастера настройки выполняется настройка параметров FTP-сервера (см. рисунок 2-32).

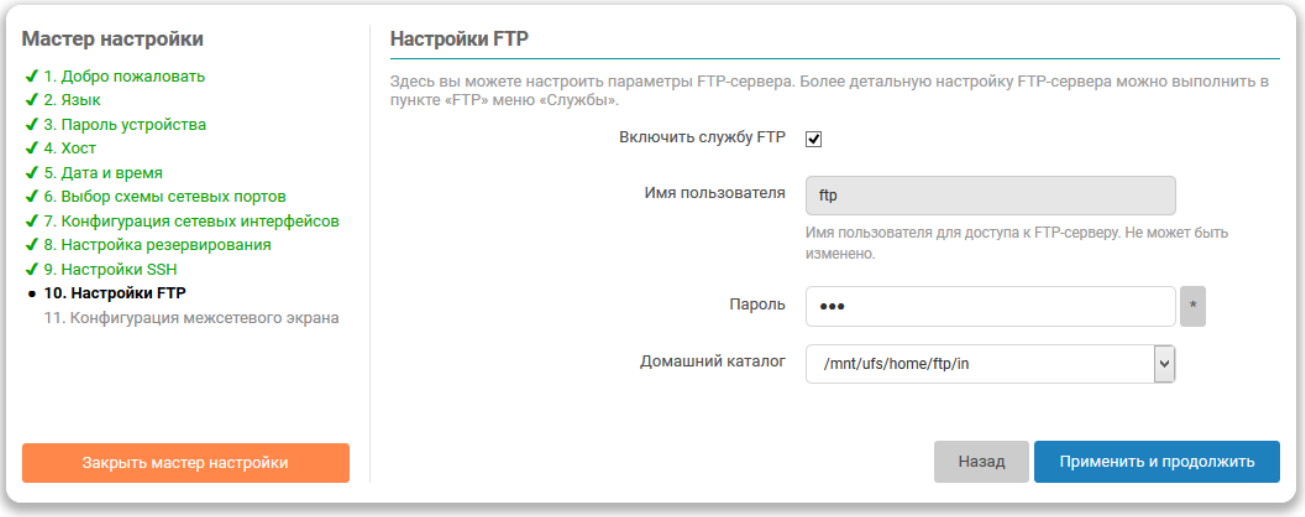


Рис. 2-32: Мастер настройки. Настройка FTP

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 6.5).

2.10 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 2-33.

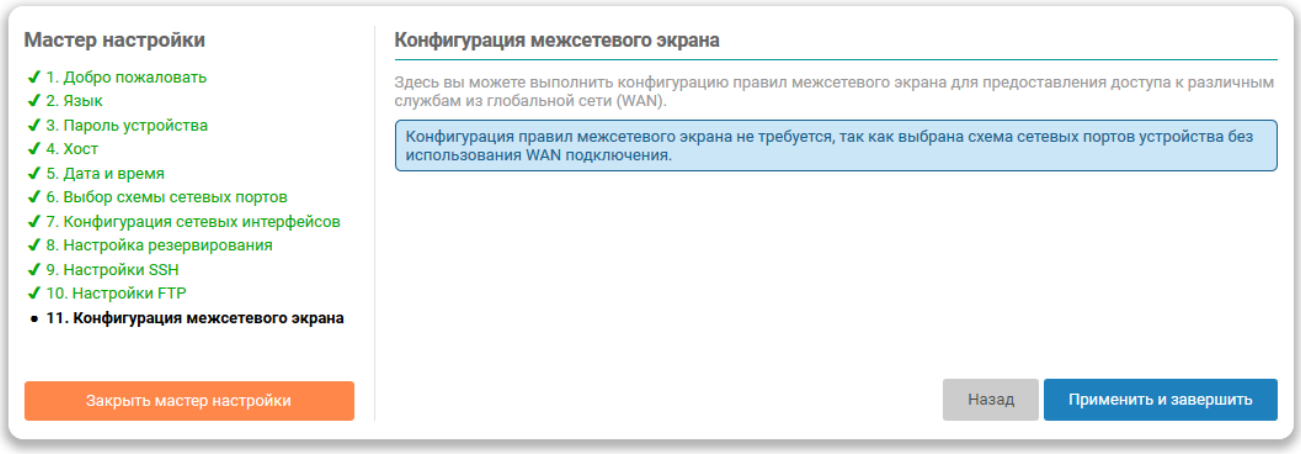


Рис. 2-33: Мастер настройки. Настройка межсетевого экрана не требуется

Для схемы сетевых портов с подключением к глобальной сети (WAN) настройки межсетевого экрана для данного шага будут выглядеть так, как показано на рисунке 2-34.

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

- «HTTP» — доступ к Web-интерфейсу LuCI по протоколу HTTP (по умолчанию TCP порт 80).
- «HTTP Secure» — доступ к Web-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).

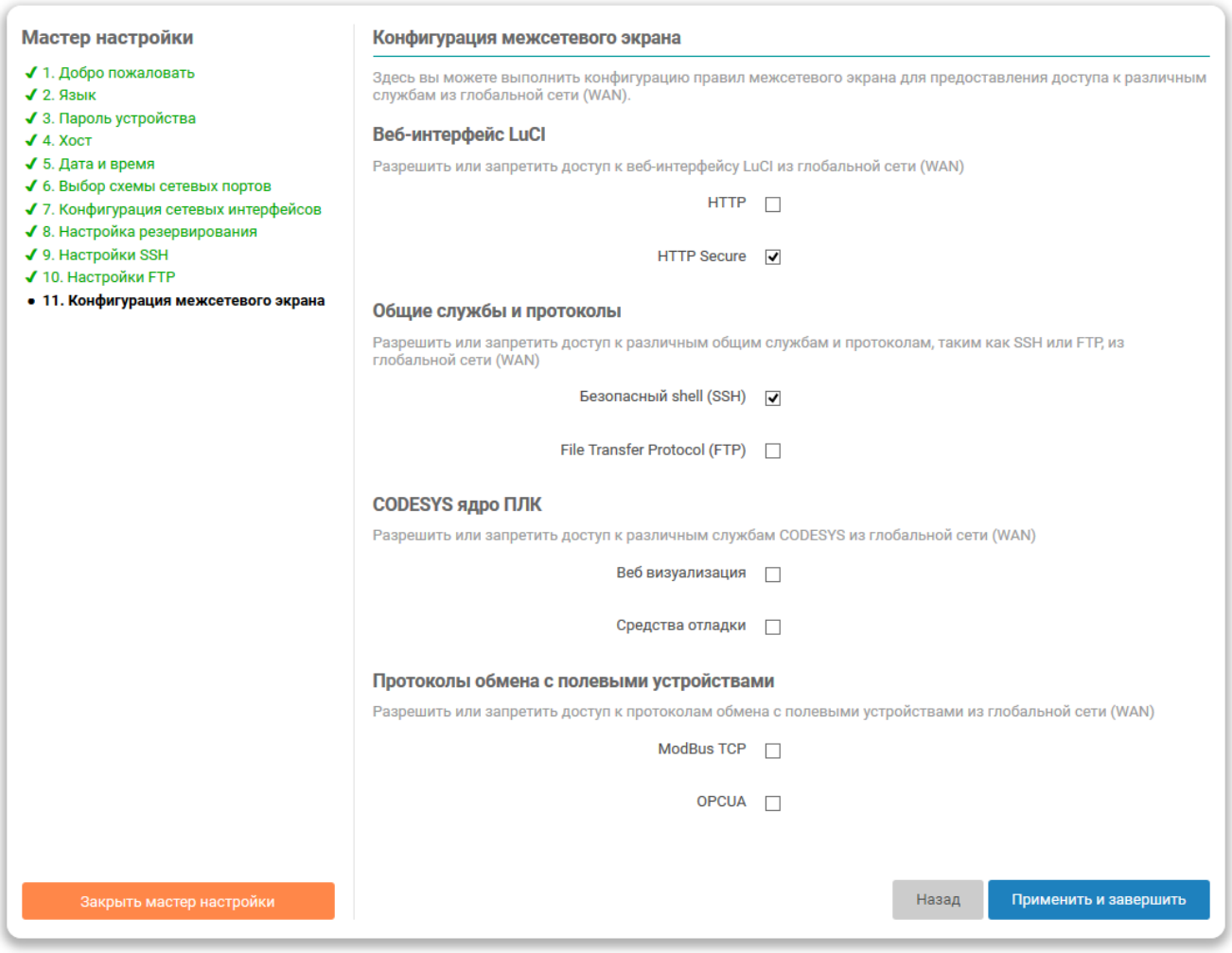


Рис. 2-34: Мастер настройки. Настройки межсетевого экрана

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

Открывая во внешнюю сеть доступ к Web-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 2.8).

Открывая во внешнюю сеть доступ по протоколу FTP, следует обязательно позаботиться о безопасном пароле (см. раздел 2.9).

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.

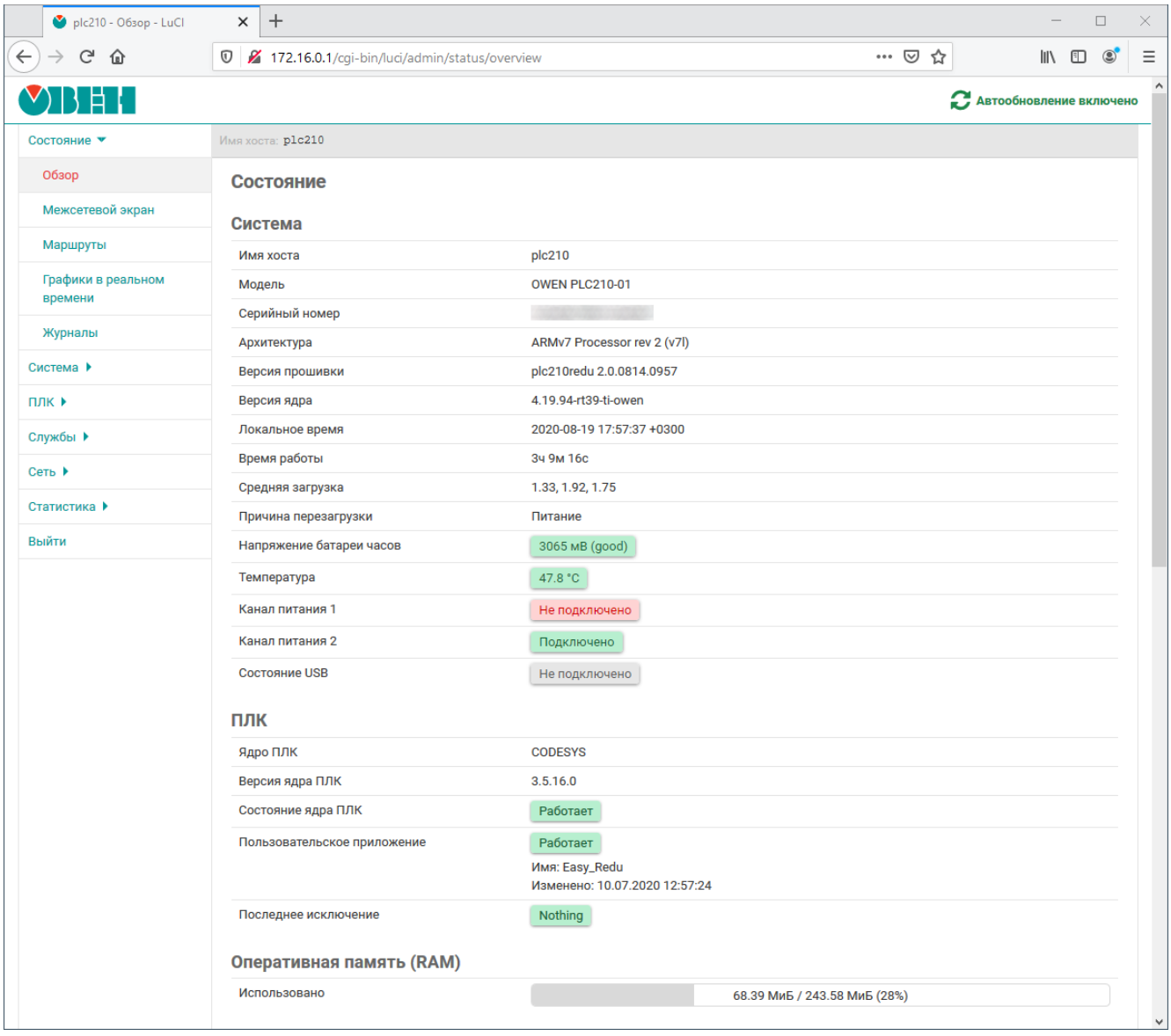


Рис. 3-1: Страница «Обзор»

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»

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].

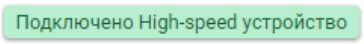


Рис. 3-3: Состояние. Подраздел «Система». Информация о скорости подключения USB устройстве

[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»

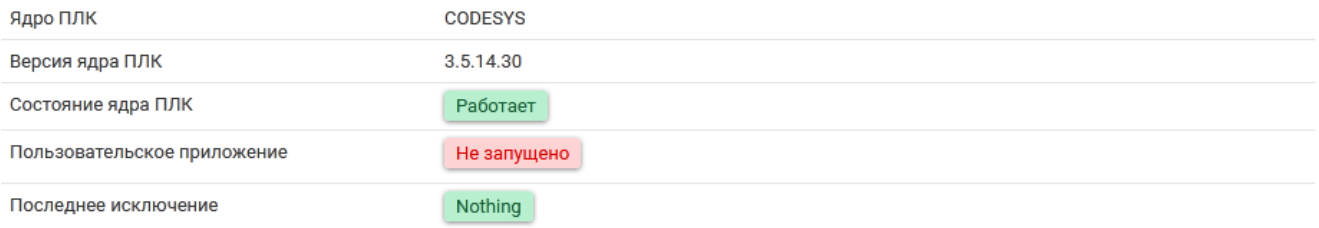


Рис. 3-5: Состояние. Подраздел «ПЛК»

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.

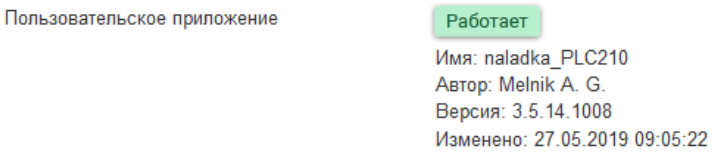


Рис. 3-6: Состояние. Подраздел «ПЛК». Информация о запущенном пользовательском приложении

- «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 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.

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 се-

тевой 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.

3.1.4.1 Режим аппаратного коммутатора на котроллерах ПЛК200

На контроллере ПЛК200 доступен режим аппаратного коммутатора (см. раздел 2.5.1). В данном режиме физические порты «Ethernet 1» и «Ethernet 2» объединены в аппаратный 3-х портовый коммутатор. Третий порт (внутренний) аппаратного коммутатора подключен к центральному процессору контроллера ПЛК200 и доступен для настройки пользователем (см. рисунок 3-9).

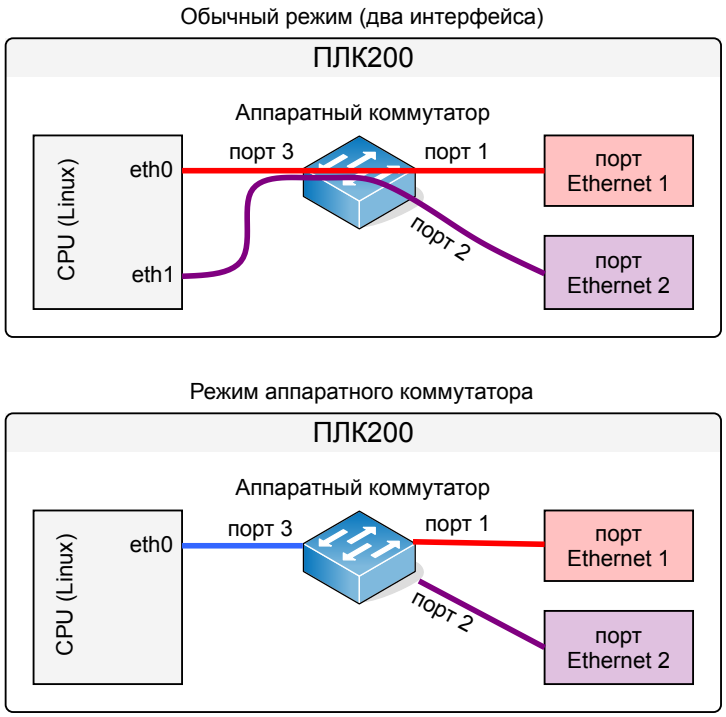


Рис. 3-9: Режимы работы коммутатора контроллера ПЛК200

В данном режиме таблица портов сетевых интерфейсов страницы «Обзор», будет выглядеть, как показано на рисунке 3-10.

Имя и MAC-адрес	Состояние подключения	Интерфейс	В составе моста	Зоны межсетевого экрана	Получение (RX)	Передача (TX)
CPU 38:0B:3C:25:89:8F	100 Мбит/с, полный дуплекс	eth0 (LAN)	–	lan	39.01 КиБ (237 пакетов)	101.57 КиБ (257 пакетов)
Ethernet 1	100 Мбит/с, полный дуплекс	–	Аппаратный коммутатор	–	–	–
Ethernet 2	Не подключено	–	Аппаратный коммутатор	–	–	–
USB RNDIS 38:0B:3C:25:89:91	Не подключено	usb0 (USB0)	–	–	–	–

Рис. 3-10: Состояние портов сетевых интерфейсов контроллера ПЛК200 в режиме аппаратного коммутатора

Порты «Ethernet 1» и «Ethernet 2» будут помечены как «Аппаратный коммутатор». Статистика полученных и принятых данных для этих портов не выводится в связи с аппаратными ограничениями режима работы коммутатора.

Третий порт аппаратного коммутатора в таблице отображается в первой строке с именем «CPU». В системе данный порт представлен системным интерфейсом eth0.

3.1.5 Подраздел «Сеть»

В подразделе «Сеть» страницы «Обзор» приводится информация об основных сетевых интерфейсах в виде блоков, как показано на рисунке 3-11.

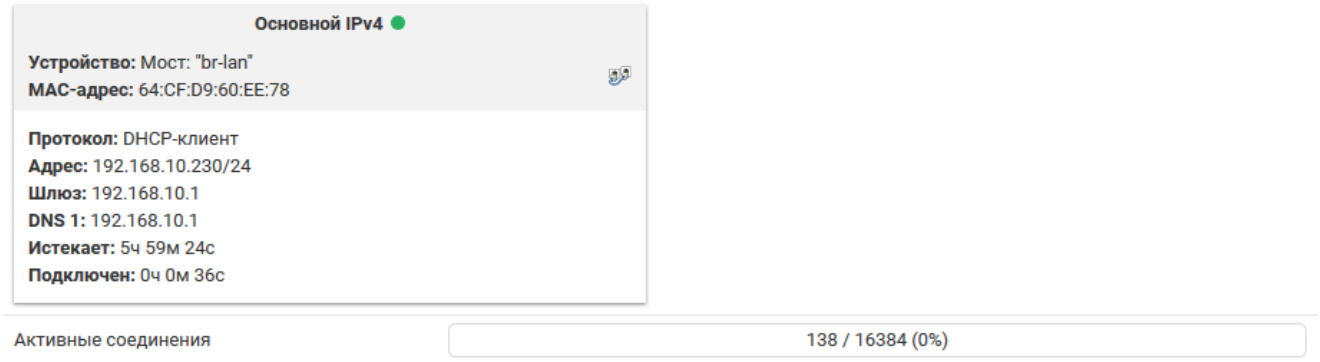


Рис. 3-11: Состояние. Подраздел «Сеть»

Кроме того, внизу подраздела «Сеть» страницы «Обзор» отображается текущее и максимально возможное количество сетевых соединений в виде шкалы (см рисунок 3-11).

3.1.6 Подраздел «Активные DHCP аренды»

В подразделе «Активные DHCP аренды» страницы «Обзор» приводится таблица активных арендованных DHCP адресов (см. рисунок 3-12).

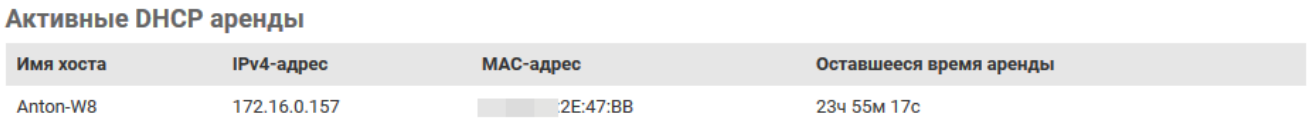


Рис. 3-12: Состояние. Подраздел «Активные DHCP аренды»

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 3-13.

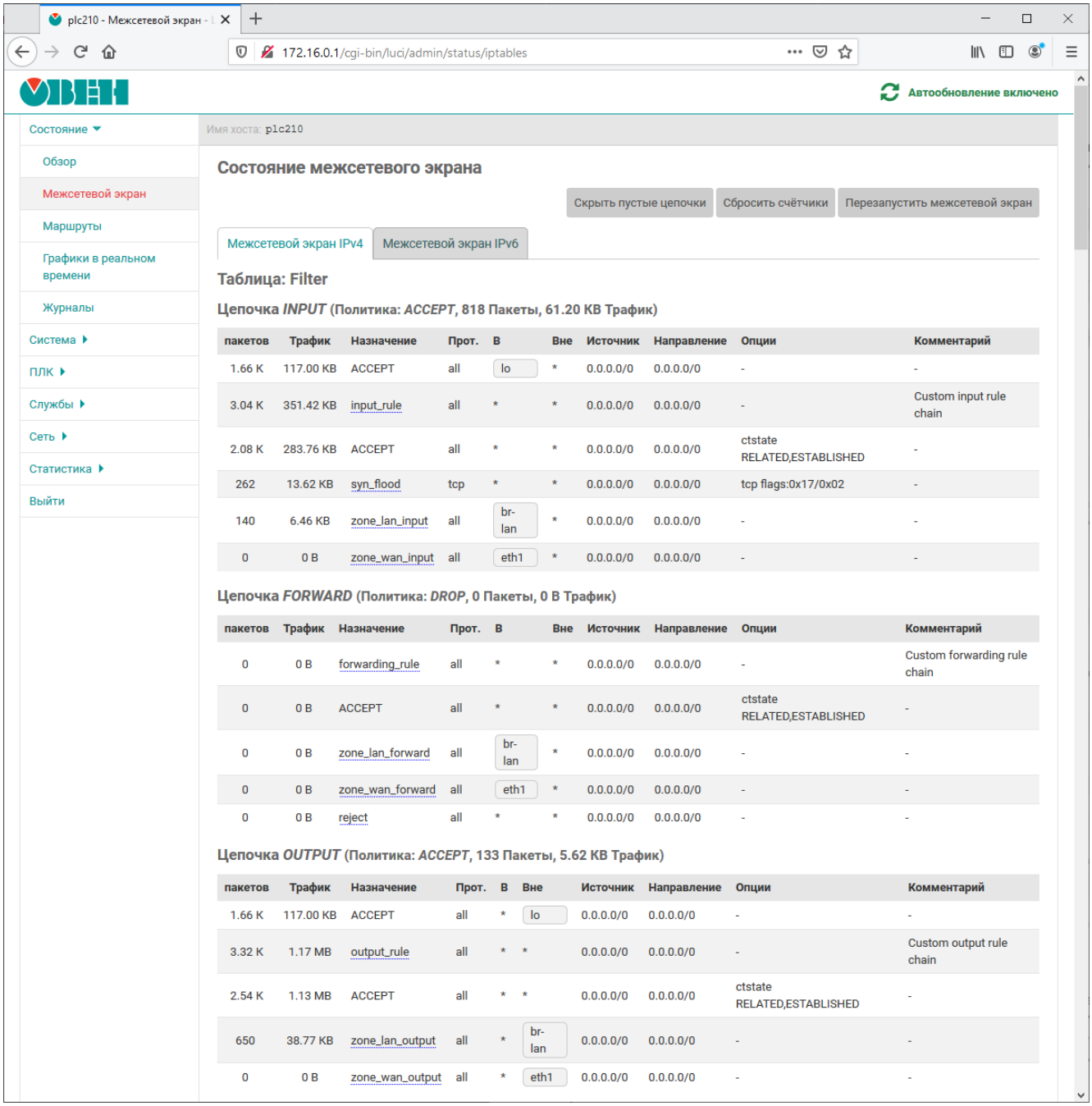


Рис. 3-13: Страница «Межсетевой экран»

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 3-14.

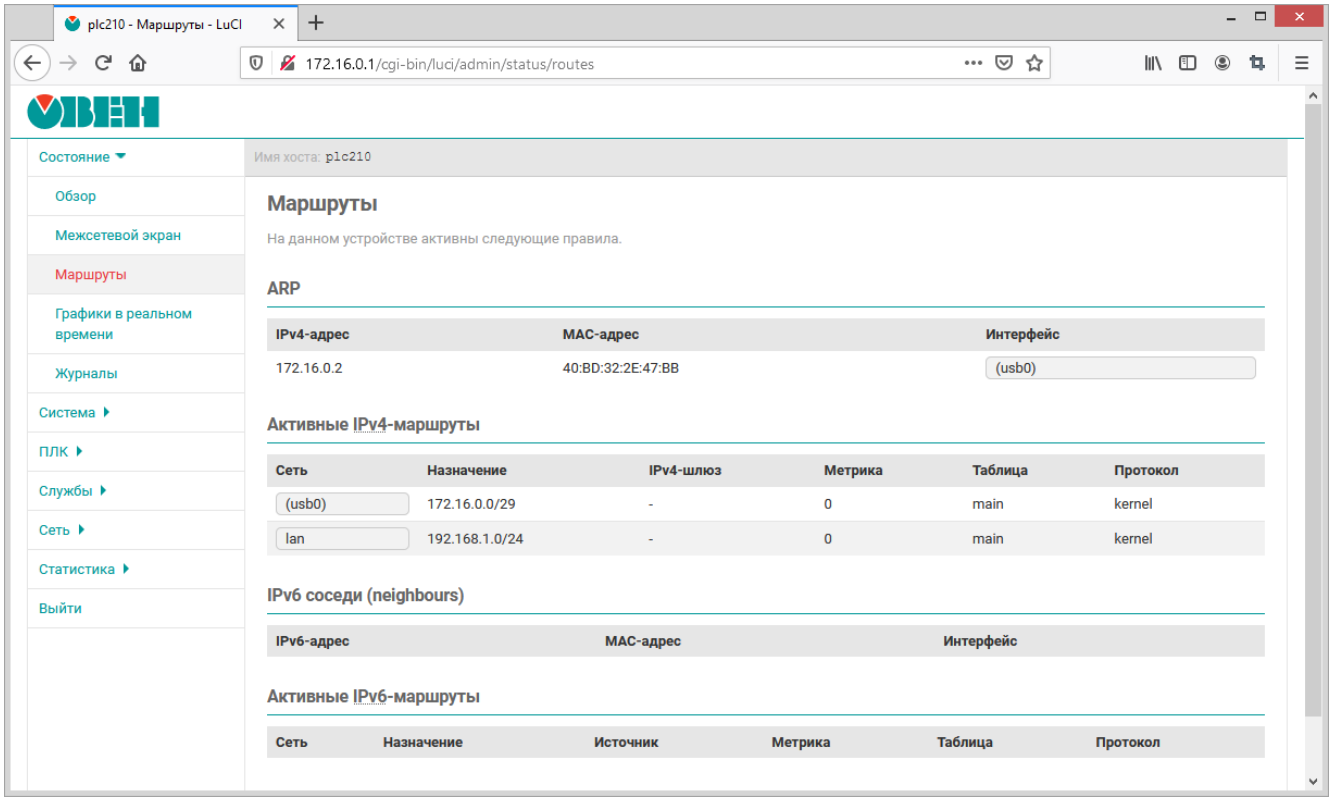


Рис. 3-14: Страница «Маршруты»

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

3.4 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.

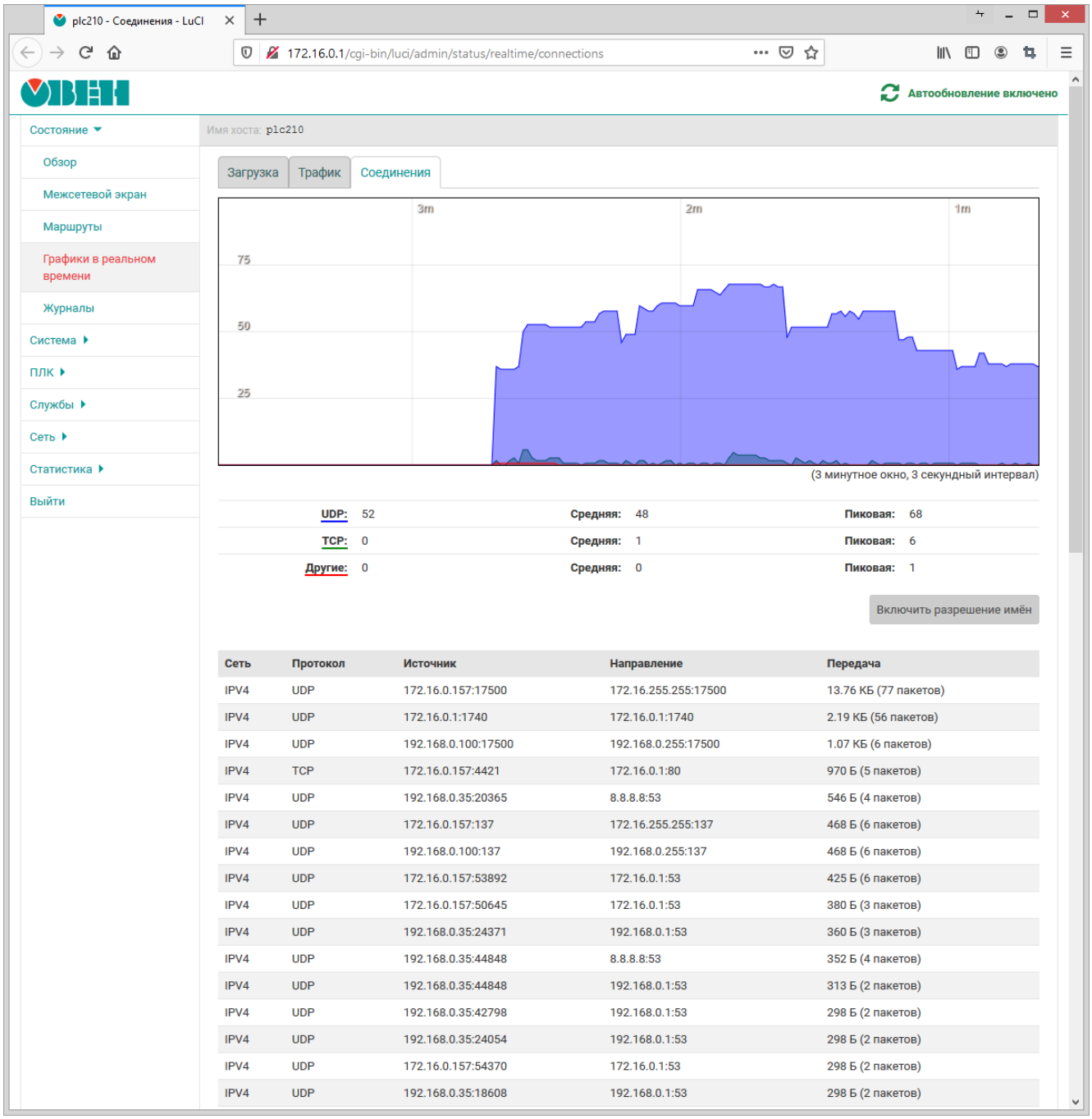


Рис. 3-15: Страница «Графики в реальном времени». График активных соединений

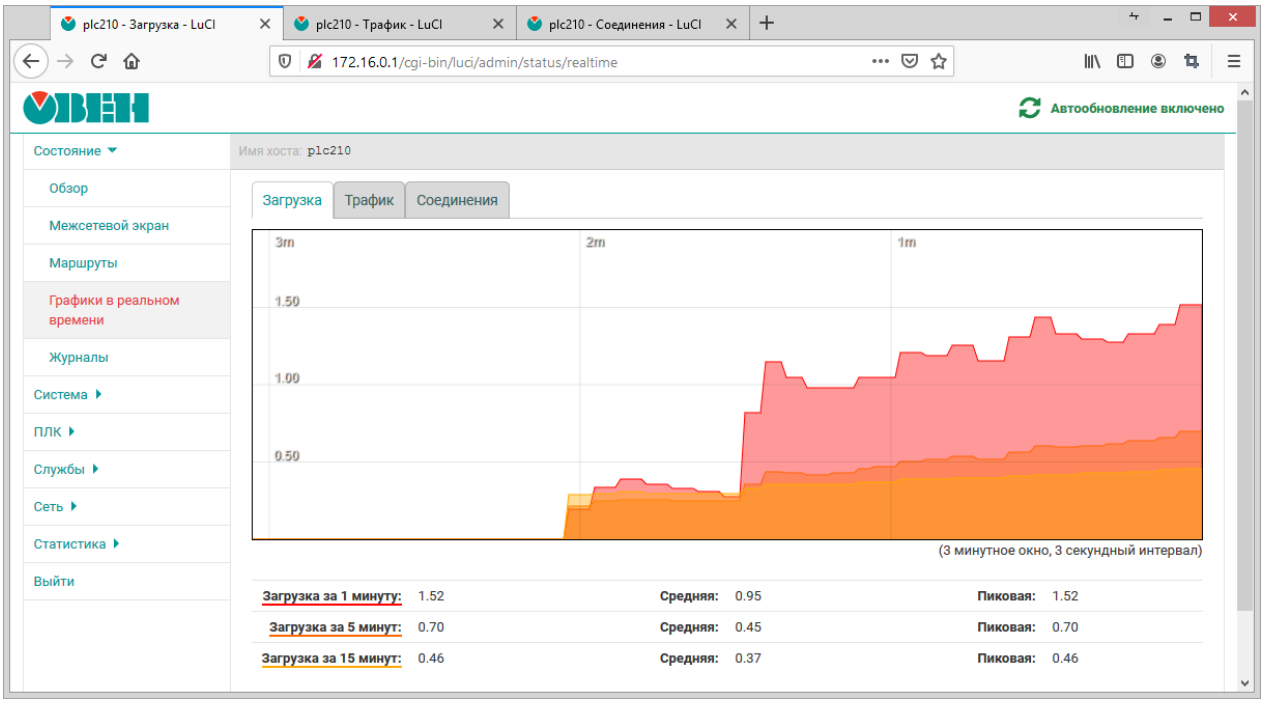


Рис. 3-16: Страница «Графики в реальном времени». График загрузки

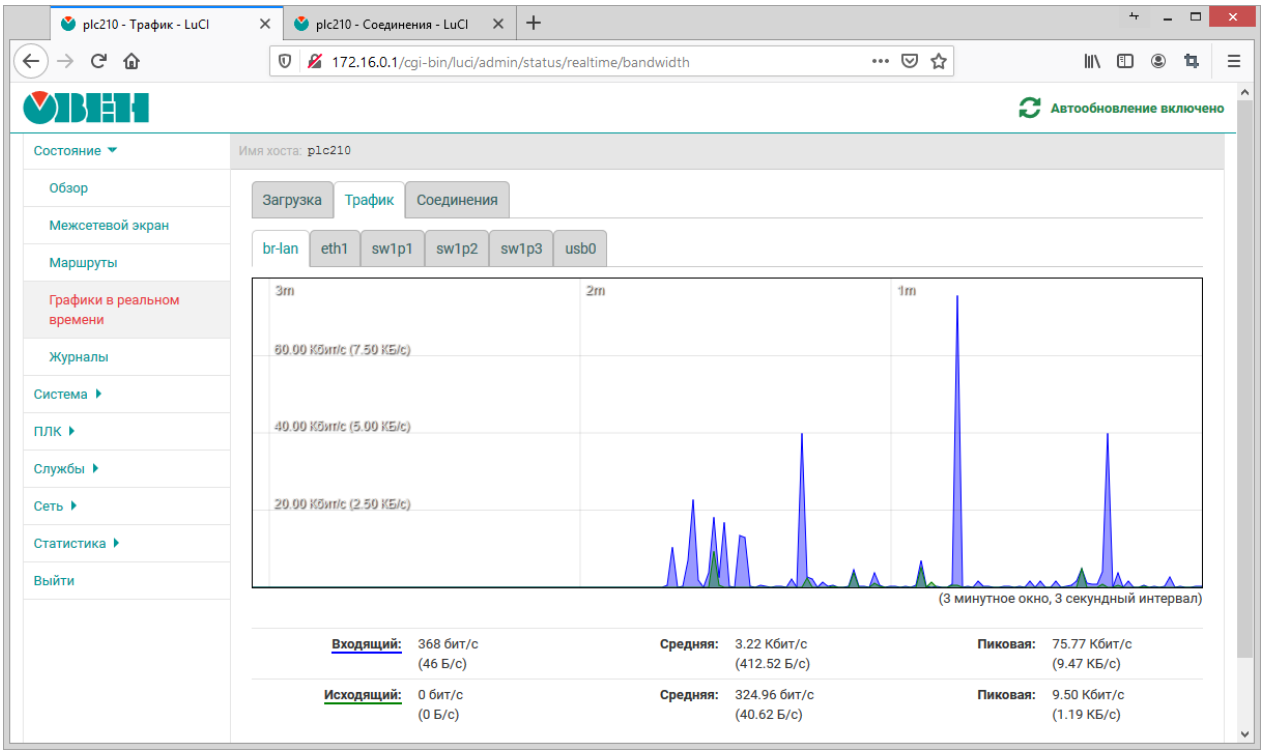


Рис. 3-17: Страница «Графики в реальном времени». График трафика моста «br-lan»

3.5 Журналы

На странице «Журналы» раздела «Состояние» отображаются записи следующих журналов:

- вкладка «Журнал ядра» — журнал ядра (см. раздел 3.5.1);
- вкладка «Системный журнал» — системный журнал (см. раздел 3.5.2).

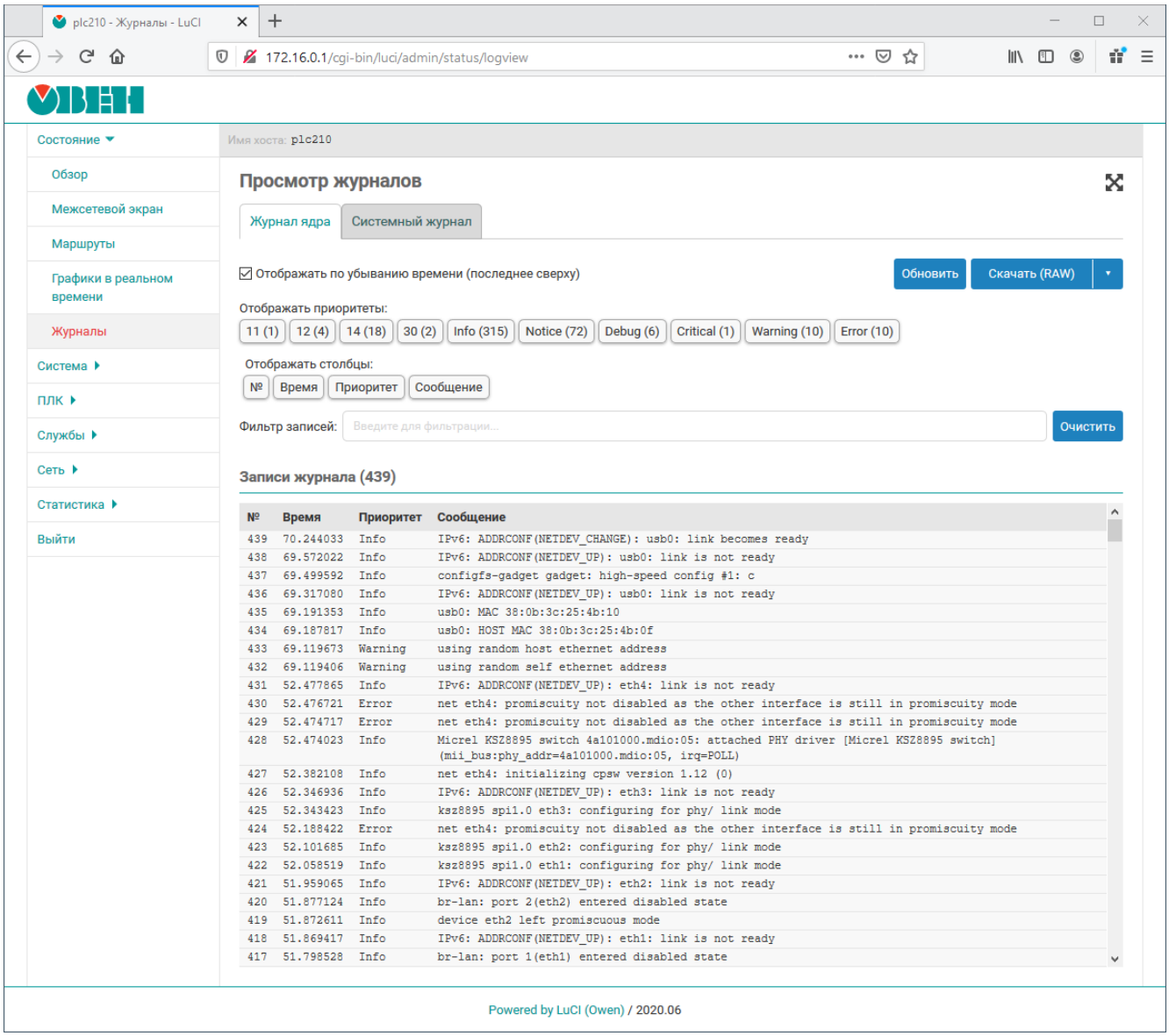


Рис. 3-18: Вкладка «Журнал ядра»

Переключение между журналами осуществляется при помощи вкладок в верхней части страницы (см. рисунок 3-18).

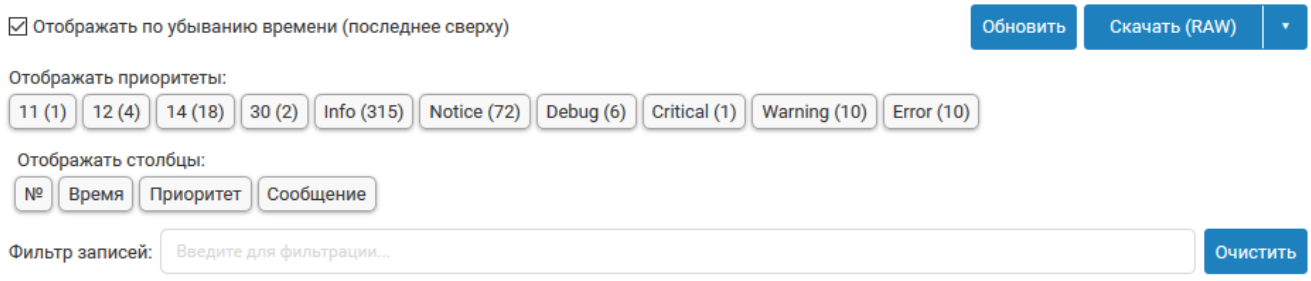


Рис. 3-19: Страницы «Журналы». Элементы управления просмотром журналов

Страница каждого журнала в верхней части содержит область со следующими элементами управления (см. рисунок 3-19):

- переключатель «Отображать по убыванию времени (последнее сверху)» — позволяет переключить режим сортировки записей. При включенном переключателе записи журнала отображаются по убыванию времени регистрации, последняя запись всегда сверху (режим отображения по умолчанию). Если переключатель выключен, то записи отображаются по возрастанию времени регистрации, последняя запись всегда снизу;
- кнопка «Обновить» — выполняет повторное чтение записей из соответствующего журнала с обновлением записей в таблице на странице;
- кнопка «Скачать (<*формат*>)» — позволяет выполнить скачивание файла журнала в требуемом формате. Доступные форматы:
  - «RAW» — простой текстовый формат (исходный формат);
  - «CSV» — текстовый формат CSV;
  - «JSON» — текстовый формат JSON;
- кнопки-переключатели «Отображать приоритеты» — позволяют включить или выключить отображение записей определенных приоритетов;
- кнопки-переключатели «Отображать столбцы» — позволяют включить или выключить отображение соответствующих столбцов в таблице записей журнала;
- поле ввода «Фильтр» — позволяет выполнить фильтрацию отображаемых записей журнала по заданному шаблону (см. рисунок 3-20).
- кнопка «Очистить» — кнопка очистки введённого шаблона фильтра в поле ввода «Фильтр».

3.5.1 Журнал ядра

Во вкладке «Журнал ядра» страницы «Журналы» раздела «Состояние» отображаются записи системного журнала, в который записываются сообщения работы ядра Linux, начиная с момента загрузки. Пример внешнего вида вкладки «Журнал ядра» показан на рисунках 3-18 и 3-20.

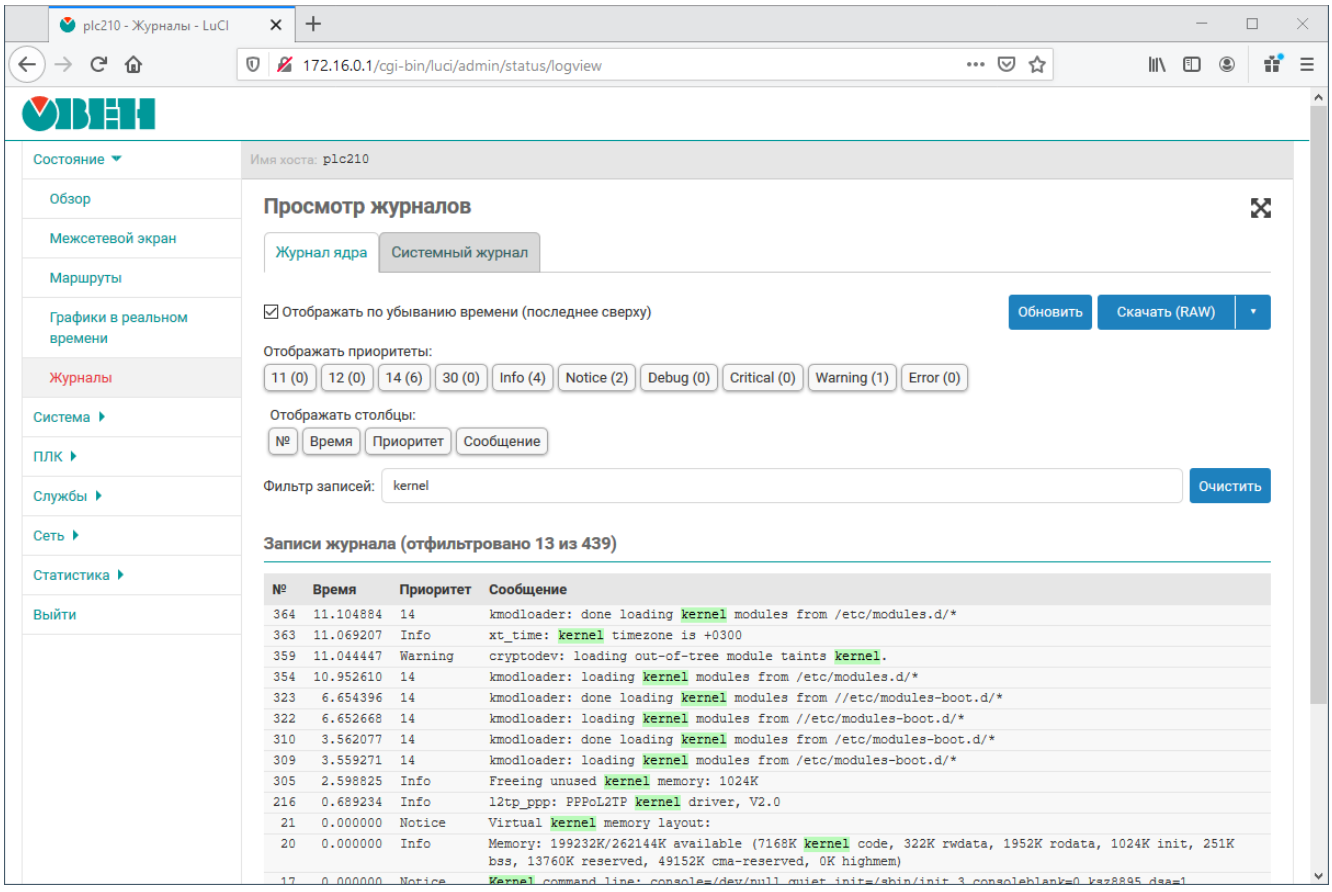


Рис. 3-20: Вкладка «Журнал ядра». Применение фильтра записей

3.5.2 Системный журнал

Во вкладке «Системный журнал» страницы «Журналы» раздела «Состояние» отображаются записи системного журнала, в который записываются все события ядра Linux, приложений и служб, запущенных в системе. Пример внешнего вида вкладки «Системный журнал» показан на рисунке 3-21.

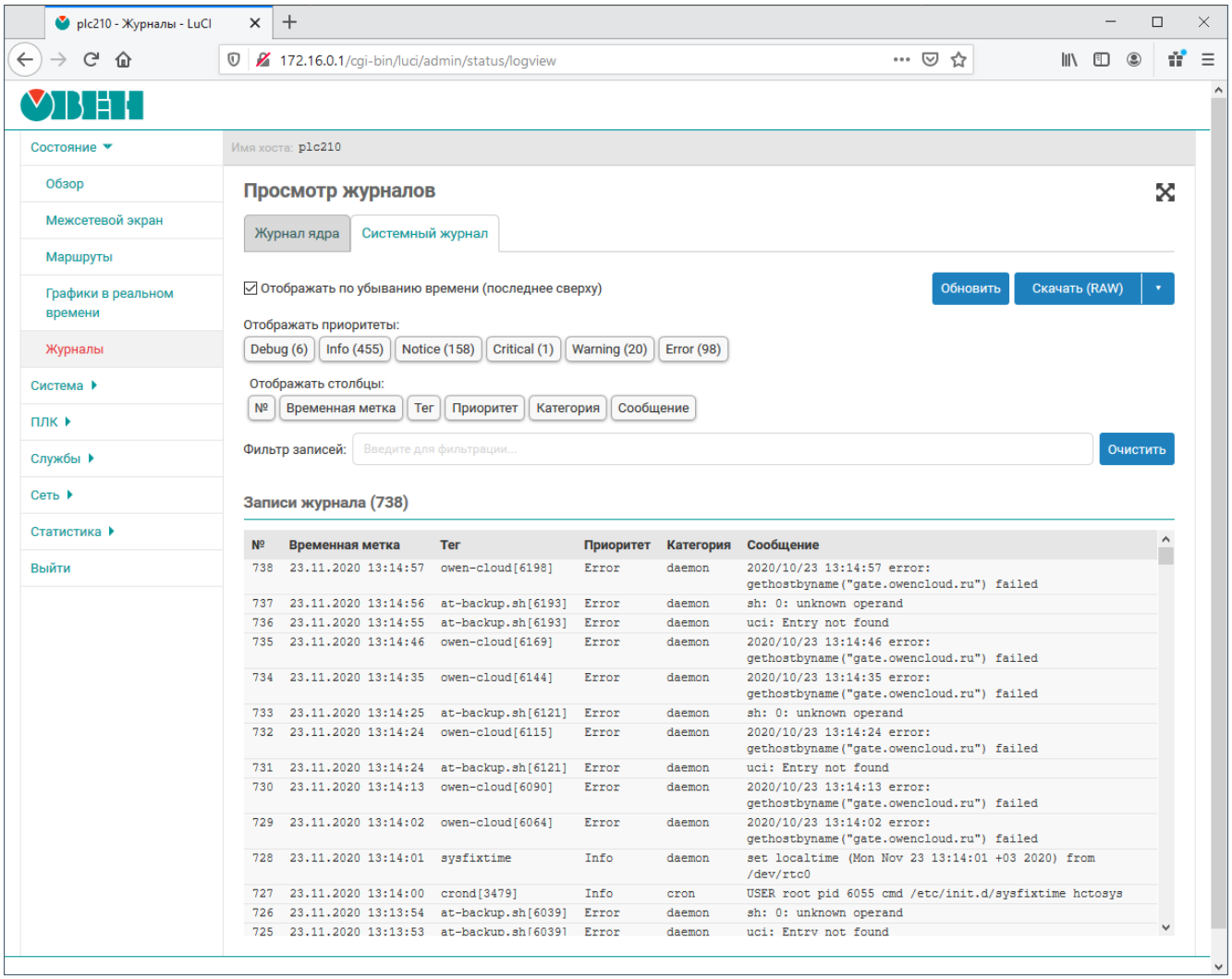


Рис. 3-21: Вкладка «Системный журнал»

Основным отличием журнала ядра (см. раздел 3.5.1) от системного журнала является то, что в журнале ядра не регистрируются какие-либо события от приложений и служб уровня пользователя.

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.

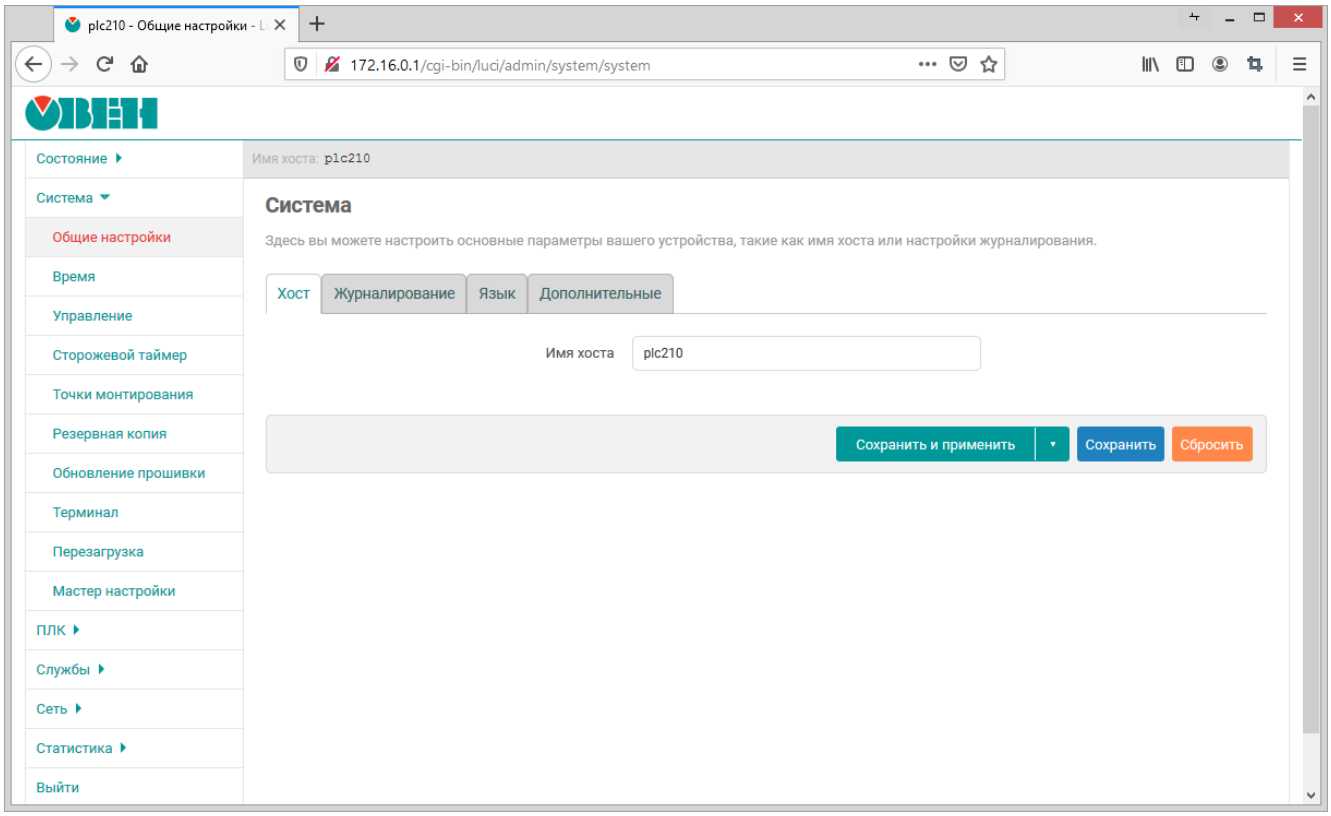


Рис. 4-1: Страница «Общие настройки»

4.1.1 Вкладка «Хост»

Вкладка «Хост» позволяет настроить имя хоста системы.

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

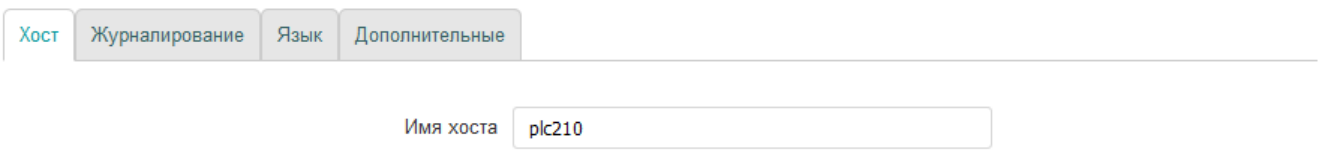


Рис. 4-2: Страница «Общие настройки». Вкладка «Хост»

4.1.2 Вкладка «Журналирование»

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

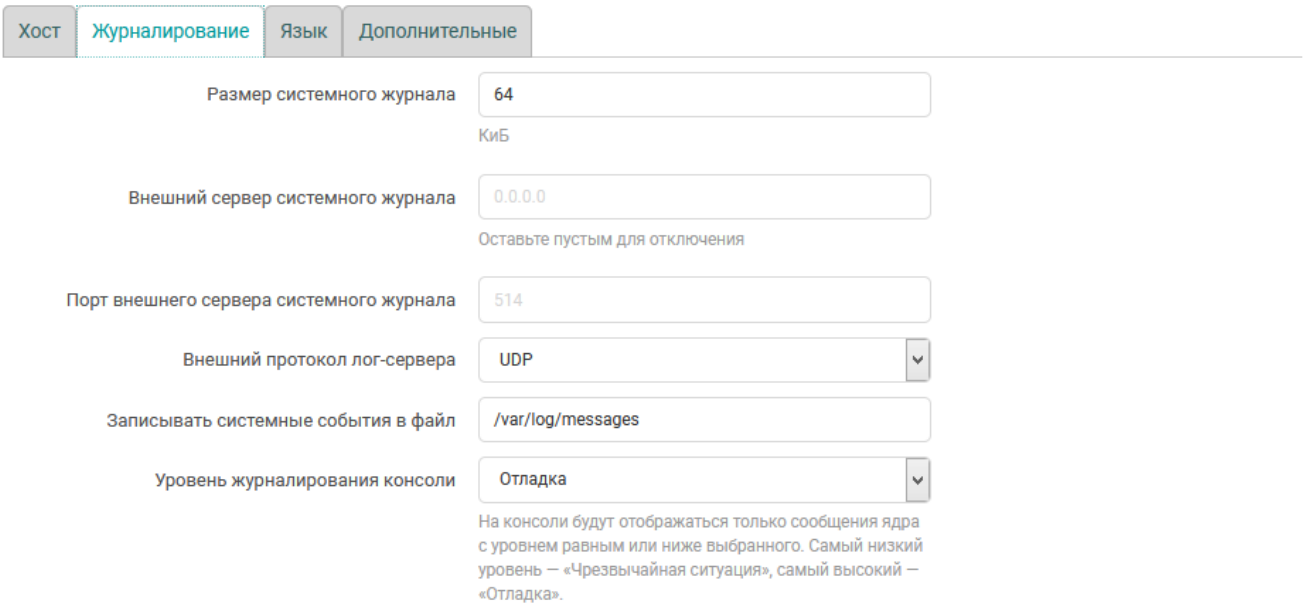


Рис. 4-3: Страница «Система». Вкладка «Журналирование»

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;
- «Уровень журналирования консоли» — на консоли будут отображаться только сообщения ядра с уровнем равным или ниже выбранного. Самый низкий уровень — «Чрезвычайная ситуация», самый высокий — «Отладка» Для выбора доступны следующие уровни:
  - «Отладка» (debug);
  - «Информация» (information);
  - «Заметка» (notice);
  - «Предупреждение» (warning);
  - «Ошибка» (error);
  - «Критическая ситуация» (critical);
  - «Тревога» (alarm);
  - «Чрезвычайная ситуация» (emergency);

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.

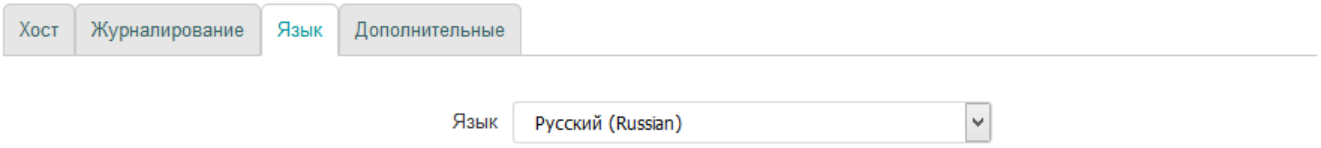


Рис. 4-4: Страница «Система». Вкладка «Язык»

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.

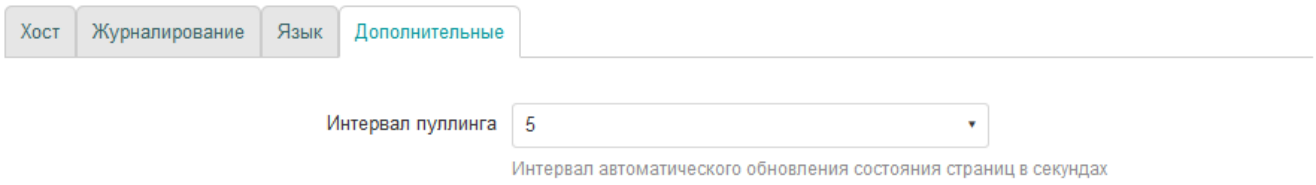


Рис. 4-5: Страница «Система». Вкладка «Дополнительные»

Настройка «Интервал пуллинга» определяет интервал автоматического обновления информации на страницах, поддерживающих данную возможность. Более подробная информация о функции автоматического обновления содержится в разделе 1.4.

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.

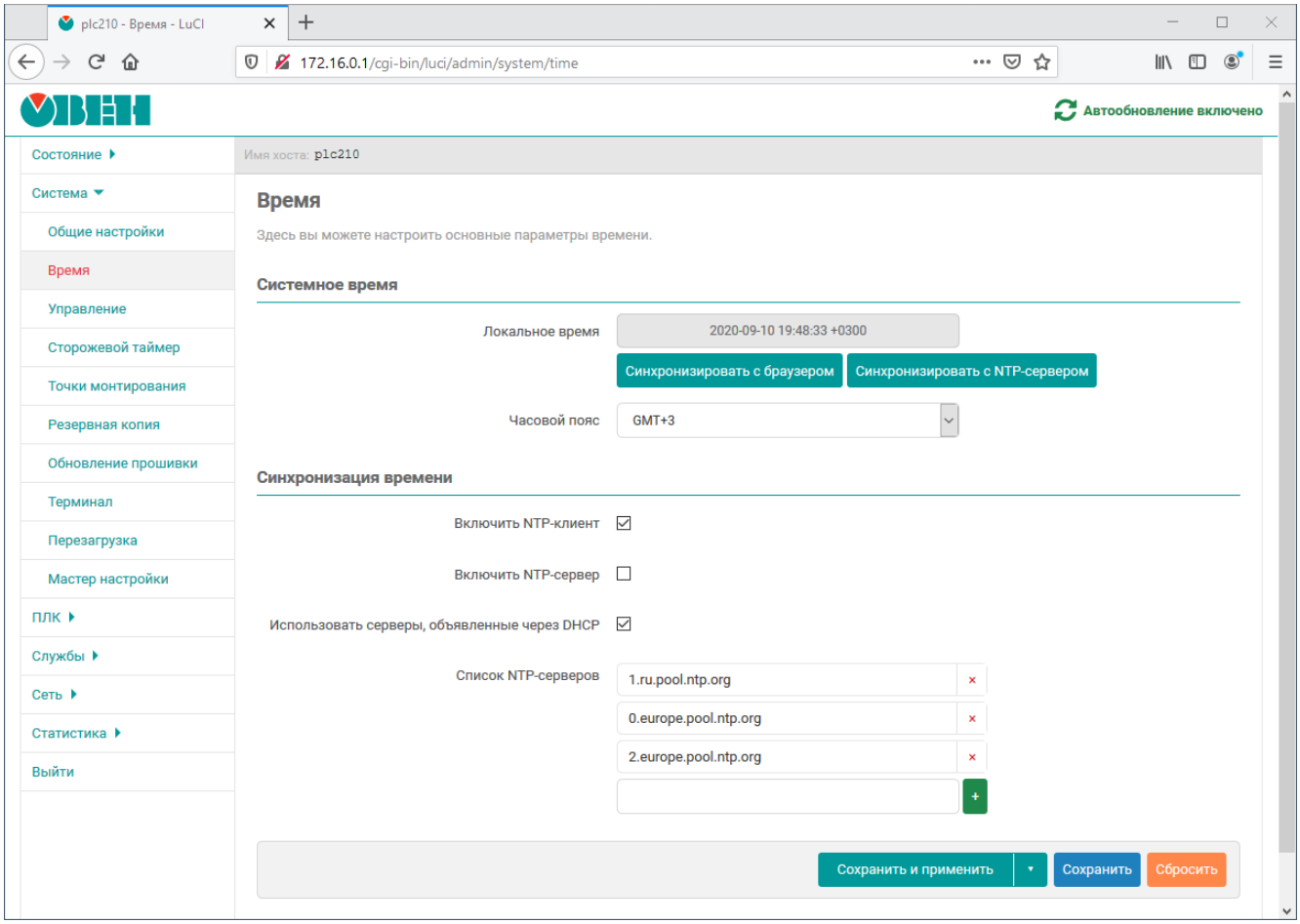


Рис. 4-6: Страница «Время»

В поле «Дата и время» отображается текущее локальное время и дата.

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

Кнопка «Синхронизировать с NTP-сервером» выполняет установку локальной даты и времени на устройстве с использованием NTP-клиента.

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.

При включении опции «Использовать серверы, объявленные через DHCP» для синхронизации времени будут использованы серверы, объявленные DHCP сервером (опция 42), который выдал устройству параметры конфигурации 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).

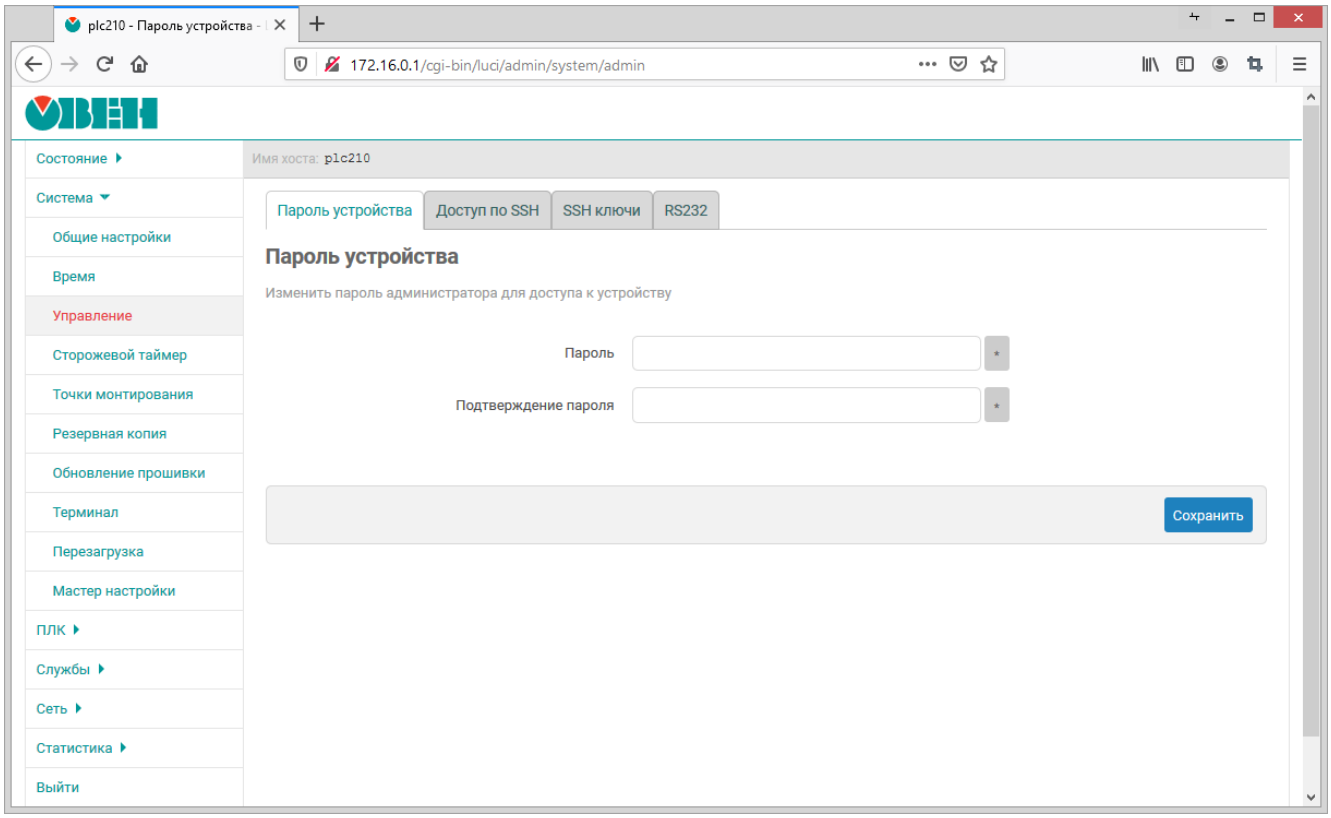


Рис. 4-7: Страница «Управление». Вкладка «Пароль маршрутизатора»

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.

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:

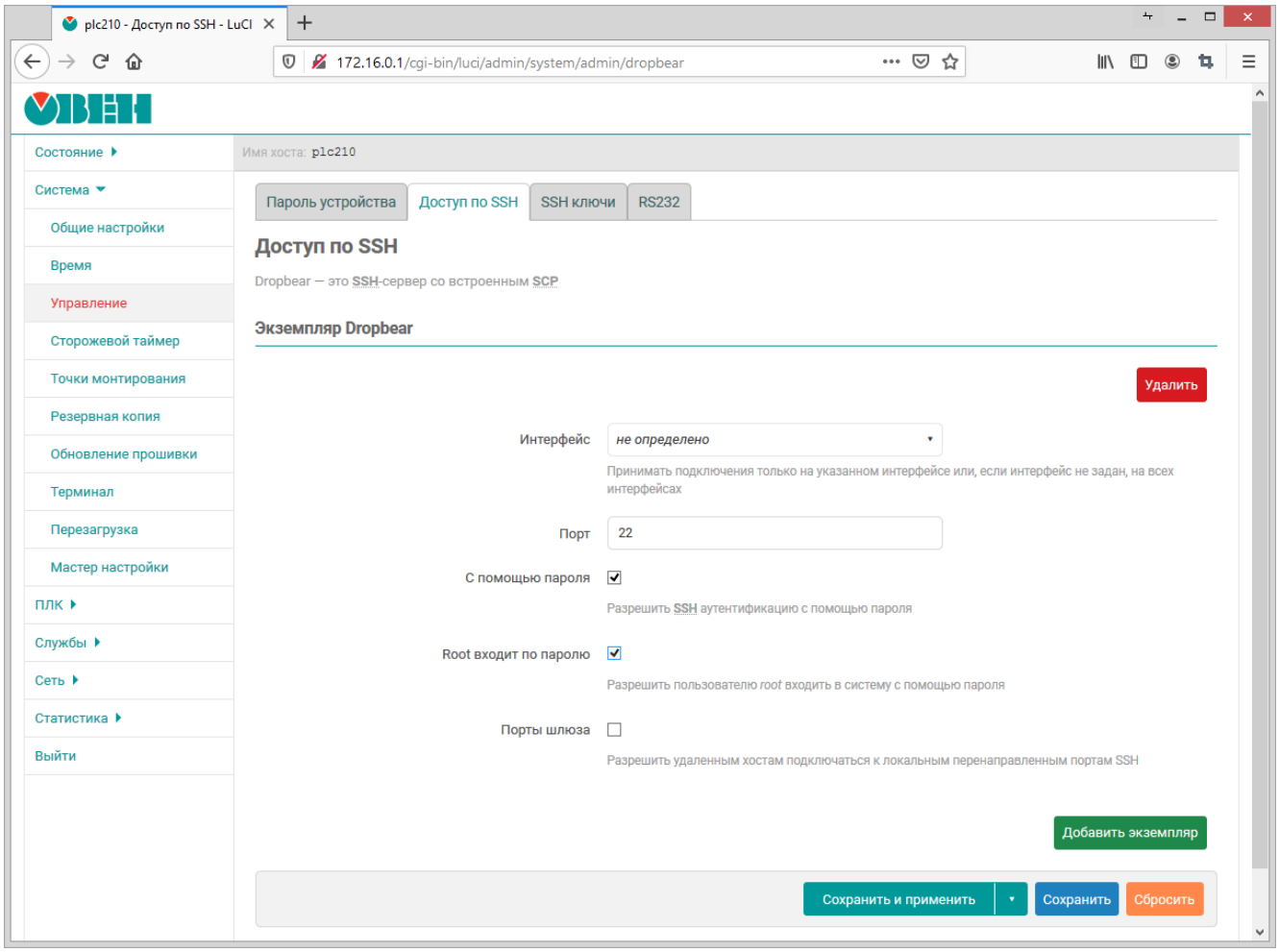


Рис. 4-8: Страница «Управление». Вкладка «Доступ по SSH»

- «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.

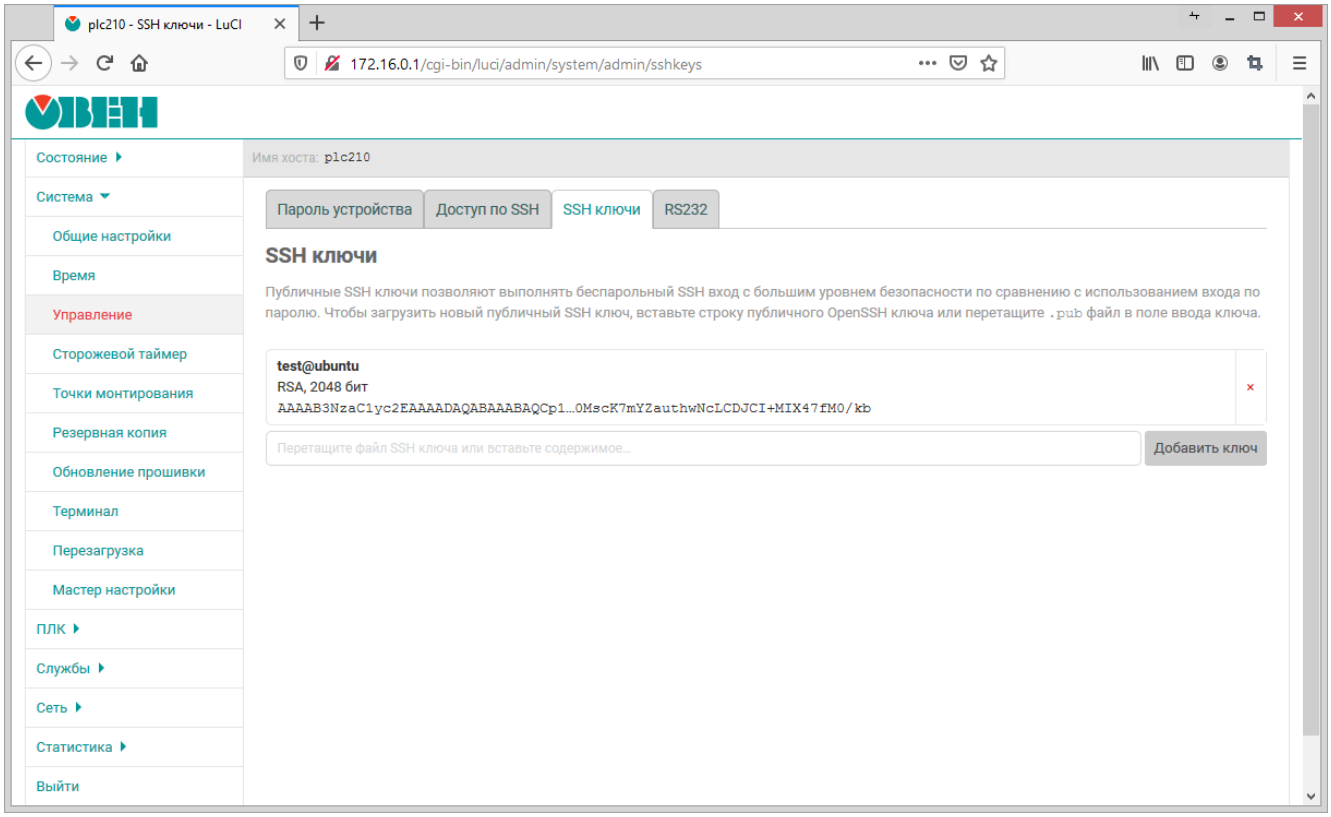


Рис. 4-9: Страница «Управление». Вкладка «SSH-ключи»

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.

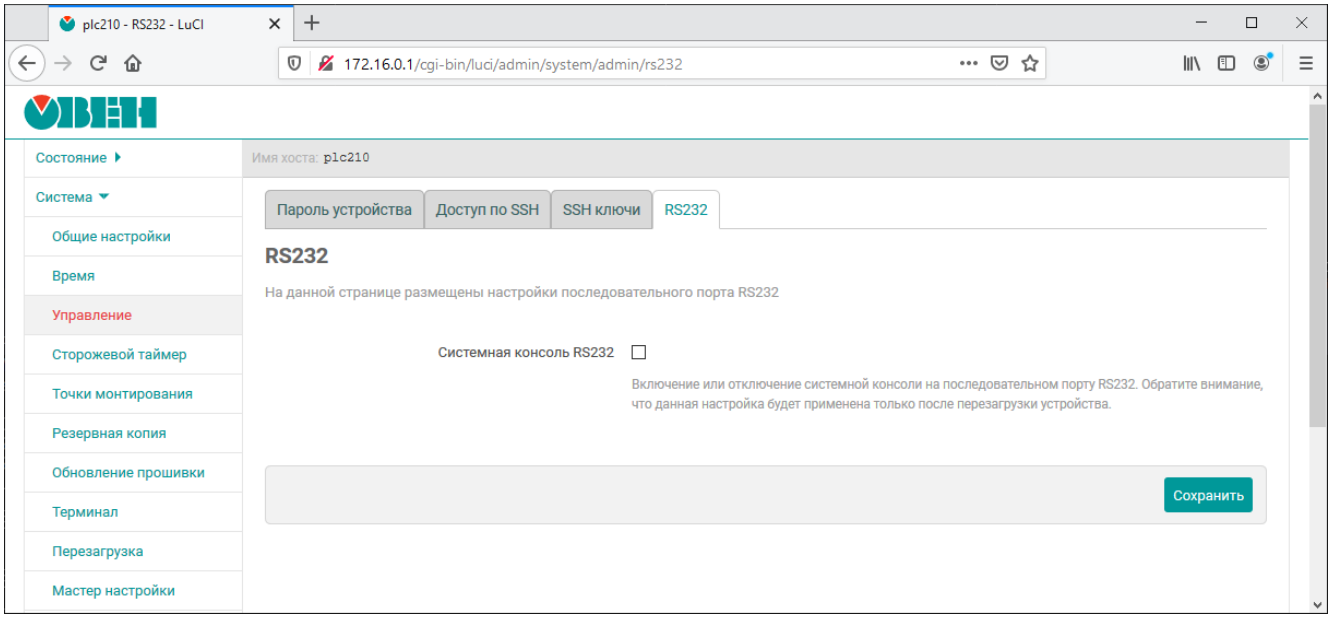


Рис. 4-10: Страница «Управление». Вкладка «RS232»

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.

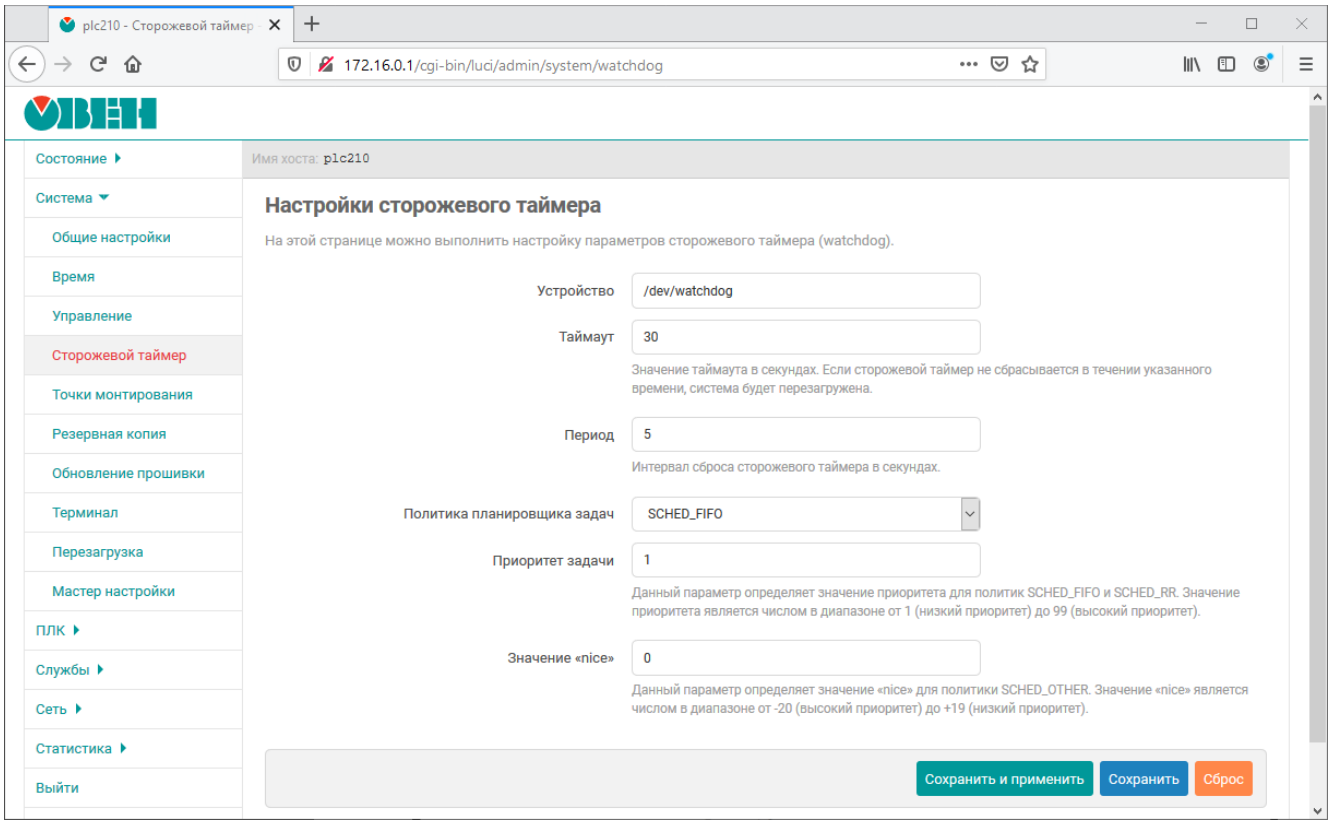


Рис. 4-11: Страница «Сторожевой таймер»

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 Точки монтирования

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

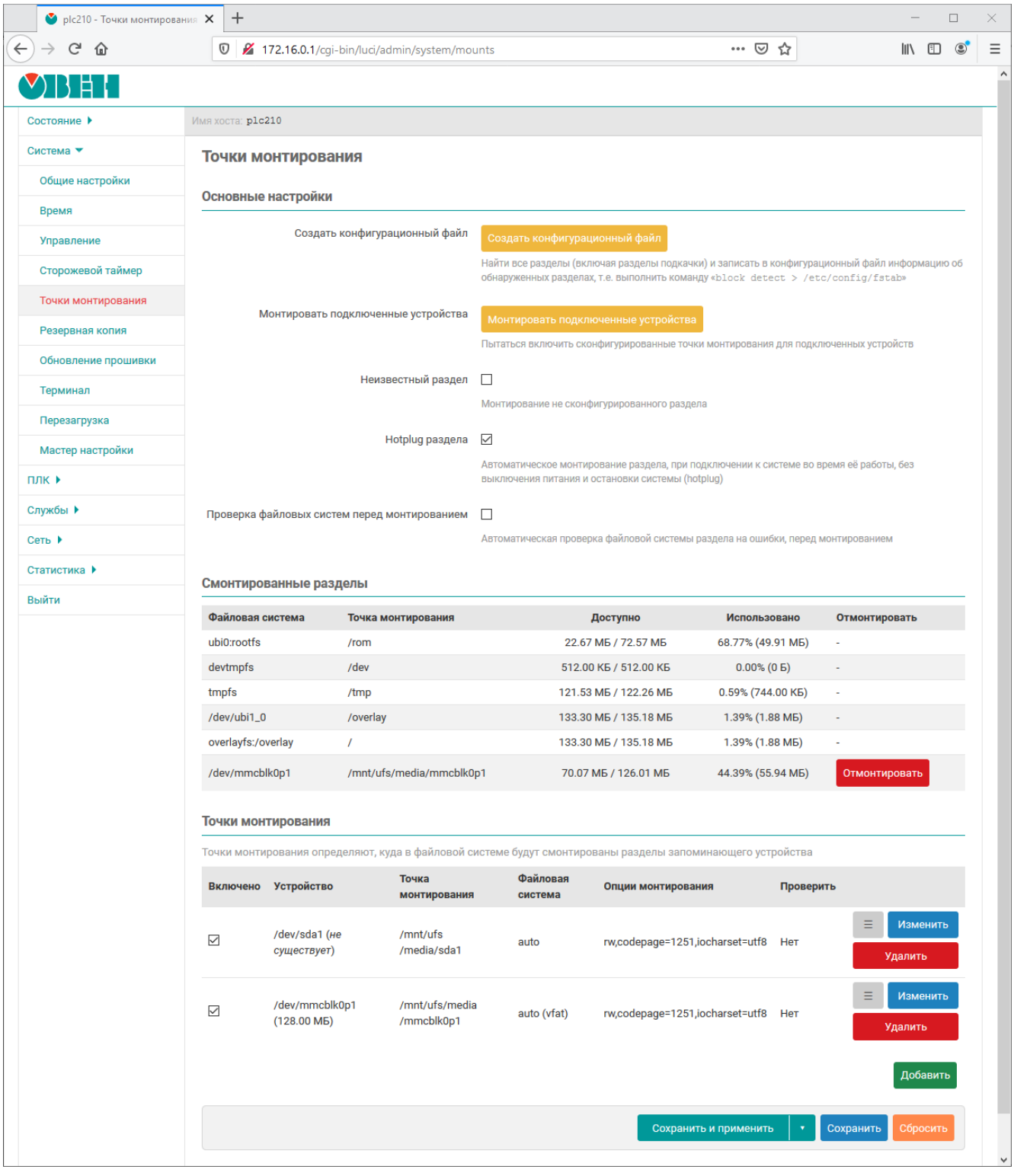


Рис. 4-12: Страница «Точки монтирования»

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

Все настройки на странице «Точки монтирования» разделены на три подраздела:

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

4.5.1 Подраздел «Глобальные настройки»

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

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

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

- Кнопка «Монтировать подключённые устройства» — выполняет монтирование текущих сконфигурированных подключённых устройств.
- «Неизвестный раздел» — автоматическое монтирование разделов, даже если эти разделы явно не указаны в конфигурации подраздела «Точки монтирования» (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 «Точки монтирования» (см. раздел 4.5.3).

  Если подключённый раздел не перечислен в таблице раздела «Точки монтирования», 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 «Точки монтирования» приведена текущая таблица монтирования (см. рисунок 4-13).

Смонтированные разделы

Файловая система	Точка монтирования	Доступно	Использовано	Отмонтировать
ubi0:rootfs	/rom	22.67 МБ / 72.57 МБ	68.77% (49.91 МБ)	-
devtmpfs	/dev	512.00 КБ / 512.00 КБ	0.00% (0 Б)	-
tmpfs	/tmp	121.18 МБ / 122.26 МБ	0.89% (1.08 МБ)	-
/dev/ubi1_0	/overlay	129.97 МБ / 131.93 МБ	1.49% (1.96 МБ)	-
overlayfs:/overlay	/	129.97 МБ / 131.93 МБ	1.49% (1.96 МБ)	-
/dev/mmcblk0p1	/mnt/ufs/media/mmcblk0p1	70.07 МБ / 126.01 МБ	44.39% (55.94 МБ)	Отмонтировать

Рис. 4-13: Страница «Точки монтирования». 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 «Точки монтирования»

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

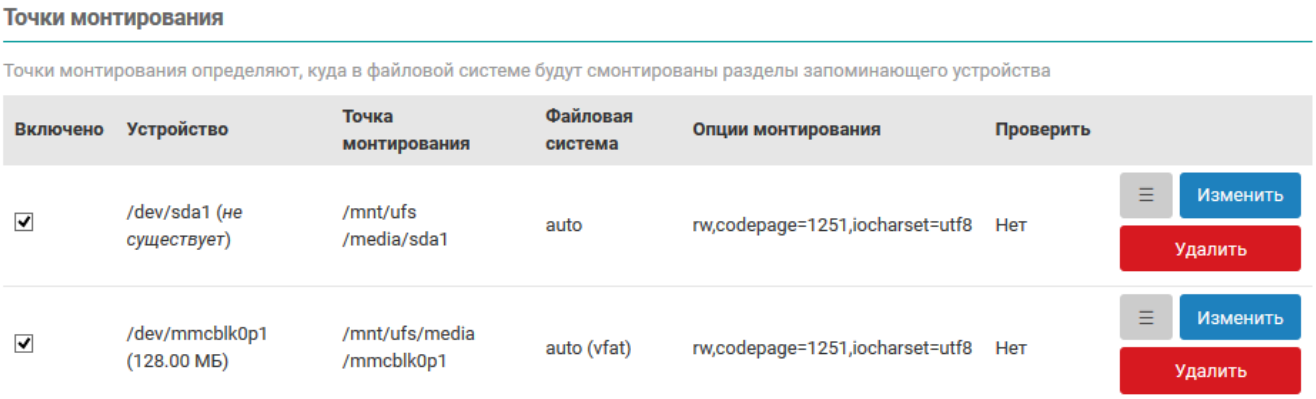


Рис. 4-14: Страница «Точки монтирования». Управление монтированием пользовательских разделов

В разделе приведена таблица уже созданных (сконфигурированных) 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 подключении соответствующих устройств 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 монтирования» — дополнительные опции, передаваемые утилите mount [7] при монтировании.
- «Проверить» — определяет, будет ли выполнена проверка файловой системы раздела при монтировании.

4.5.3.1 Редактирование точки монтирования

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

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

Во вкладке «Общие настройки» размещены следующие настройки:

- «Включено» — определяет включена ли данная точка монтирования.
- «UUID» — если выбрана данная опция, то монтируемый раздел будет идентифицироваться по выбранному UUID.

  Возможен ручной ввод UUID или выбор из списка UUID всех подключённых разделов на момент загрузки страницы.
- «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.

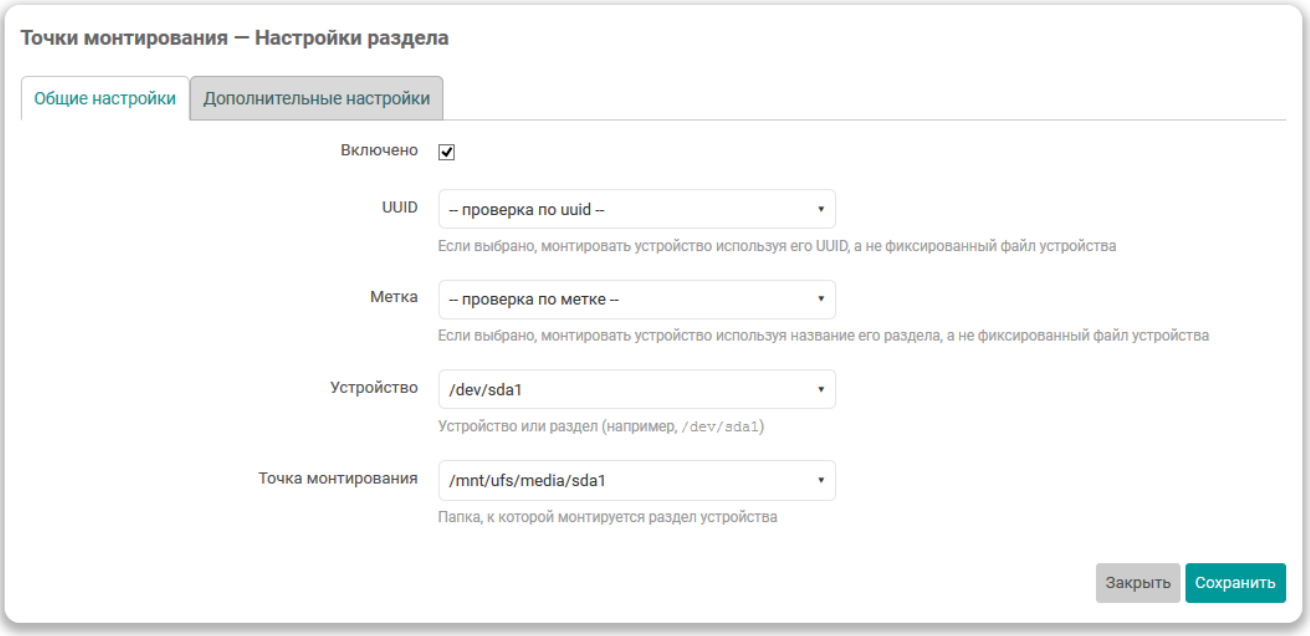


Рис. 4-15: Общие настройки точки монтирования раздела

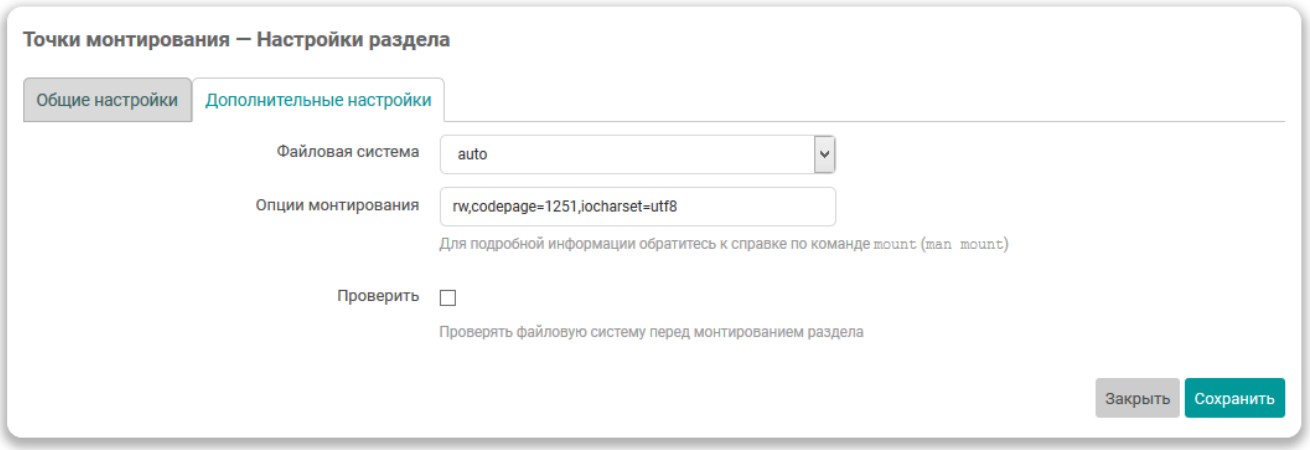


Рис. 4-16: Дополнительные настройки точки монтирования раздела

- «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
```

- «Проверить» — определяет, будет ли выполнена проверка файловой системы раздела при монтировании.

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 такое же окно 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 правой части строки соответствующего раздела таблицы точек монтирования (см. рисунок 4-14).

4.6 Резервное копирование

На странице «Резервная копия» раздела «Система» расположены настройки, связанные с созданием и восстановлением резервной копии файлов конфигурации устройства. Настройка списка сохраняемых файлов описана в разделе 4.6.2. Кроме того, на данной странице можно выполнить сброс устройства к заводским настройкам (factory reset).

Внешний вид страницы «Резервная копия» показан на рисунке 4-17.

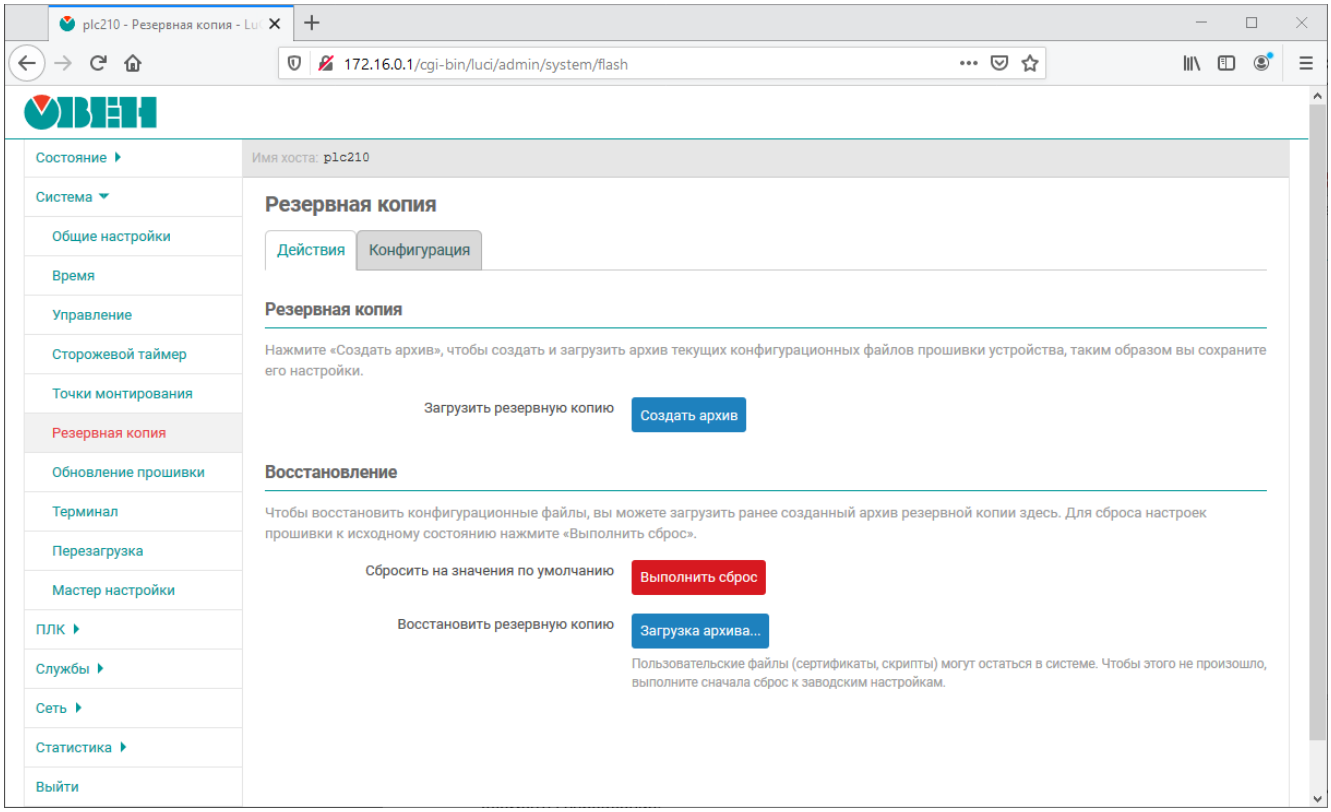


Рис. 4-17: Страница «Резервная копия»

На странице «Резервная копия» 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 «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 (см. раздел 4.6.1).

4.6.1 Восстановление резервной копии настроек

Восстановление резервной копии настроек производится при помощи кнопки «Загрузка архиве...», расположенной в подразделе «Восстановление» страницы «Резервная копия».

При нажатии кнопки «Загрузка архива...» будет отображено всплывающее окно, как показано на рисунке 4-18.

Рис. 4-18: Восстановление резервной копии. Выбор файла для загрузки

В данном окне необходимо выбрать файл архива резервной копии на локальной файловой системе при помощи кнопки «Обзор...» (см. рисунок 4-18). После выбора файла архива для загрузки, во всплывающем окне будет отображена информация о выбранном файле (имя и размер), как показано на рисунке 4-19. При этом, кнопка «Загрузить» становится активной.

Рис. 4-19: Восстановление резервной копии. Подтверждение загрузки

Для подтверждения загрузки выбранного файла необходимо нажать кнопку «Загрузить». В случае успешной загрузки файла архива резервной копии и его правильного формата (архив в формате «.tar.gz»), будет отображено окно подтверждения восстановления со списком всех восстанавливаемых файлов, как показано на рисунке 4-20.

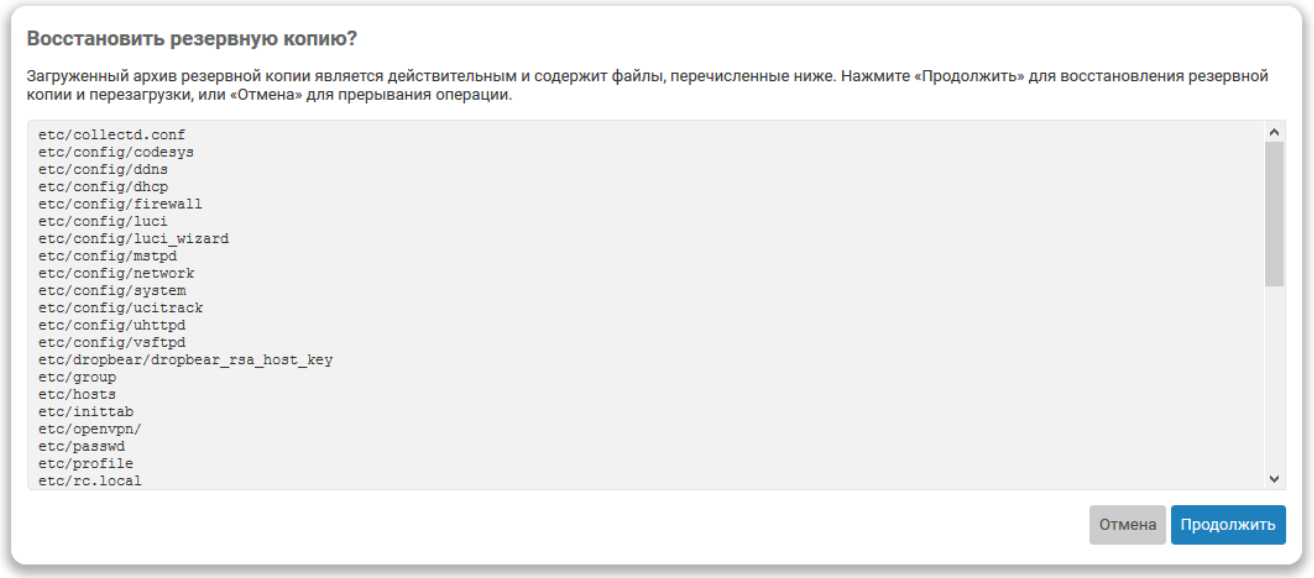


Рис. 4-20: Восстановление резервной копии. Подтверждение восстановления

Для подтверждения восстановления резервной копии необходимо нажать кнопку «Продолжить». В этом случае будет выполнено восстановление файлов из загруженного файла архива резервной копии с последующей перезагрузкой устройства.

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.

В том случае, если загружаемый повреждён или имеет неверный формат, после нажатия кнопки «Загрузить» (см. рисунок 4-20), всплывающее окно будет закрыто, а в верхней части страницы будет отображено сообщение о том, что загруженный файл не удаётся прочитать, как показано на рисунке 4-21.

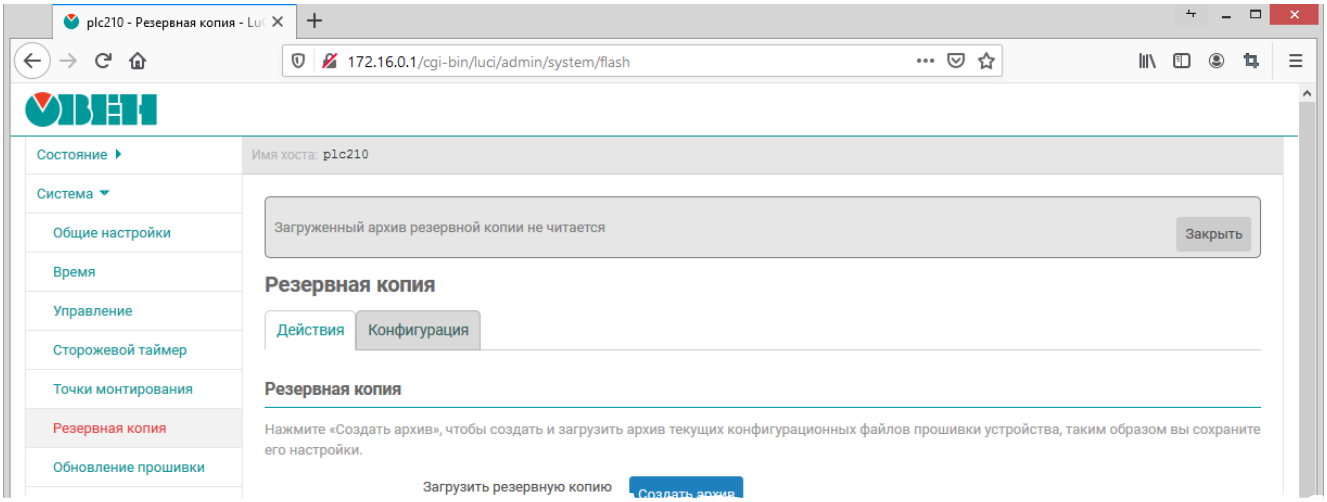


Рис. 4-21: Восстановление резервной копии. Ошибка чтения загруженного файла

4.6.2 Настройка списка файлов резервной копии

На вкладке «Конфигурация» страницы «Резервная копия» можно выполнить настройку списка файлов, которые будут сохраняться в резервной копии. Внешний вид вкладки «Конфигурация» показан на рисунке 4-22.

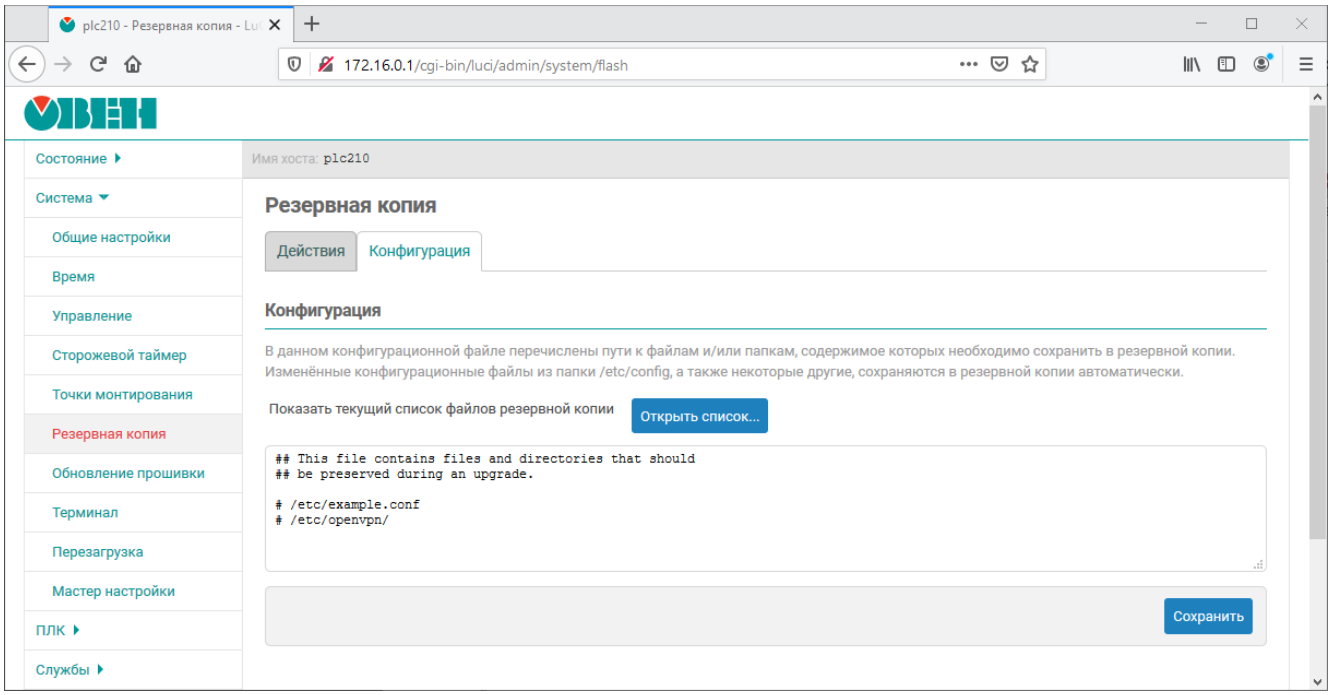


Рис. 4-22: Страница «Резервная копия». Вкладка «Конфигурация»

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

При нажатии кнопки «Открыть список...» будет отображён полный список файлов во всплывающем окне, которые будут сохранены в резервную копию с учётом конфигурационного файла «/etc/sysupgrade.conf» (см. рисунок 4-23).

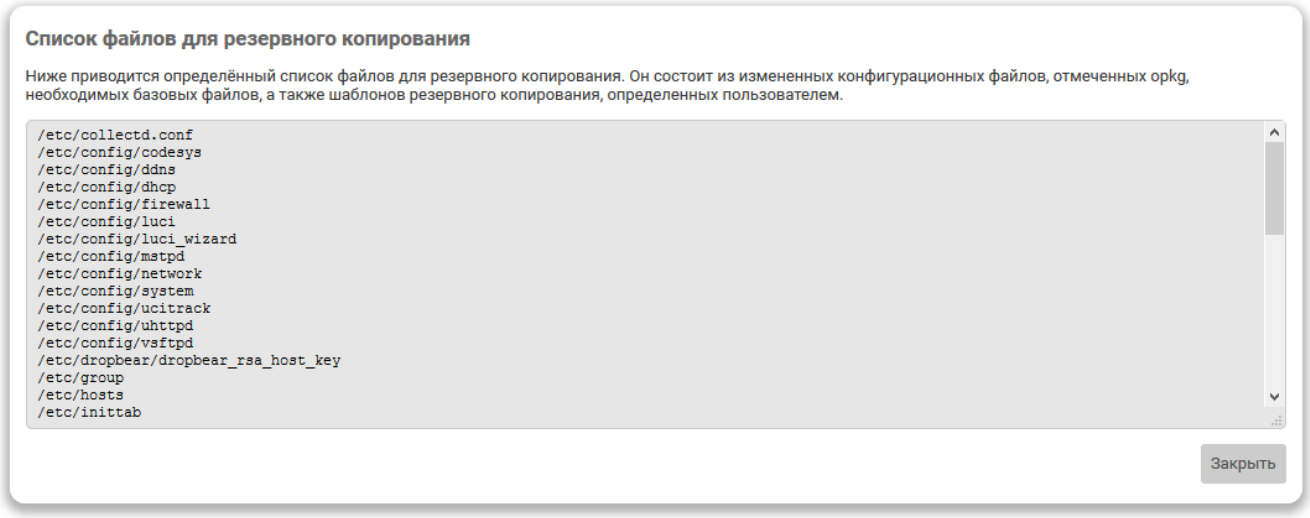


Рис. 4-23: Страница «Резервная копия». Вкладка «Конфигурация». Список файлов

4.7 Обновление прошивки

На странице «Обновление прошивки» раздела «Система» расположен функционал обновления прошивки устройства. Внешний вид страницы «Обновление прошивки» показан на рисунке 4-24.

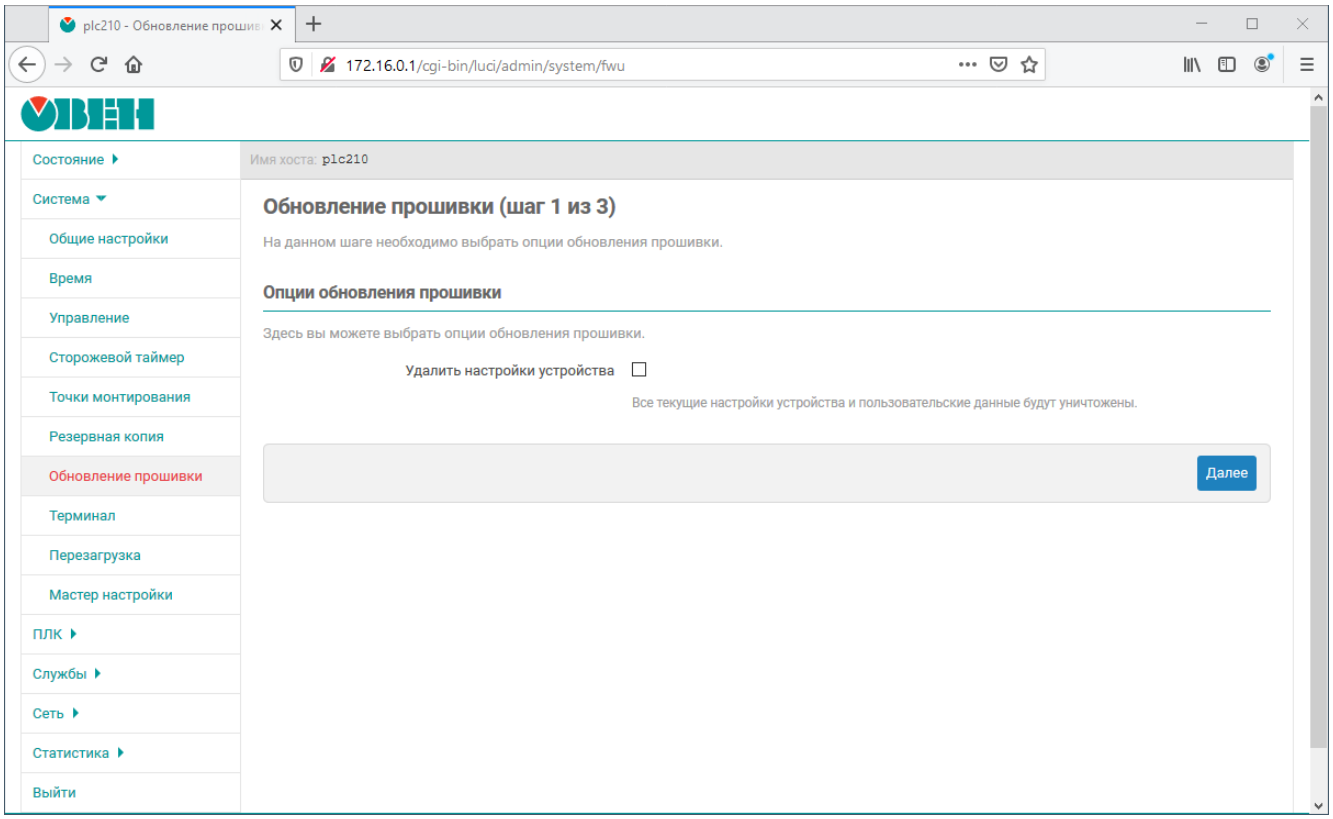


Рис. 4-24: Страница «Обновление прошивки»

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 4-24). Если данная настройка включена, то при выполнении обновления прошивки все пользовательские настройки и данные на устройстве будут уничтожены. Если же настройка не включена, то при выполнении обновления прошивки все пользовательские настройки и данные на устройстве будут сохранены.

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 4-25.

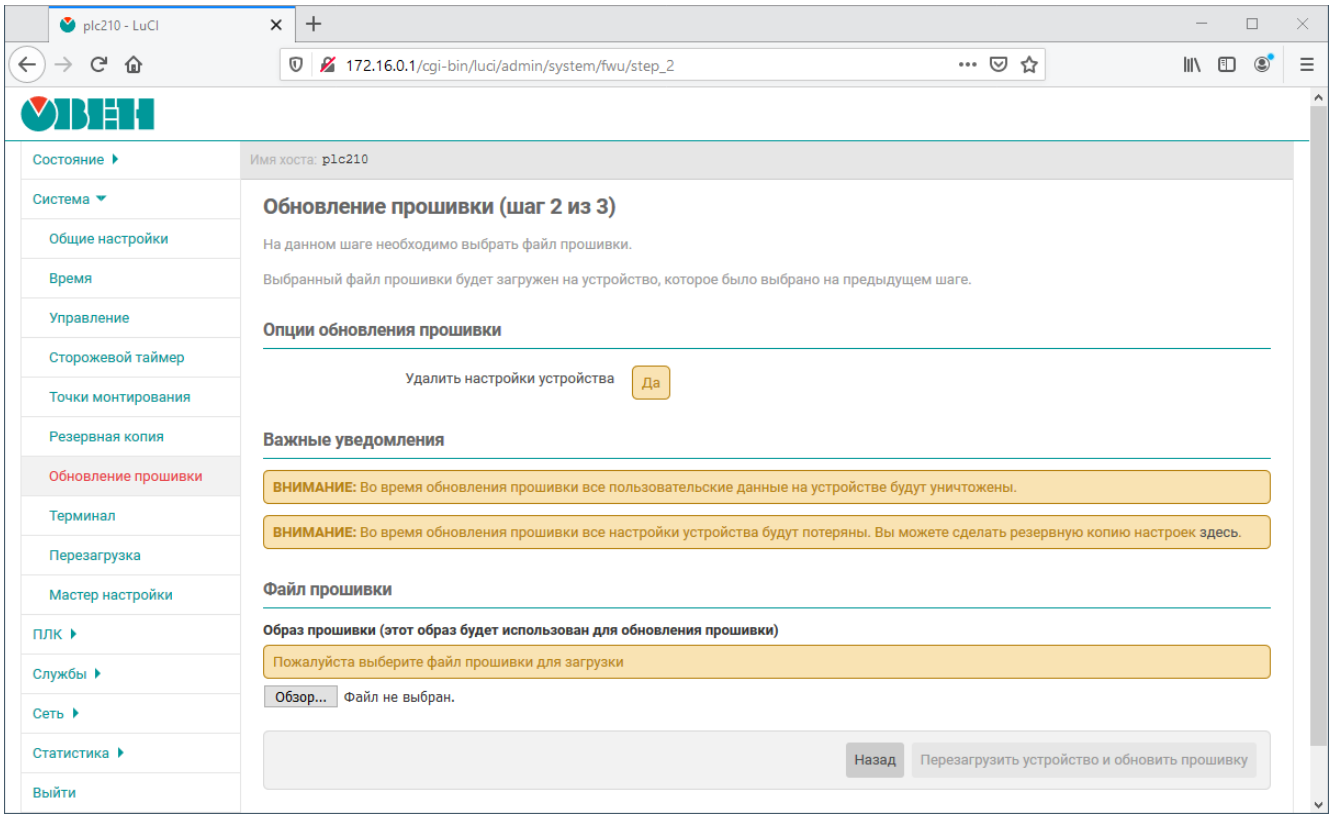


Рис. 4-25: Страница «Обновление прошивки». Загрузка файла прошивки

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 4-26.

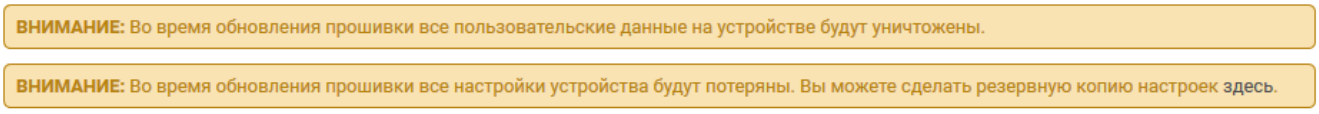


Рис. 4-26: Страница «Обновление прошивки». Область важных уведомлений

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 4-27.

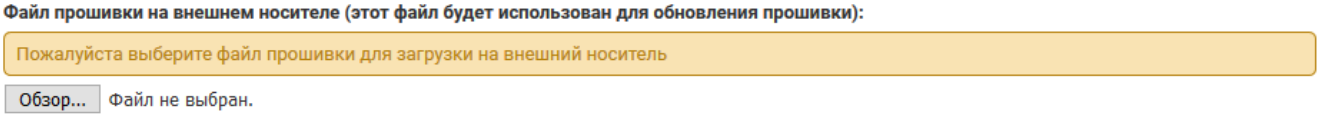


Рис. 4-27: Страница «Обновление прошивки». Отсутствие файла прошивки на внешнем устройстве

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 4-28.

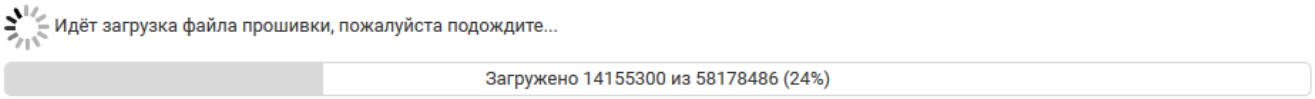


Рис. 4-28: Страница «Обновление прошивки». Процесс загрузки файла прошивки

Если загружен файл образа прошивки, который не предназначен для прошивки на устройстве ПЛК210, то подраздел «Файл прошивки» будет выглядеть так, как показано на рисунке 4-29. В этом случае необходимо выбрать новый файл образа прошивки для загрузки на внешнее устройство при помощи кнопки «Обзор...».

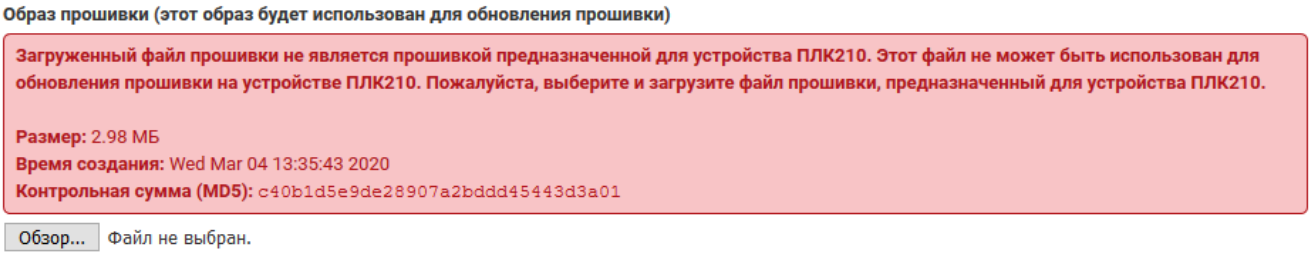


Рис. 4-29: Страница «Обновление прошивки». Некорректный файл прошивки на внешнем устройстве

Если же загружен файл образа прошивки, который предназначен для прошивки на устройстве ПЛК210, то подраздел «Файл прошивки» будет выглядеть так, как показано на рисунке 4-30.

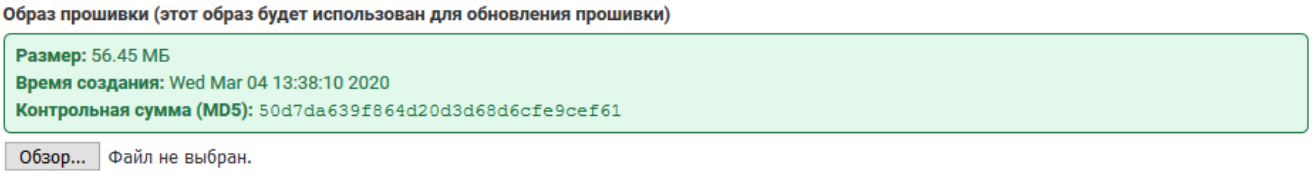


Рис. 4-30: Страница «Обновление прошивки». Корректный файл прошивки на внешнем устройстве

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 4-31.

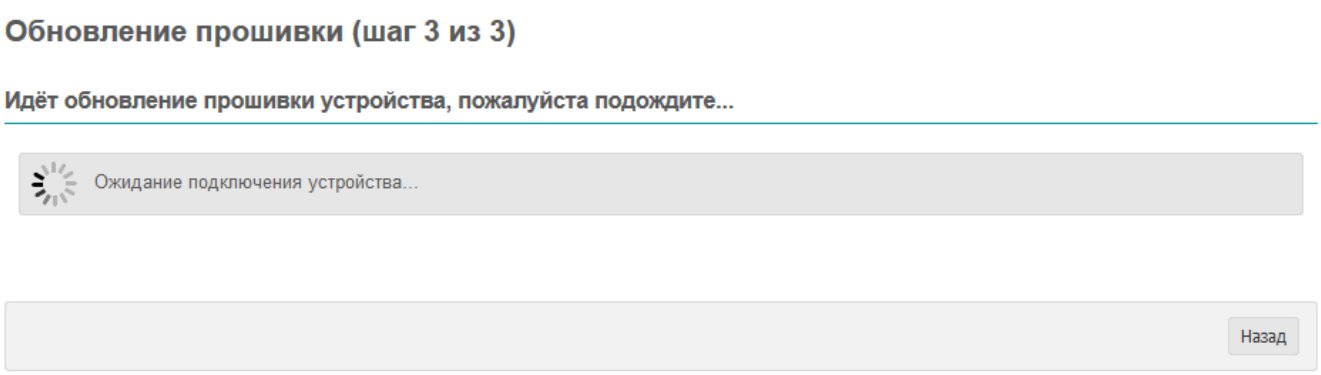


Рис. 4-31: Страница «Обновление прошивки». Обновление прошивки устройства

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 1.3). 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 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 4-32.

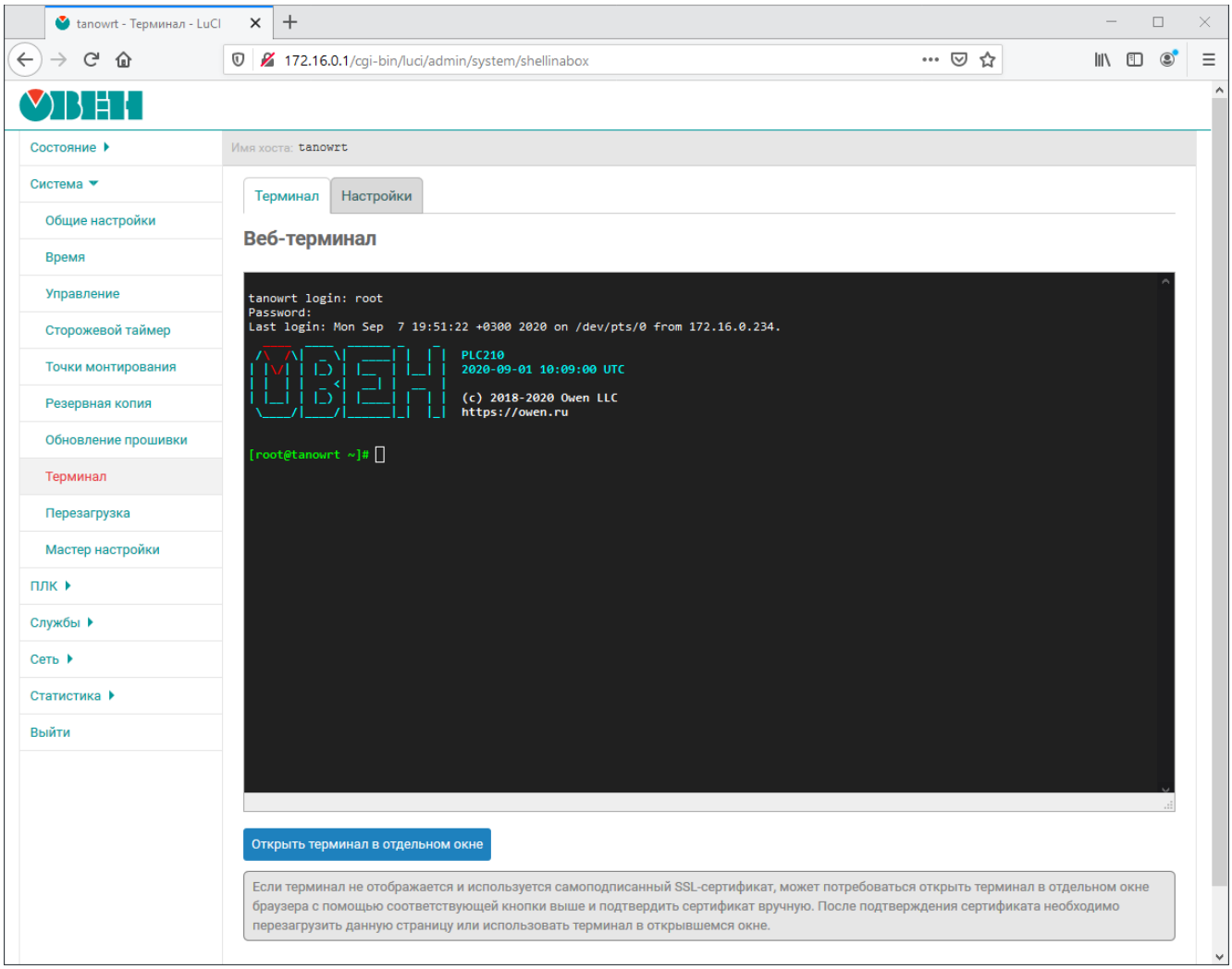


Рис. 4-32: Страница «Терминал»

При использовании самоподписанного SSL сертификата область терминала на странице «Терминал» может выглядеть так, как показано на рисунке 4-33.

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.

На рисунке 4-33 показано содержимое области терминала для браузера Mozilla Firefox. В других браузерах внешний вид и содержание данного сообщения может отличаться.

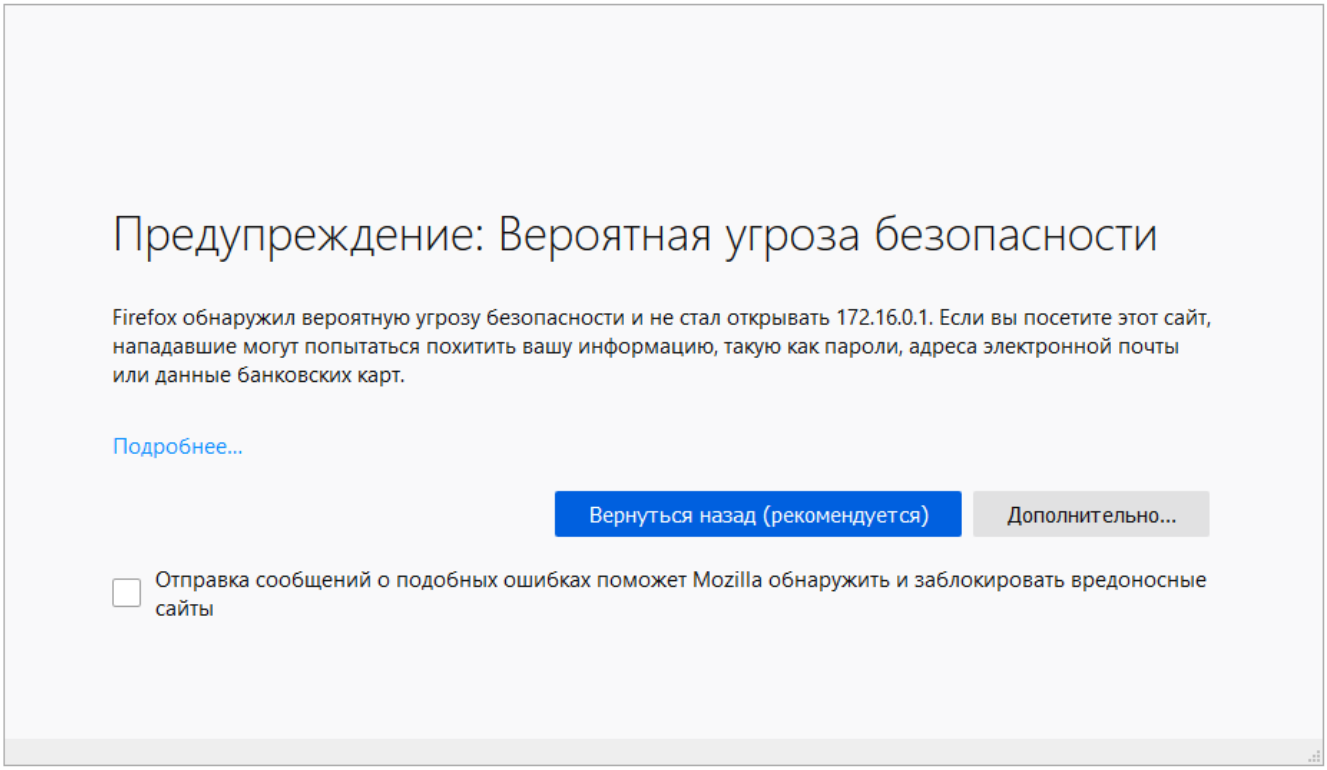


Рис. 4-33: Страница «Терминал». Ошибка проверки сертификата в браузере Mozilla Firefox

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 4-32).
2) В открывшемся окне будет отображено сообщение, аналогичное показанному на рисунке 4-33. Необходимо нажать кнопку «Дополнительно...».
3) В открывшейся области дополнительной информации (см. рисунок 4-34) необходимо нажать кнопку «Принять риск и продолжить».

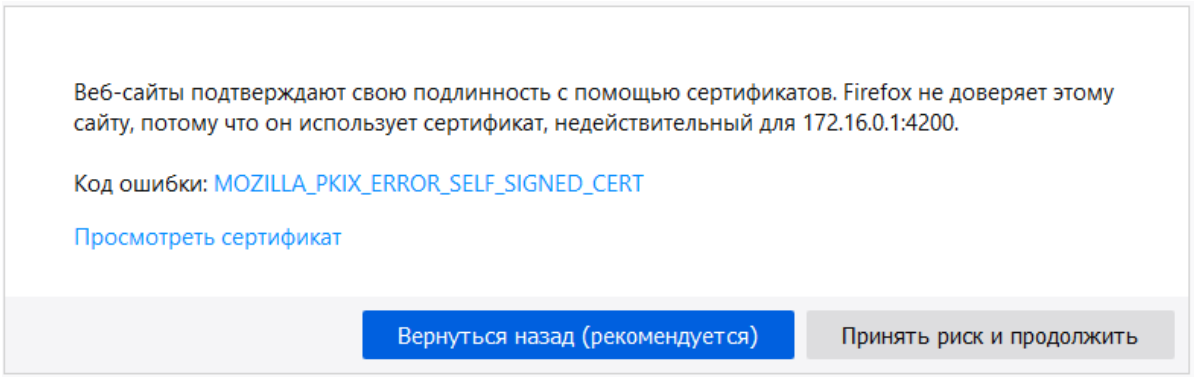


Рис. 4-34: Страница «Терминал». Дополнительная информация об ошибке проверки сертификата на примере браузера Mozilla Firefox

4) Будет открыт терминал с приглашением к вводу имени пользователя, как показано на рисунке 4-35.

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

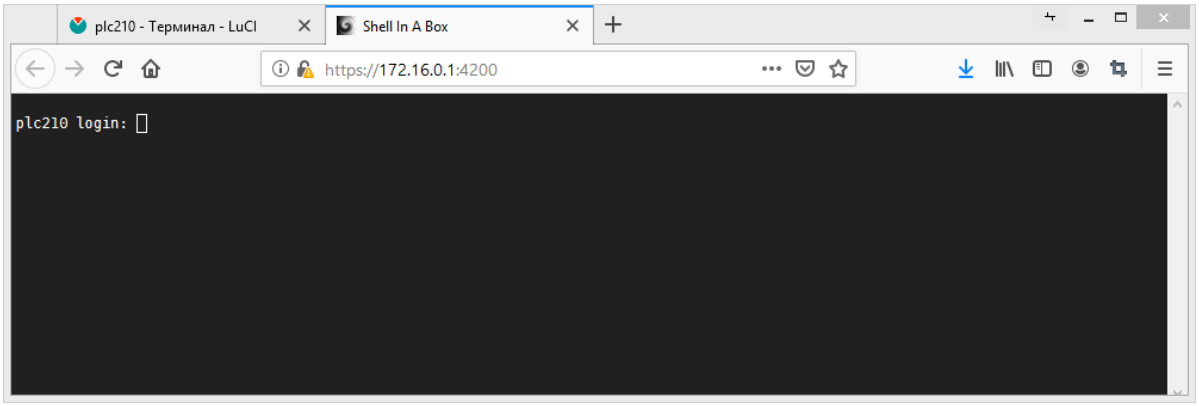


Рис. 4-35: Страница «Терминал». Открытие терминала после подтверждения самоподписанного сертификата

5) Отдельное окно браузера можно закрыть. После обновления основного окна, в котором была открыта страница «Терминал», область терминала должна выглядеть, как показано на рисунке 4-32.

4.8.1 Настройки терминала

Страница настроек терминала показана на рисунке 4-36.

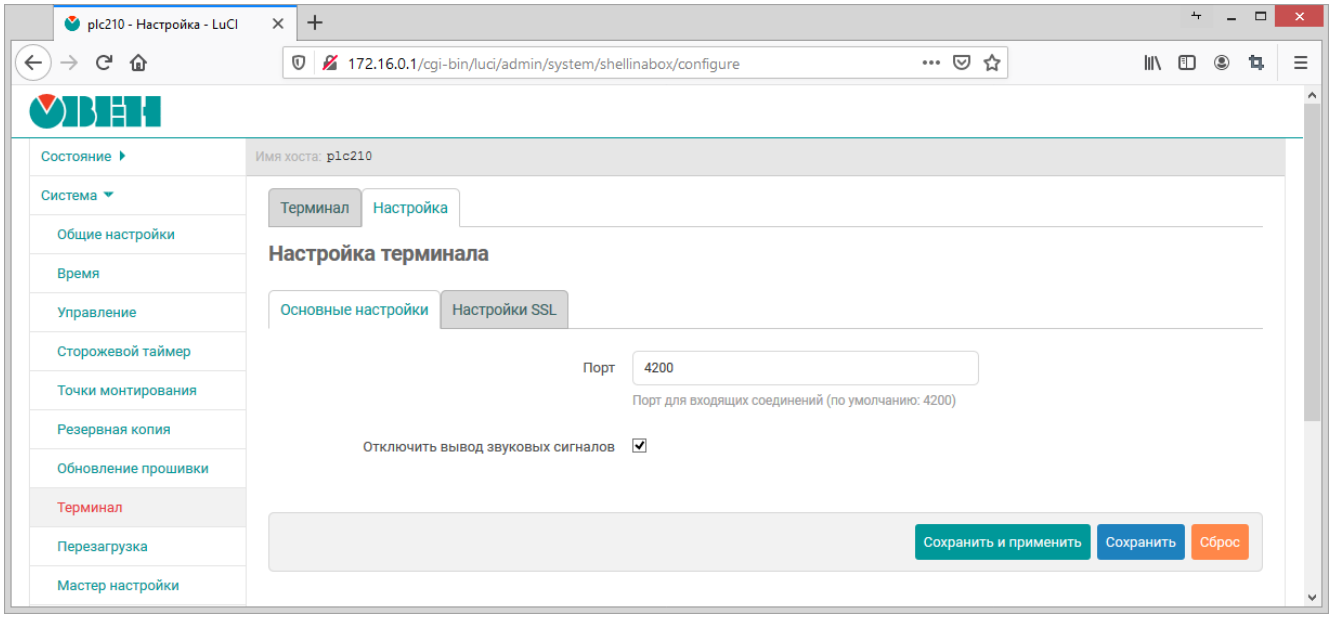


Рис. 4-36: Страница основных настроек терминала

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 4-37

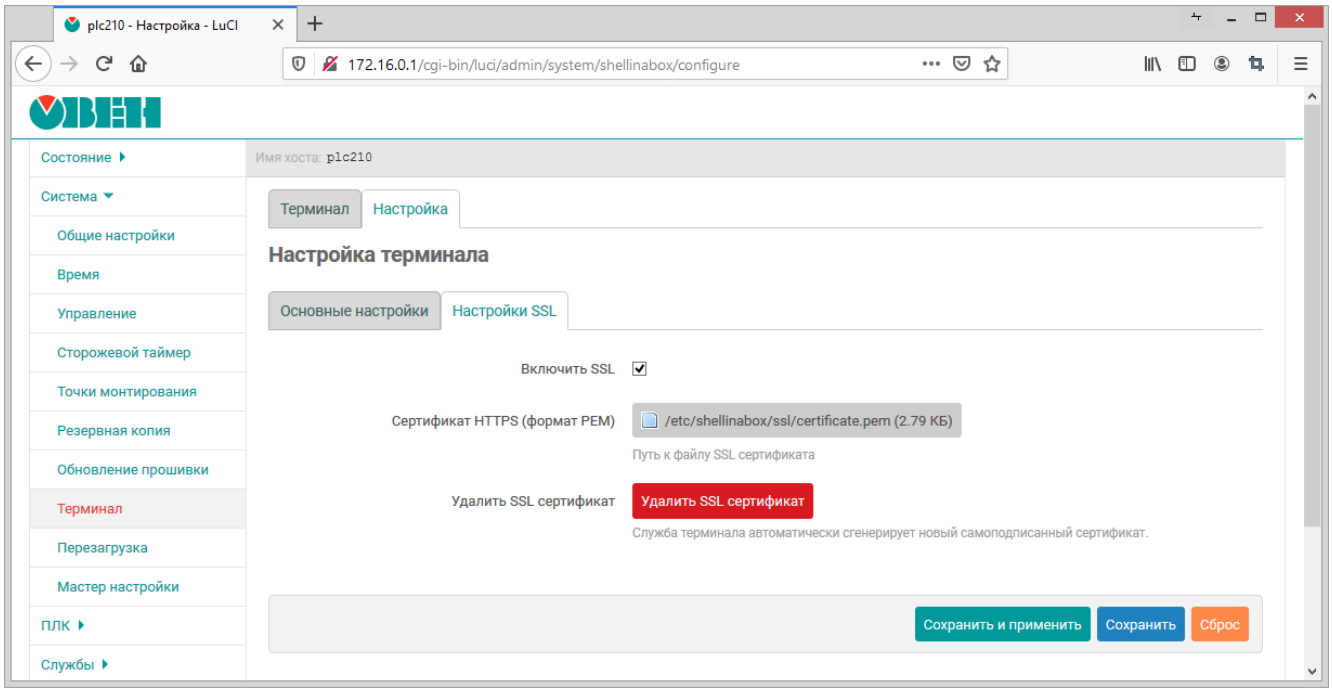


Рис. 4-37: Страница SSL настроек терминала

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 4-38.

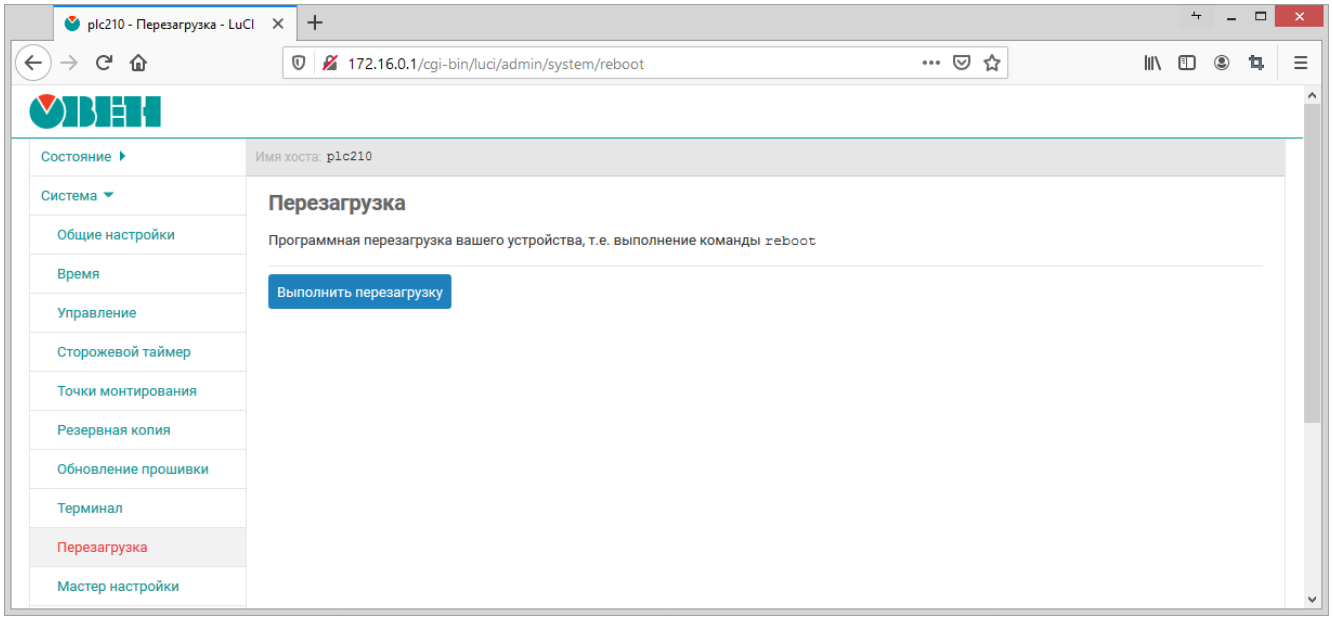


Рис. 4-38: Страница «Перезагрузка»

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 4-39.

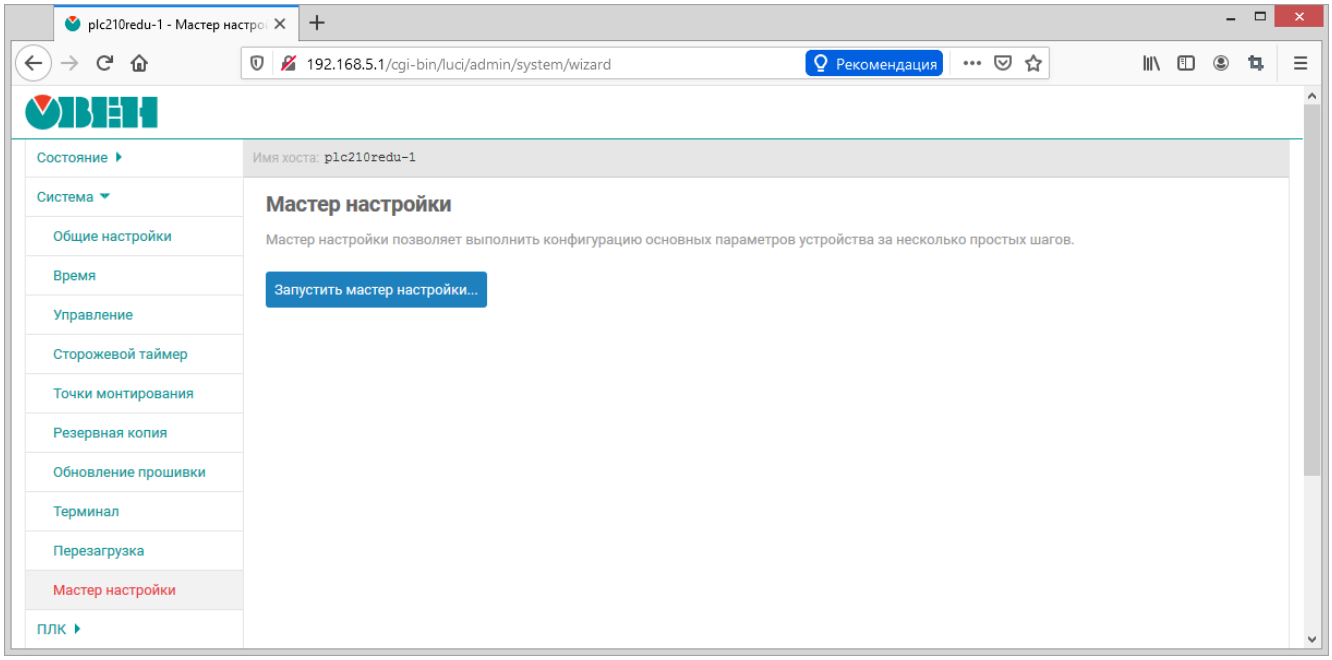


Рис. 4-39: Страница «Мастер настройки»

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.

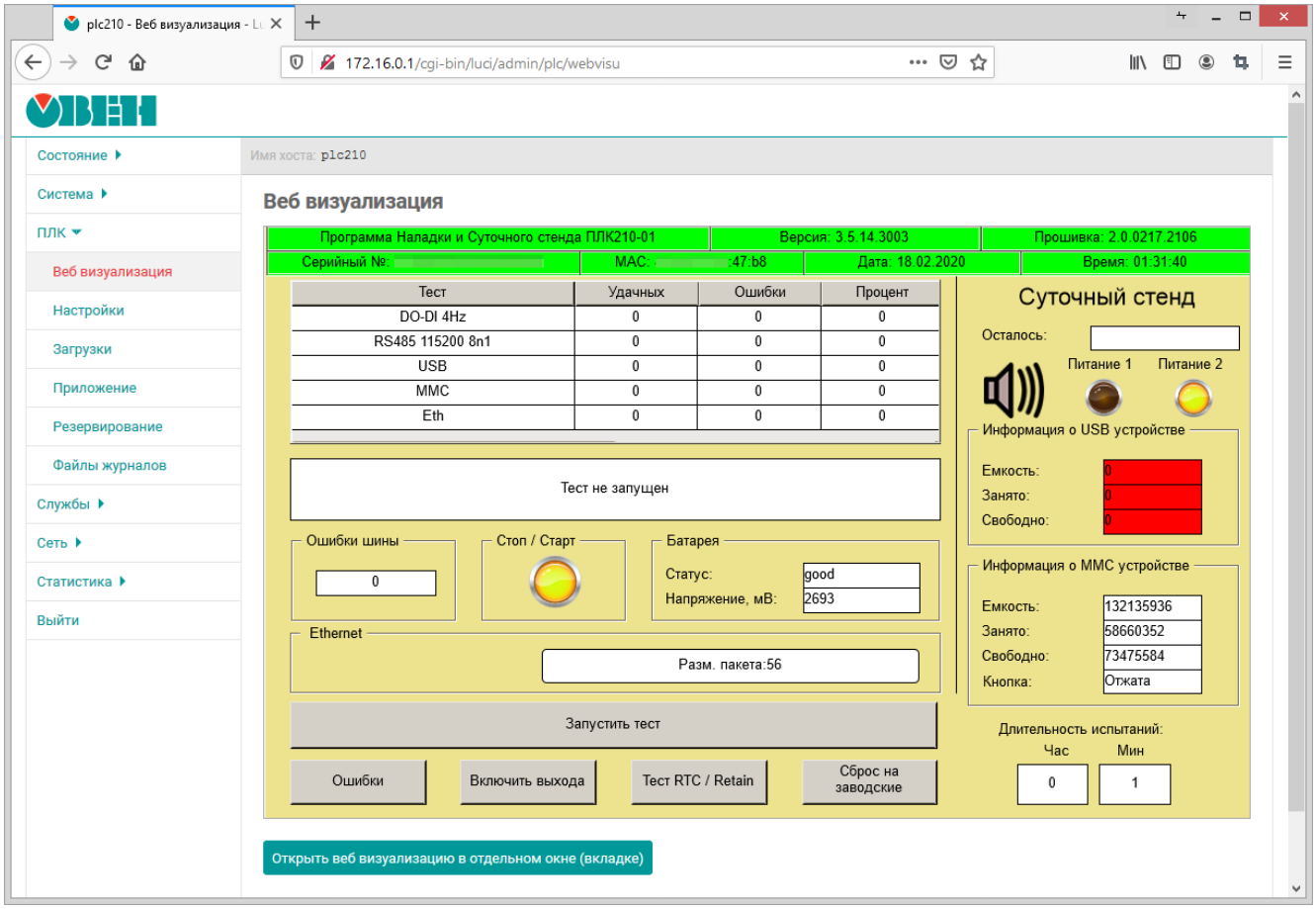


Рис. 5-1: Страница «Веб визуализация»

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).

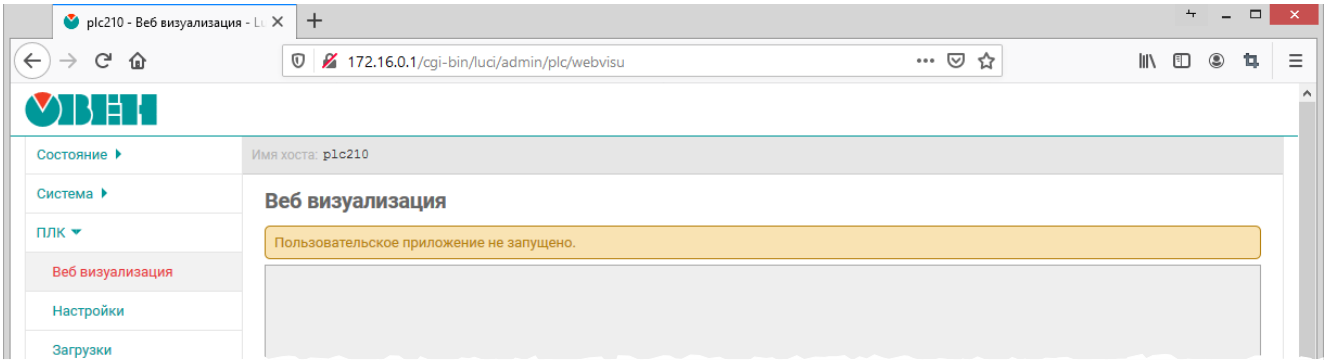


Рис. 5-2: Страница «Веб визуализация». Пользовательское приложение не запущено

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.

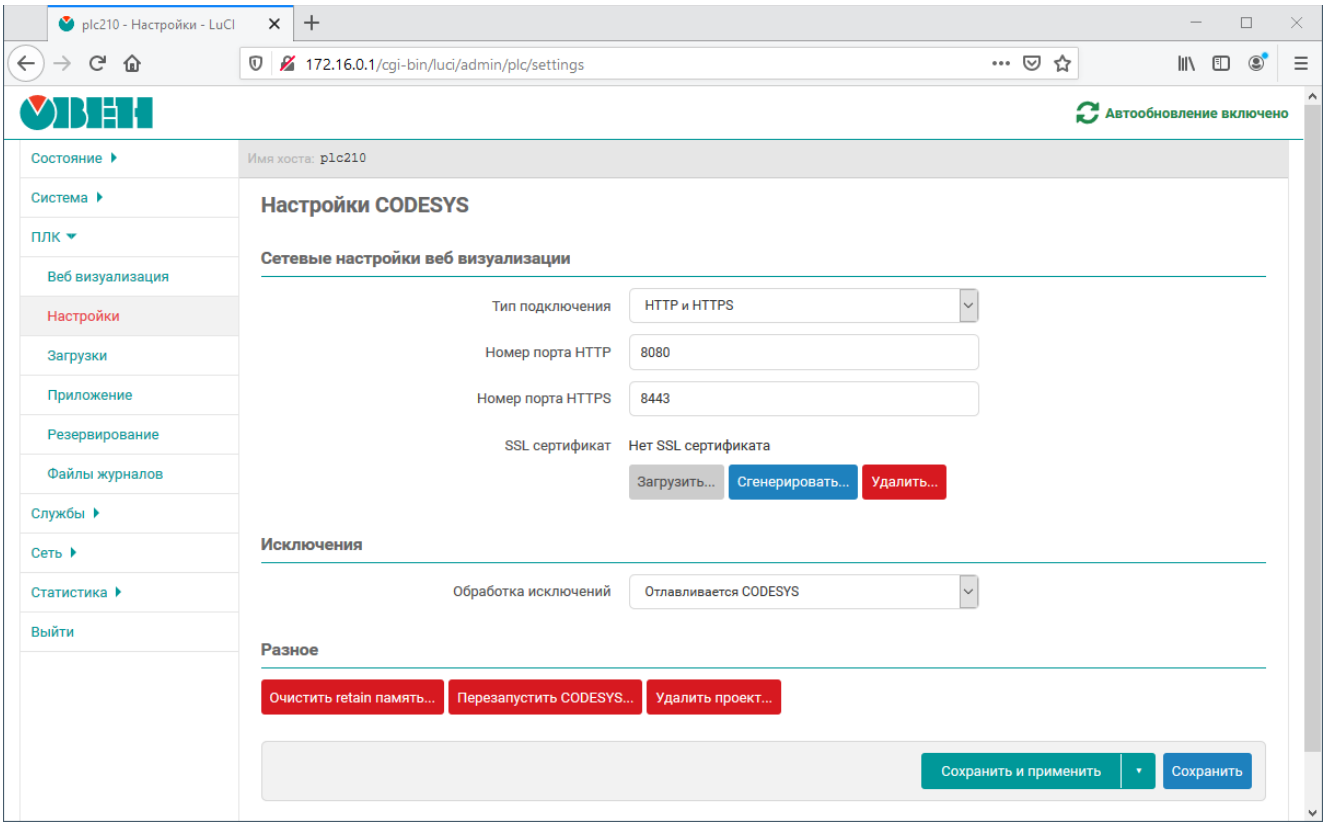


Рис. 5-3: Страница «Настройки»

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).

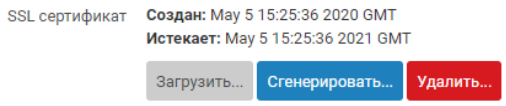


Рис. 5-4: Информация о текущем SSL сертификате веб визуализации CODESYS

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.

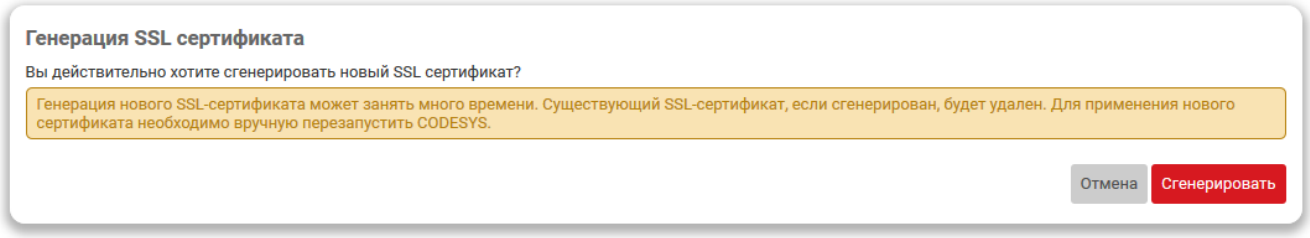


Рис. 5-5: Подтверждение генерации нового SSL сертификата

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

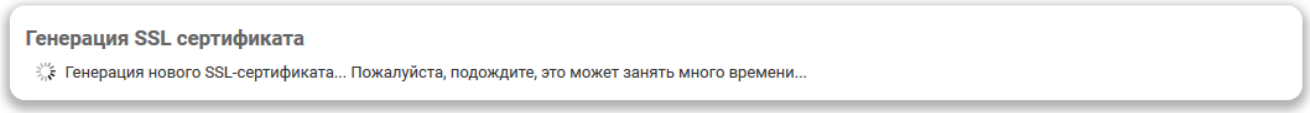


Рис. 5-6: Генерация нового SSL сертификата

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.

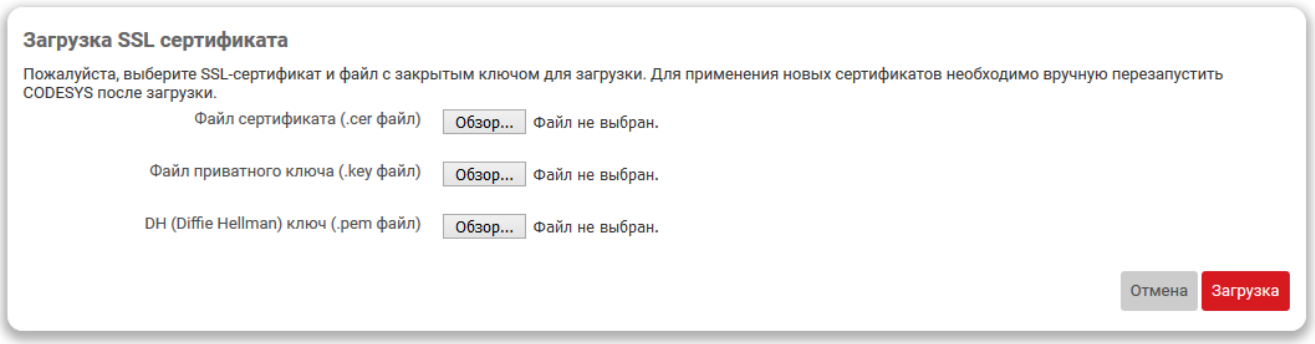


Рис. 5-10: Модальное окно загрузки SSL сертификата веб-визуализации CODESYS

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.

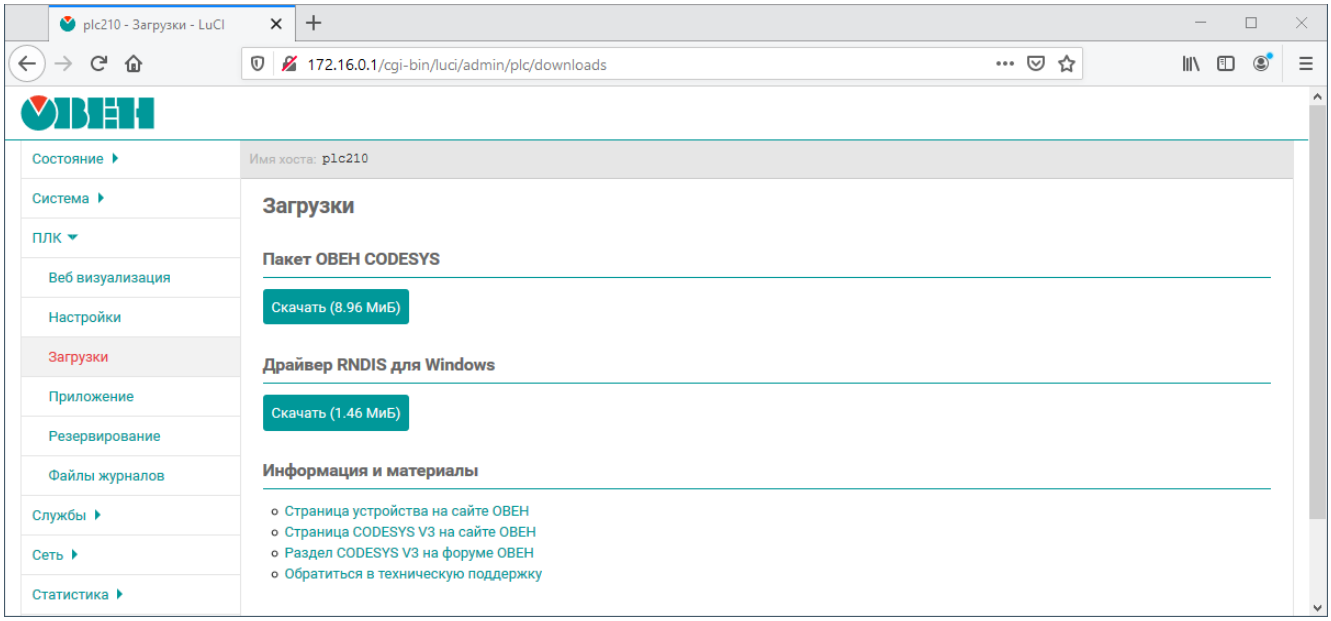


Рис. 5-22: Страница «Загрузки»

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.

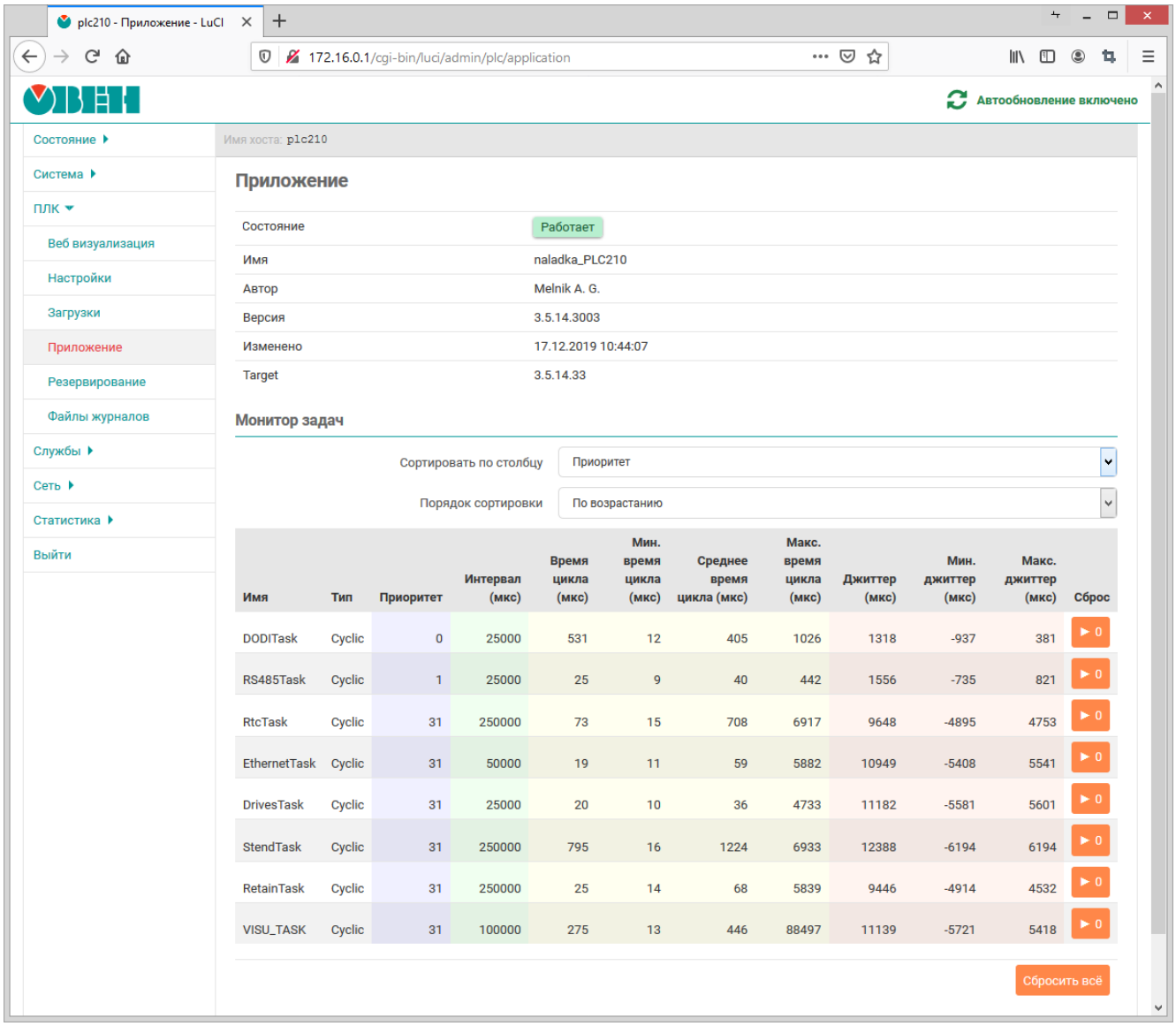


Рис. 5-23: Страница «Приложение»

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.

Состояние	Не запущено
Имя	*не указано*
Автор	*не указано*
Версия	*не указано*
Изменено	*не указано*
Target	*не указано*

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	521	12	405	1026	1318	-937	381	▶ 0
RS485Task	Cyclic	1	25000	24	9	40	442	1556	-735	821	▶ 0
RtcTask	Cyclic	31	250000	991	15	709	6917	9648	-4895	4753	▶ 0
EthernetTask	Cyclic	31	50000	27	11	59	5882	10949	-5408	5541	▶ 0
DrivesTask	Cyclic	31	25000	26	10	36	4733	11182	-5581	5601	▶ 0
StendTask	Cyclic	31	250000	963	16	1227	6933	12388	-6194	6194	▶ 0
RetainTask	Cyclic	31	250000	26	14	68	5839	9446	-4914	4532	▶ 0
VISU_TASK	Cyclic	31	100000	138	13	439	88497	11139	-5721	5418	▶ 0

Сбросить всё

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 Резервирование

Данный раздел присутствует только в Web-интерфейсе управления контроллеров ПЛК210 с поддержкой функции резервирования.

На странице «Резервирование» раздела «ПЛК» отображается информация и элементы управления функцией резервирования ПЛК.

Внешний вид страницы «Резервирование» раздела «ПЛК», при запущенном пользовательском приложении и настроенной функции резервирования между двумя устройствами, показан на рисунке 5-27.

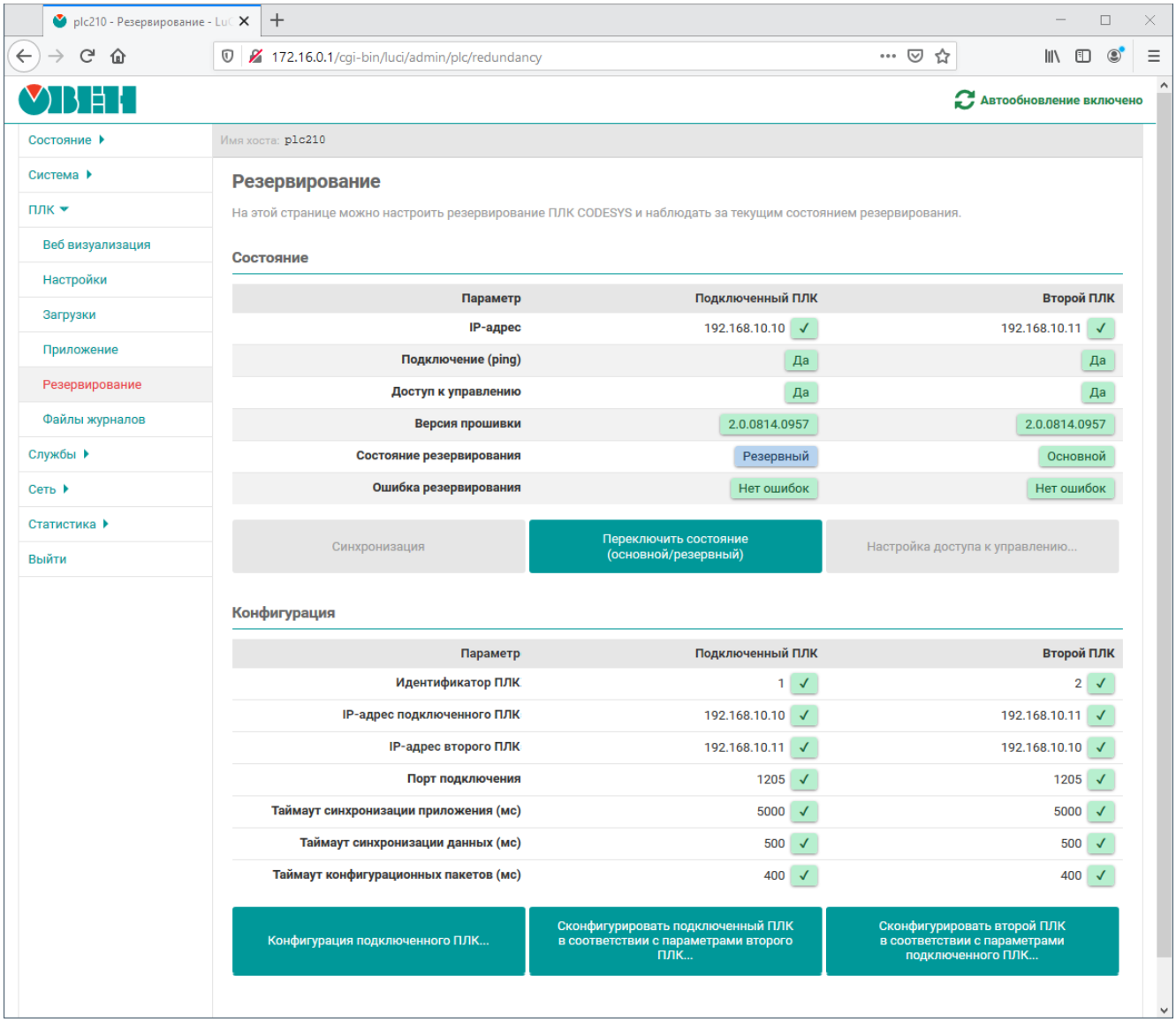


Рис. 5-27: Страница «Резервирование»

Страница «Резервирование» разделена на два подраздела:

- «Состояние» — содержит информацию о текущем состоянии резервирования и основные элементы управления (см. раздел 5.5.1);
- «Конфигурация» — содержит информацию о конфигурации функции резервирования подключенного и резервного ПЛК, а также содержит элементы управления синхронизации конфигурации (см. раздел 5.5.2).

5.5.1 Подраздел «Состояние»

В подразделе «Состояние» отображается таблица с информацией о текущем состоянии функции резервирования. Внешний вид таблицы состояния приведён на рисунке 5-28.

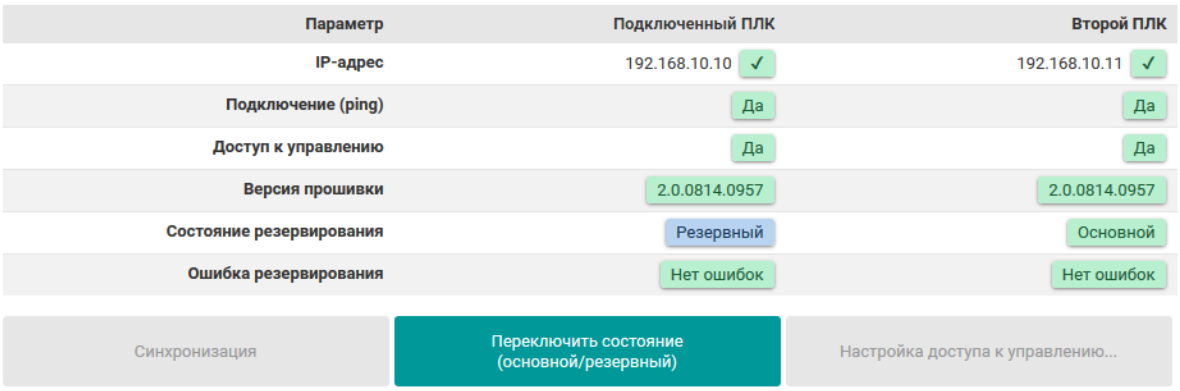


Рис. 5-28: Страница «Резервирование». Таблица состояния

Таблица состояния содержит следующие столбцы:

- «Параметр» — имя отображаемого параметра состояния;
- «Подключенного ПЛК» — значение параметра для подключенного ПЛК;
- «Второй ПЛК» — значение параметра для второго (резервного) ПЛК.

В строках таблицы отображаются значения для следующих параметров:

- «IP-адрес» — сконфигурированный IP-адрес ПЛК. Конфигурация IP-адресов для подключенного и второго ПЛК выполняется в подразделе «Конфигурация» (см. раздел 5.5.2). Если IP-адрес не сконфигурирован, то значение параметра будет отображаться как «Не сконфигурировано» (см. рисунок 5-29).

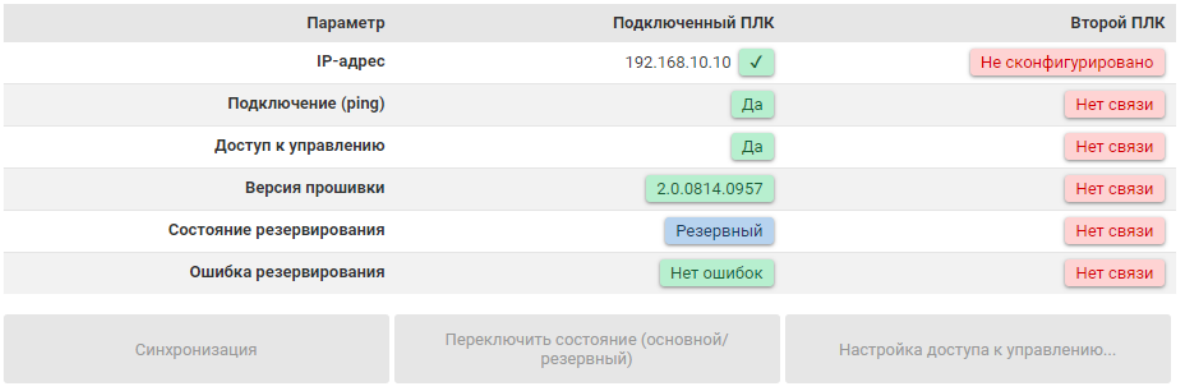


Рис. 5-29: Страница «Резервирование». Таблица состояния. IP-адрес не сконфигурирован

- «Подключение (ping)» — результат выполнения проверки подключения к ПЛК. Проверка выполняется путём отправки ICMP пакета «ECHO_REQUEST» [9] сконфигурированному IP-адресу с временем ожидания ответа равным 1 секунде. В том случае, если за время ожидания не будет получен ответ (ICMP пакет «ECHO_REPLY»), значение этого и всех последующих параметров будет отображаться как «Нет связи» (см. рисунок 5-30).

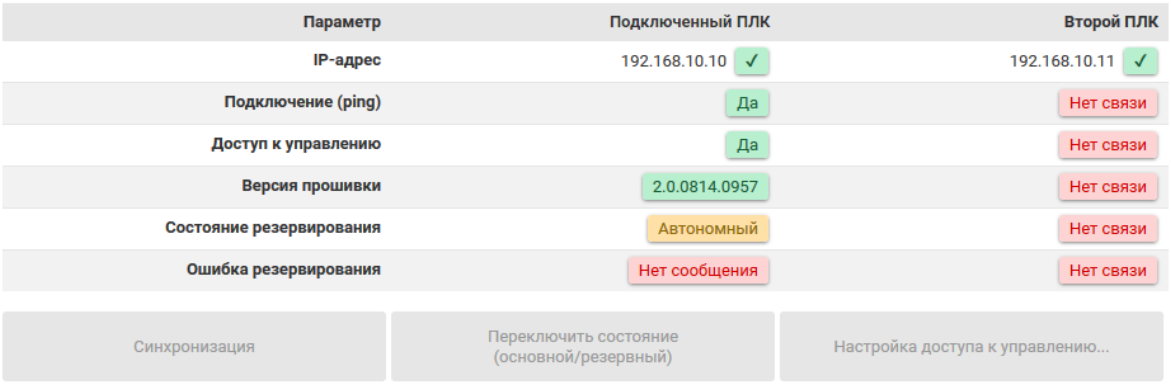


Рис. 5-30: Страница «Резервирование». Таблица состояния. Отсутствие связи со вторым ПЛК

Значение «Нет связи» также отображается в случае не сконфигурированного IP-адреса ПЛК.

- «Доступ к управлению» — результат выполнения проверки наличия доступа к управлению ПЛК. В случае подключенного ПЛК, доступ к управлению определяется тем, запущено ли ядро ПЛК (CODESYS) или нет. В случае второго ПЛК, для обеспечения доступа к управлению, помимо запущенного ядра ПЛК, также необходимо наличие беспарольного SSH-доступа ко второму ПЛК. Для настройки такого доступа необходимо воспользоваться кнопкой «Настройка доступа к управлению...», которая становится активной в случае отсутствия доступа к управлению вторым ПЛК (см. раздел 5.5.1.3).

  В случае отсутствия доступа к управлению, значение этого и всех последующих параметров будет отображаться как «Нет доступа» (см. рисунок 5-31).

  Состояние «Нет доступа» может отображаться во время перезапуска ядра ПЛК, например, при изменении конфигурации.

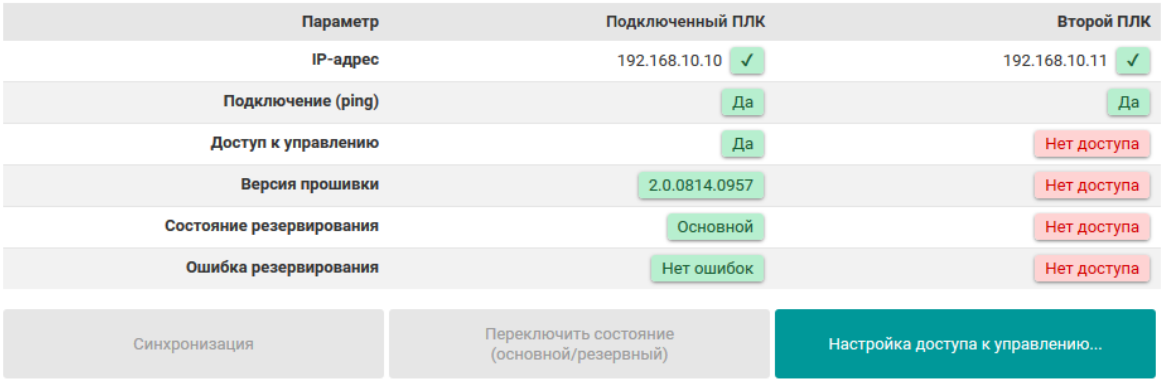


Рис. 5-31: Страница «Резервирование». Таблица состояния. Отсутствие доступа к управлению вторым ПЛК

- «Версия прошивки» — версия прошивки ПЛК. Если на подключенном и втором ПЛК версии прошивки различаются, то более ранняя версия будет отмечена красным цветом (см. рисунок 5-32). В таком случае, на этом устройстве рекомендуется выполнить обновление прошивки (см. раздел 4.7).

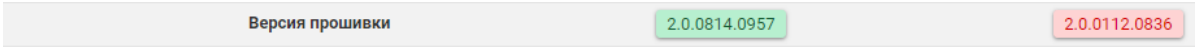


Рис. 5-32: Страница «Резервирование». Таблица состояния. Разные версии прошивок

- «Состояние резервирования» — текущее состояние резервирования. Возможны следующие состояния:
  - «Запуск» — выполняется запуск;
  - «Синхронизация» — выполняется синхронизация;
  - «Основной» — резервирование работает нормально, ПЛК является основным;

- «Резервный» — резервирование работает нормально, ПЛК является резервным;
- «Автономный» — ПЛК работает автономно без резервирования;
- «Ошибка» — произошла ошибка;
- «Симуляция» — режим симуляции;
- «Ошибка загрузки» — произошла ошибка загрузки;
- «Отключение основного» — выполняется отключение основного ПЛК;
- «Отключение резервного» — выполняется отключение резервного ПЛК;
- «Ошибка синхронизации» — произошла ошибка синхронизации;
- «Запуск симуляции» — выполняется запуск симуляции;
- «Нет лицензии» — отсутствует лицензия;
- «Неизвестно» — получить информацию о текущем состоянии не удалось.

- «Ошибка резервирования» — информация об ошибке резервирования. Возможны следующие ошибки:
  - «Нет ошибок» — ошибок нет, резервирование работает нормально;
  - «Ошибка» — произошла ошибка;
  - «Ошибка загрузки» — произошла ошибка загрузки;
  - «Ошибка синхронизации» — произошла ошибка синхронизации;
  - «Ошибка цикла» — произошла ошибка цикла;
  - «Неверное сообщение» — получено неверное сообщение;
  - «Ошибка связи» — произошла ошибка связи;
  - «Ошибка полевой шины» — произошла ошибка полевой шины;
  - «Ошибка приёма сообщения» — произошла ошибка при приёме сообщения;
  - «Нет сообщения» — отсутствует сообщение;
  - «Ошибка конфигурации» — произошла ошибка конфигурации;
  - «CRC ошибка области ввода» — произошла ошибка контрольной суммы области ввода;
  - «Нет лицензии» — отсутствует лицензия;
  - «Неизвестная ошибка» — произошла неизвестная ошибка.

В нижней части таблицы расположены три кнопки:

- «Синхронизация» — см. раздел 5.5.1.1;
- «Переключить состояние (основной/резервный)» — см. раздел 5.5.1.2;
- «Настройка доступа к управлению...» — см. раздел 5.5.1.3.

5.5.1.1 Синхронизация

В том случае, когда синхронизация между ПЛК нарушена (восстановление связи после обрыва, замена резервного ПЛК, ошибки синхронизации и т.п.), необходимо выполнить ручную синхронизацию ПЛК.

Если выполнение операции синхронизации возможно в соответствии с текущим состоянием подключенного и второго ПЛК, то в нижней части таблицы состояния будет активна кнопка «Синхронизация» (см. рисунок 5-33).

Нажатие кнопки «Синхронизации» приведёт к запуску процесса синхронизации. Во время выполнения синхронизации, будет отображаться всплывающее окно, показанное на рисунке 5-37.

В случае успешного завершения синхронизации всплывающее окно будет закрыто, а в таблице состояния будут отображены обновлённые значения параметров.

В случае ошибки синхронизации будет отображено всплывающее окно с кодом и описанием ошибки.

5.5.1.2 Переключение состояний

В том случае, когда оба ПЛК (подключенный и второй) работают нормально и между ними имеется связь, один ПЛК становится основным, а второй резервным.

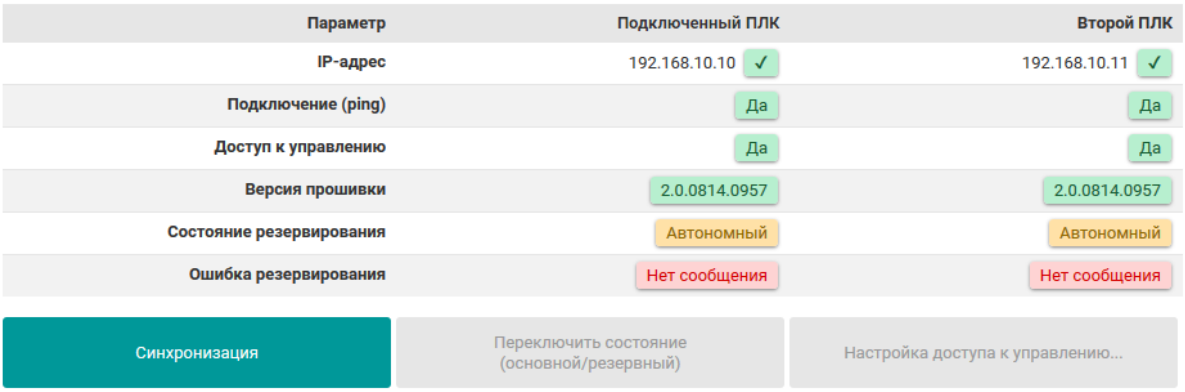


Рис. 5-33: Страница «Резервирование». Таблица состояния. Активная кнопка «Синхронизация»

Рис. 5-34: Страница «Резервирование». Выполнение операции синхронизации ПЛК

Для переключения состояний двух ПЛК предназначена кнопка «Переключить состояние (основной/резервный)», расположенная в нижней части таблицы состояния. Если выполнение операции переключения состояния возможно, в соответствии с текущим состоянием подключенного и второго ПЛК, то кнопка переключения состояний будет активна, как показано на рисунке 5-28.

Нажатие кнопки переключения состояний приведёт к запуску процесса переключения. Во время выполнения операции будет отображаться всплывающее окно, показанное на рисунке 5-35.

Рис. 5-35: Страница «Резервирование». Выполнение операции переключения состояний

В случае успешного завершения операции всплывающее окно будет закрыто, а в таблице состояния будут отображены обновлённые значения параметров:

- ПЛК, который до выполнения операции имел состояние «Основной», будет переключён в состояние «Резервный»;
- ПЛК, который до выполнения операции имел состояние «Резервный», будет переключён в состояние «Основной».

В случае возникновения ошибки будет отображено всплывающее окно с кодом и описанием ошибки.

5.5.1.3 Настройка доступа к управлению вторым ПЛК

Для обеспечения доступа к управлению вторым (резервным) ПЛК используется беспарольный SSH доступ с авторизацией с применением приватных ключей. Если доступ к управлению вторым ПЛК отсутствует, то в нижней части таблицы состояния будет активна кнопка «Настройка доступа к управлению...» (см. рисунок 5-31).

При нажатии кнопки «Настройка доступа к управлению...» будет отображено всплывающее окно, показанное на рисунке 5-36.

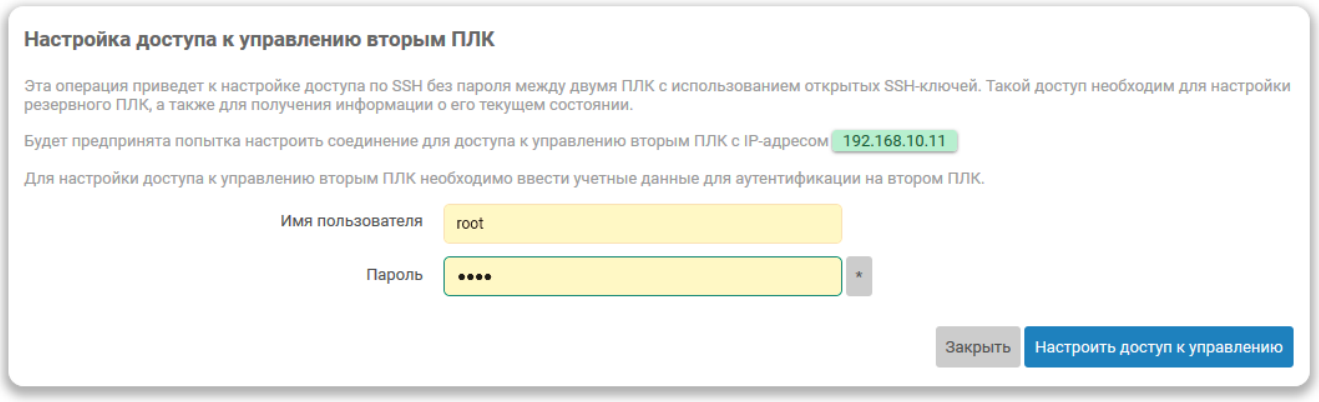


Рис. 5-36: Страница «Резервирование». Всплывающее окно настройки доступа к управлению вторым ПЛК

Во всплывающем окне, в соответствующие поля для ввода, необходимо ввести данные для аутентификации на втором ПЛК:

- «Имя пользователя» — имя пользователя для входа (по умолчанию «root»);
- «Пароль» — пароль для входа (по умолчанию «owen»).

После ввода данные для аутентификации необходимо нажать кнопку «Настроить доступ к управлению». Во время выполнения настройки будет отображаться окно, показанное на рисунке 5-37.

Рис. 5-37: Страница «Резервирование». Выполнение операции настройки доступа к управлению вторым ПЛК

В случае успешного завершения настройки доступа к управлению вторым ПЛК всплывающее окно будет закрыто, а в таблице состояния значение параметра «Доступ к управлению» будет отображено как «Да» (см. рисунок 5-28).

В случае ошибки настройки доступа к управлению (неверные данные для аутентификации, неверный IP-адрес и т.п.) будет отображено всплывающее окно с кодом и описанием ошибки (см. рисунок 5-38).

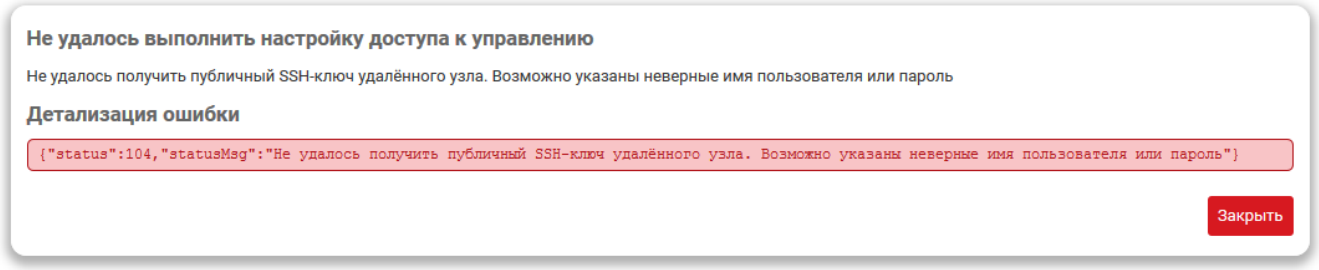


Рис. 5-38: Страница «Резервирование». Ошибка настройки доступа к управлению вторым ПЛК

5.5.2 Подраздел «Конфигурация»

В подразделе «Конфигурация» отображается таблица с информацией о текущей конфигурации функции резервирования. Внешний вид таблицы конфигураций приведён на рисунке 5-39.

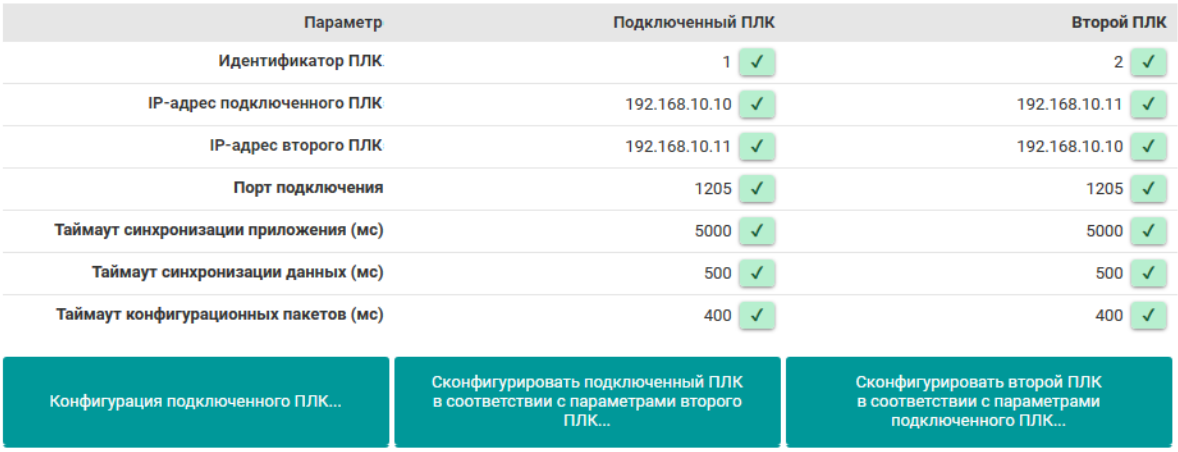


Рис. 5-39: Страница «Резервирование». Таблица конфигураций

Таблица конфигурации содержит следующие столбцы:

- «Параметр» — имя конфигурационного параметра;
- «Подлкюченный ПЛК» — значение параметра для подключенного ПЛК;
- «Второй ПЛК» — значение параметра для второго (резервного) ПЛК.

В строках таблицы отображаются текущие значения конфигурационных параметров для подключенного и второго (резервного) ПЛК. Полный перечень всех отображаемых конфигурационных параметров с их описанием приведён в разделе 5.5.2.2.

В нижней части таблицы расположены три кнопки:

- «Конфигурация подключенного ПЛК...» — см. раздел 5.5.2.2;
- «Сконфигурировать подключенный ПЛК в соответствии с параметрами второго ПЛК...» — см. раздел 5.5.2.3;
- «Сконфигурировать второй ПЛК в соответствии с параметрами подключенного ПЛК...» — см. раздел 5.5.2.3.

5.5.2.1 Проверка (валидация) конфигураций

При наличии доступа к конфигурации обоих ПЛК выполняется проверка (валидация) конфигураций.

В том случае, если какой-либо конфигурационный параметр не сконфигурирован, его значение в таблице конфигураций будет отображаться как «Не сконфигурировано» (см. рисунок 5-40).

Дополнительно выполняются следующие проверки:

- идентификаторы ПЛК на подключенном и втором ПЛК не должны совпадать;
- IP-адрес подключенного ПЛК на втором ПЛК должен соответствовать IP-адресу второго ПЛК на подключенном ПЛК;
- IP-адрес второго ПЛК на втором ПЛК должен соответствовать IP-адресу подлюченного ПЛК на подключенном ПЛК;
- значения порта подключения и таймаутов должны совпадать на обоих ПЛК.

В случае наличия каких-либо несоответствий в конфигурациях подключенного и второго ПЛК, эта информация будет отображена в таблице (см. рисунок 5-40).

Параметр	Подключенный ПЛК	Второй ПЛК
Идентификатор ПЛК	Не сконфигурировано	2 ✓
IP-адрес подключенного ПЛК	192.168.10.10 ✓	192.168.10.11 ✓
IP-адрес второго ПЛК	192.168.10.11 ✓	192.168.10.10 ✓
Порт подключения	1205 ✓	1205 ✓
Таймаут синхронизации приложения (мс)	5100 Не соответствует	5000 Не соответствует
Таймаут синхронизации данных (мс)	500 ✓	500 ✓
Таймаут конфигурационных пакетов (мс)	450 Не соответствует	400 Не соответствует

Конфигурация подключенного ПЛК... | Сконфигурировать подключенный ПЛК в соответствии с параметрами второго ПЛК... | Сконфигурировать второй ПЛК в соответствии с параметрами подключенного ПЛК...

Рис. 5-40: Страница «Резервирование». Таблица конфигурации. Проверка конфигураций

5.5.2.2 Конфигурация подключенного ПЛК

Для изменения конфигурационных параметров резервирования подключенного ПЛК нужно нажать кнопку «Конфигурация подключенного ПЛК», расположенную в нижней части таблицы конфигураций (см. рисунок 5-39). Нажатие кнопки приведёт к отображению всплывающего окна редактирования конфигурационных параметров (см. рисунки 5-41 и 5-42).

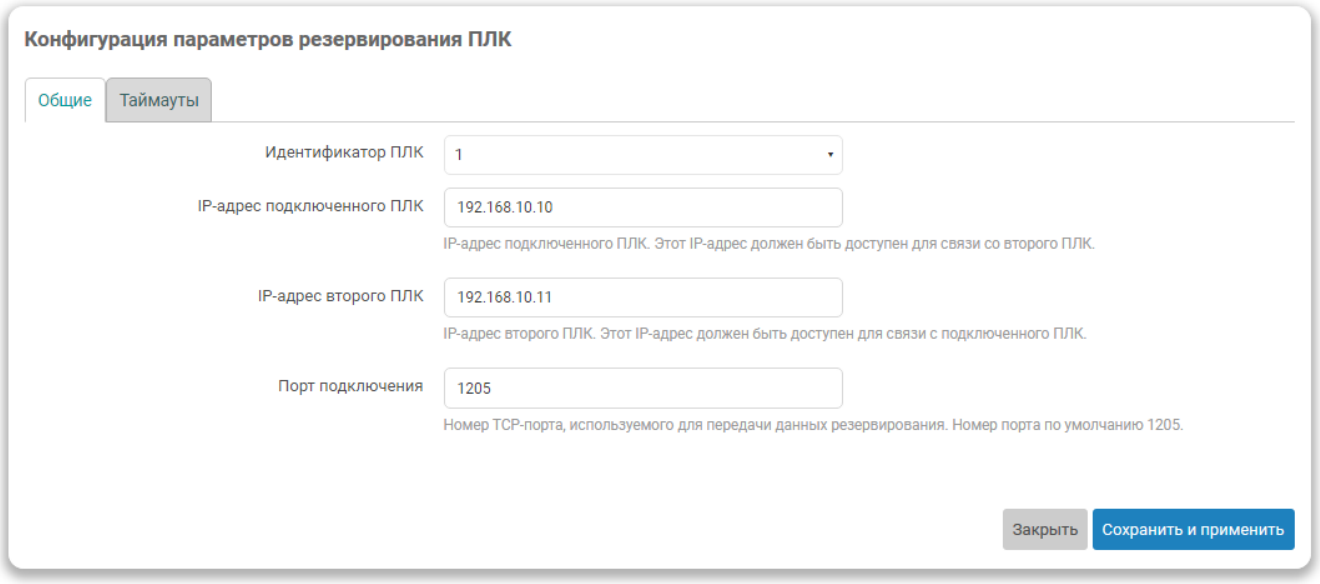


Рис. 5-41: Страница «Резервирование». Окно редактирования конфигурационных параметров. Вкладка «Общие»

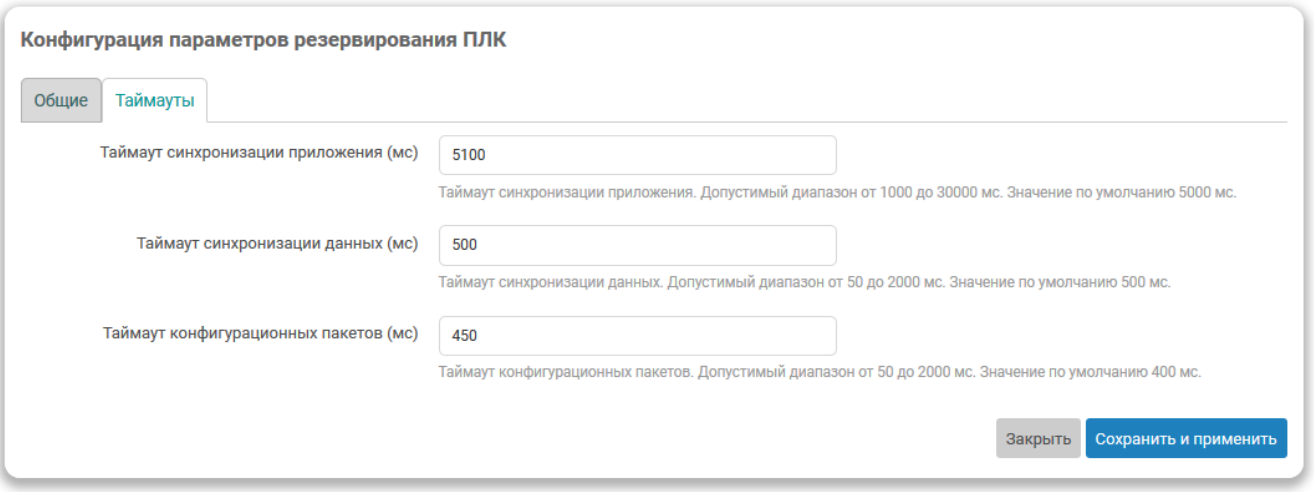


Рис. 5-42: Страница «Резервирование». Окно редактирования конфигурационных параметров. Вкладка «Таймауты»

Конфигурационные параметры во всплывающем окне разделены на две вкладки:

- «Общие»;
- «Таймауты».

Во вкладке «Общие» расположены следующие конфигурационные параметры:

- «Идентификатор ПЛК» — идентификатор подключенного ПЛК.
- «IP-адрес подключенного ПЛК» — IP-адрес подключенного ПЛК. Для подключенного ПЛК это собственный IP-адрес сетевого интерфейса резервирования.
- «IP-адрес второго ПЛК» — IP-адрес второго ПЛК. Для подключенного ПЛК это IP-адрес второго (резервного) ПЛК. Данный IP-адрес должен быть доступен для подключенного ПЛК через сетевой интерфейс резервирования.
- «Порт подключения» — номер порта, используемый для передачи данных функции резервирования.

Во вкладке «Таймауты» расположены следующие конфигурационные параметры:

- «Таймаут синхронизации приложения (мс)» — таймаут синхронизации приложения. Допустимый диапазон от 1000 до 30000 мс (1–30 с). Значение по умолчанию 5000 мс (5 с).
- «Таймаут синхронизации данных (мс)» — таймаут синхронизации данных. Допустимый диапазон от 50 до 2000 мс. Значение по умолчанию 500 мс.
- «Таймаут конфигурационных пакетов (мс)» — таймаут конфигурационных пакетов. Допустимый диапазон от 50 до 2000 мс. Значение по умолчанию 400 мс.

Нажатие кнопки «Сохранить и применить», в случае изменения значения какого-либо конфигурационного параметра, приведёт к автоматическому перезапуску ядра ПЛК (CODESYS).

5.5.2.3 Синхронизация конфигураций

В нижней части таблицы конфигураций расположены две кнопки (см. рисунок 5-39), предназначенные для выполнения синхронизации конфигураций между подключенным и вторым (резервным) ПЛК:

- «Сконфигурировать подключенный ПЛК в соответствии с параметрами второго ПЛК...» — синхронизация конфигурации подключенного ПЛК (далее устройство-назначение конфигурации) с использованием конфигурационных параметров второго ПЛК (далее устройство-источник конфигурации).
- «Сконфигурировать второй ПЛК в соответствии с параметрами подключенного ПЛК...» — синхронизация конфигурации второго ПЛК (далее устройство-назначение конфигурации) с использованием конфигурационных параметров подключенного ПЛК (далее устройство-источник конфигурации).

Выполнение синхронизации возможно только при следующих условиях:

- имеется доступ к управлению устройством-источником и устройством-назначением (см. раздел 5.5.1.3);
- конфигурация устройства-источника не имеет не сконфигурированных значений (см. раздел 5.5.2.1).

Если хотя бы одно из условий не выполняется, то соответствующая кнопка синхронизации будет не активной.

Нажатие кнопки синхронизации конфигурации приведёт к отображению всплывающего окна с подробной информацией о синхронизируемых параметрах, как показано на рисунке 5-43.

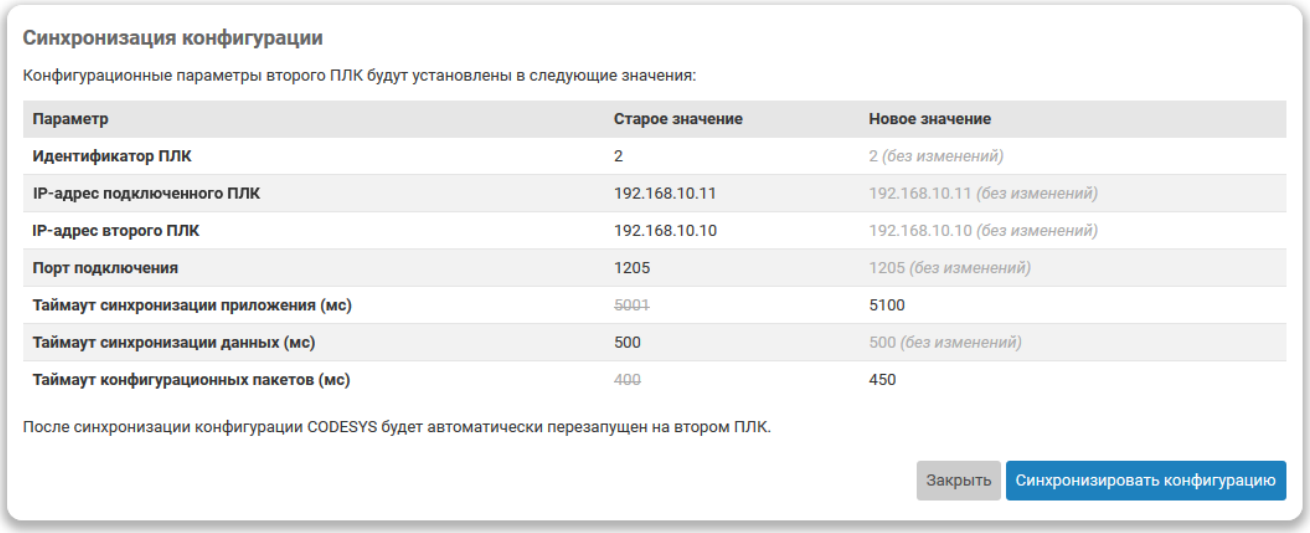


Рис. 5-43: Страница «Резервирование». Окно синхронизации конфигурационных параметров

Во всплывающем окне приводится таблица конфигурационных параметров с их старыми (текущими) значениями (столбец «Старое значение») и новыми значениями (столбец «Новое значение»).

Нажатие кнопки «Синхронизировать конфигурацию» приведёт к выполнению синхронизации конфигурации на устройстве-назначении.

Значения конфигурационных параметров «IP-адрес подключенного ПЛК» и «IP-адрес второго ПЛК» синхронизируются только при выполнении синхронизации второго (резервного) ПЛК с использованием конфигурационных параметров подключенного ПЛК. В обратном направлении данные параметры не синхронизируются.

Нажатие кнопки «Синхронизировать конфигурацию» приведёт к автоматическому перезапуску ядра ПЛК (CODESYS) на устройстве-назначении конфигурации.

Во время выполнения операции синхронизации будет отображаться окно, показанное на рисунке 5-44.

Рис. 5-44: Страница «Резервирование». Выполнение операции синхронизации конфигурации

В случае успешного завершения синхронизации всплывающее окно будет закрыто, а в таблице конфигураций будут отображены значения новых сконфигурированных параметров.

В том случае, если синхронизация конфигурационных параметров не требуется (конфигурации совпадают), внешний вид всплывающего окна при нажатии кнопки синхронизации будет выглядеть, как показано на рисунке 5-45, а кнопка «Синхронизировать конфигурацию» не будет отображена.

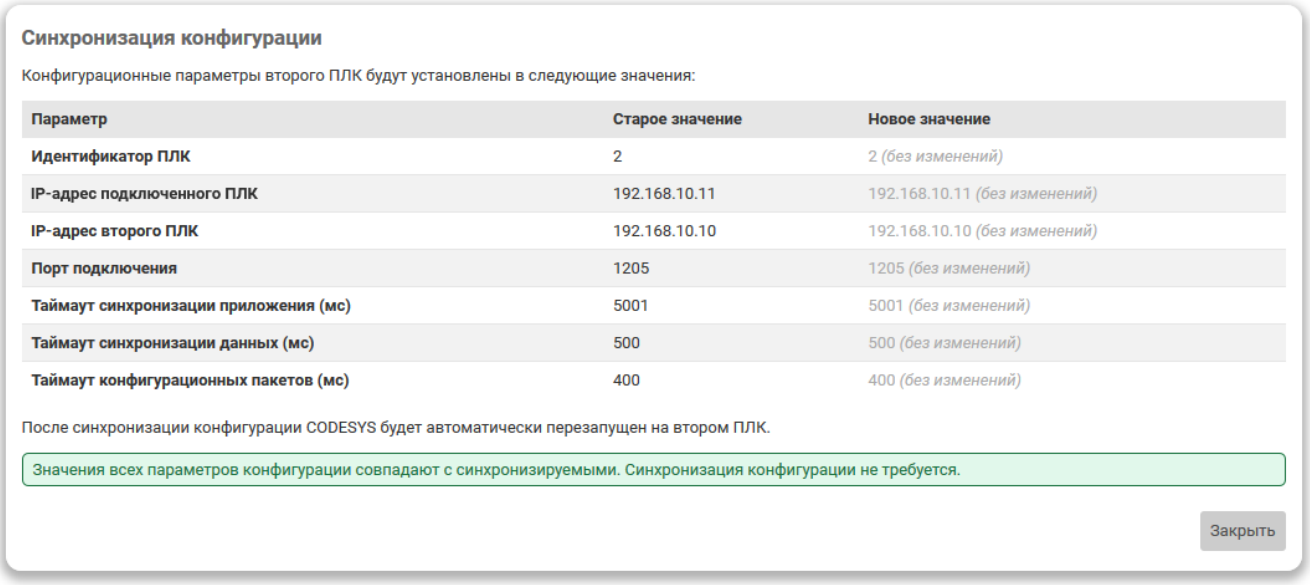


Рис. 5-45: Страница «Резервирование». Окно синхронизации конфигурационных параметров. Синхронизация не требуется

5.6 Файлы журналов

На странице «Файлы журналов» раздела «ПЛК» отображаются данные журналов сообщений среды исполнения CODESYS. Внешний вид страницы «Файлы журналов» показан на рисунке 5-46.

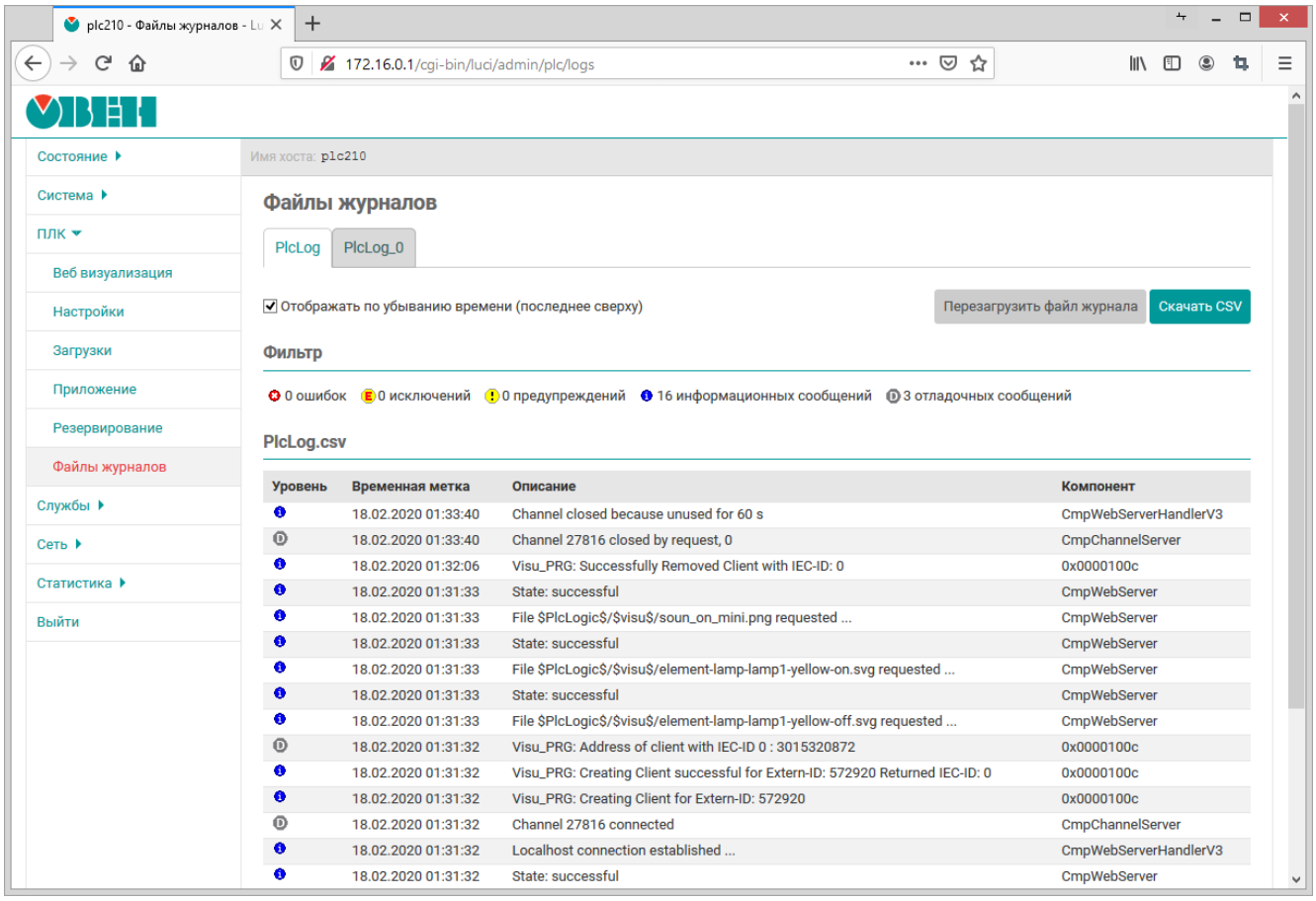


Рис. 5-46: Страница «Файлы журналов»

5.6.1 Основные элементы управления

Все элементы управления расположены в верхней части страницы.

На рисунке 5-46 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 5-47.

Рис. 5-47: 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 [10]. Кнопка «Скачать CSV» позволяет скачать (загрузить) оригинальный файл журнала в формате CSV.

5.6.2 Фильтр записей

В подразделе «Фильтр» расположены элементы управления фильтра отображаемых записей журнала (см. рисунок 5-48).

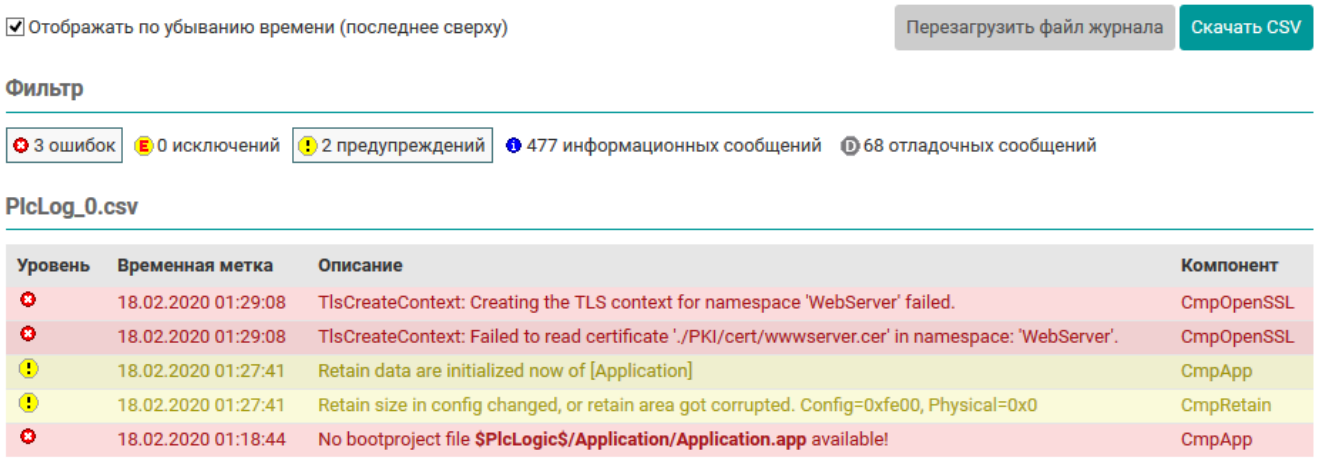


Рис. 5-48: Страница «Файлы журналов». Фильтр записей журнала

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 5-48, 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.

5.6.3 Сообщения журнала

В подразделе с именем файла журнала (например, «PlcLog.csv») отображаются записи журнала в виде таблицы (см. рисунок 5-49).

Таблица записей журнала имеет следующие столбцы:

- «Уровень» — уровень сообщения, представленный в виде графической иконки (соответствие графических иконок уровням сообщений описано в разделе 5.6.2);
- «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»).

PlcLog.csv

Уровень	Временная метка	Описание	Компонент
ℹ	18.02.2020 01:33:40	Channel closed because unused for 60 s	CmpWebServerHandlerV3
Ⓓ	18.02.2020 01:33:40	Channel 27816 closed by request, 0	CmpChannelServer
ℹ	18.02.2020 01:32:06	Visu_PRG: Successfully Removed Client with IEC-ID: 0	0x0000100c
ℹ	18.02.2020 01:31:33	State: successful	CmpWebServer
ℹ	18.02.2020 01:31:33	File $PlcLogic$/$visu$/soun_on_mini.png requested ...	CmpWebServer
ℹ	18.02.2020 01:31:33	State: successful	CmpWebServer
ℹ	18.02.2020 01:31:33	File $PlcLogic$/$visu$/element-lamp-lamp1-yellow-on.svg requested ...	CmpWebServer
ℹ	18.02.2020 01:31:33	State: successful	CmpWebServer
ℹ	18.02.2020 01:31:33	File $PlcLogic$/$visu$/element-lamp-lamp1-yellow-off.svg requested ...	CmpWebServer
Ⓓ	18.02.2020 01:31:32	Visu_PRG: Address of client with IEC-ID 0 : 3015320872	0x0000100c
ℹ	18.02.2020 01:31:32	Visu_PRG: Creating Client successful for Extern-ID: 572920 Returned IEC-ID: 0	0x0000100c
ℹ	18.02.2020 01:31:32	Visu_PRG: Creating Client for Extern-ID: 572920	0x0000100c
Ⓓ	18.02.2020 01:31:32	Channel 27816 connected	CmpChannelServer
ℹ	18.02.2020 01:31:32	Localhost connection established ...	CmpWebServerHandlerV3
ℹ	18.02.2020 01:31:32	State: successful	CmpWebServer
ℹ	18.02.2020 01:31:32	File $PlcLogic$/$visu$/application.imagepoolcollection.csv requested ...	CmpWebServer
ℹ	18.02.2020 01:31:32	State: successful	CmpWebServer
ℹ	18.02.2020 01:31:32	File $PlcLogic$/$visu$/webvisu.cfg.json requested ...	CmpWebServer
ℹ	18.02.2020 01:31:31	State: successful	CmpWebServer

Рис. 5-49: Страница «Файлы журналов». Таблица записей журнала

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.

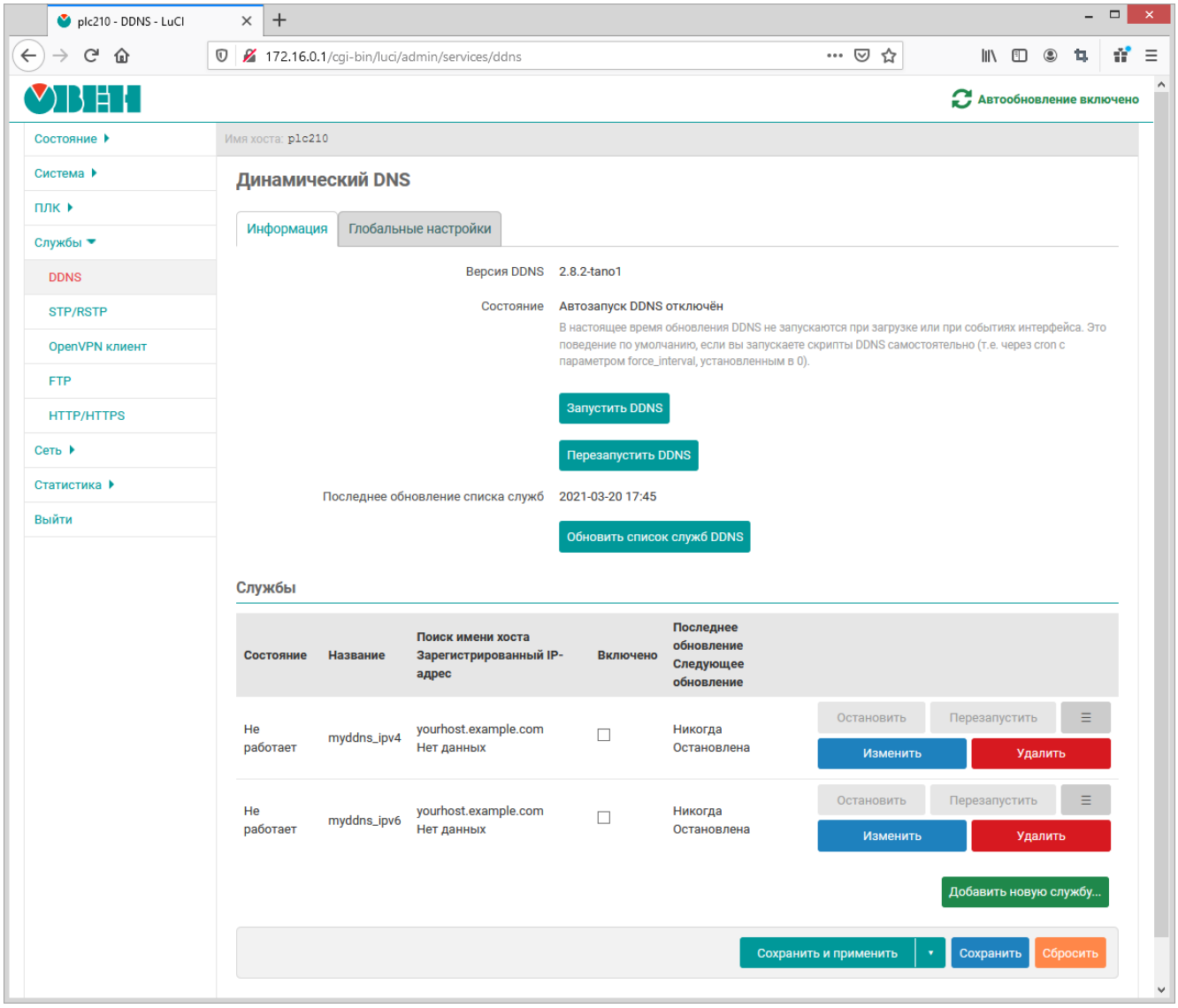


Рис. 6-1: Страница «DDNS»

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

Верхняя часть страницы «DDNS» имеет две вкладки:

- «Информация» (см. раздел 6.1.1);
- «Глобальные настройки» (см. раздел 6.1.2).

В нижней части страницы расположена таблица со списком настроенных DDNS служб (см. раздел 6.1.3).

6.1.1 Информация

Внешний вид вкладки «Информация» страницы «DDNS» показан на рисунке 6-2.

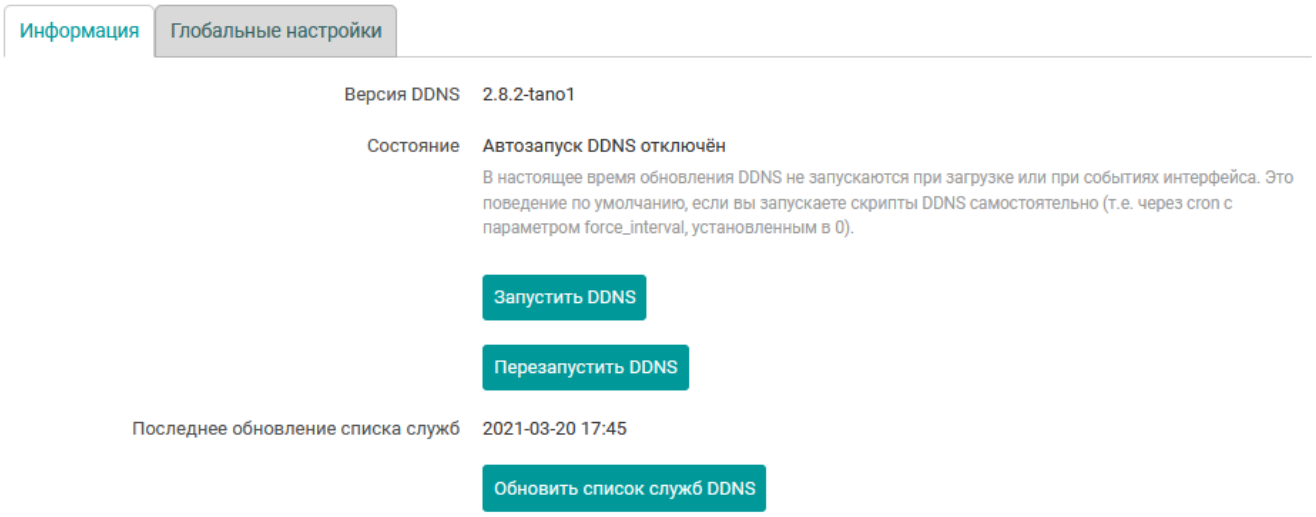


Рис. 6-2: Страница «DDNS». Вкладка «Информация». Автозапуск службы выключен

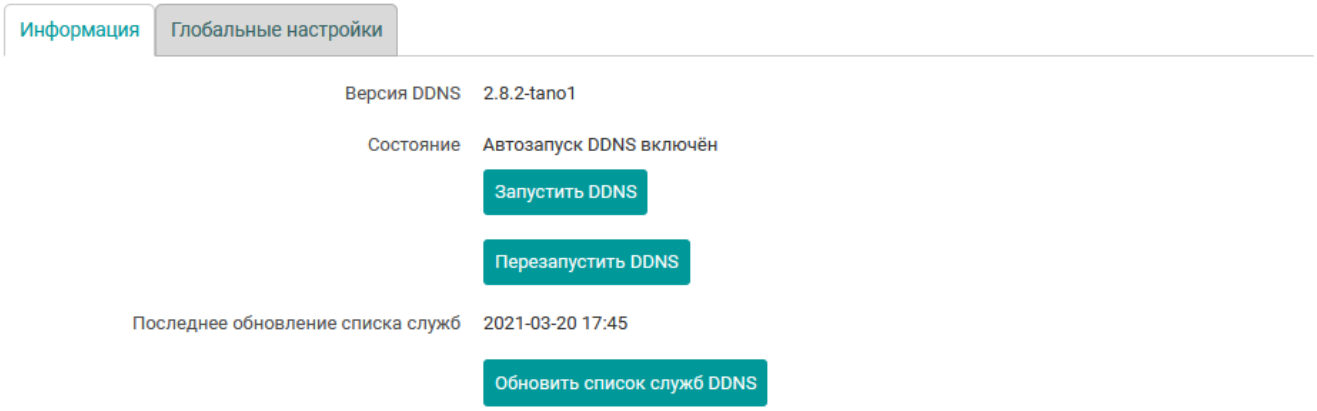


Рис. 6-3: Страница «DDNS». Вкладка «Информация». Автозапуск службы включён

В данной вкладке приведена информация о версии установленного пакета DDNS и о текущем состоянии автоматического запуска службы DDNS.

В том случае, если автоматический запуск службы DDNS отключён, как показано на рисунке 6-2, то в подразделе «Информация» будет отображена кнопка «Запустить DDNS», которая запускает службу DDNS, а также включает автоматический запуск службы при загрузке системы.

При включенной автоматической загрузке службы DDNS при запуске системы, внешний вид подраздела «Информация» будет выглядеть как показано на рисунке 6-3.

При включенном автоматическом запуске службы DDNS будет отображена кнопка «Остановить DDNS», которая останавливает службу DDNS, а также выключает автоматический запуск службы при загрузке системы.

Кнопка «Перезапустить DDNS» позволяет выполнить перезапуск (или запуск, если не запущена) службы DDNS. Состояние автоматического запуска службы при использовании кнопки «Перезапустить DDNS» не изменяется.

6.1.2 Глобальные настройки

Во вкладке «Глобальные настройки» содержаться некоторые общие настройки службы динамического DNS. Внешний вид вкладки «Глобальные настройки» страницы «DDNS» показан на рисунке 6-4.

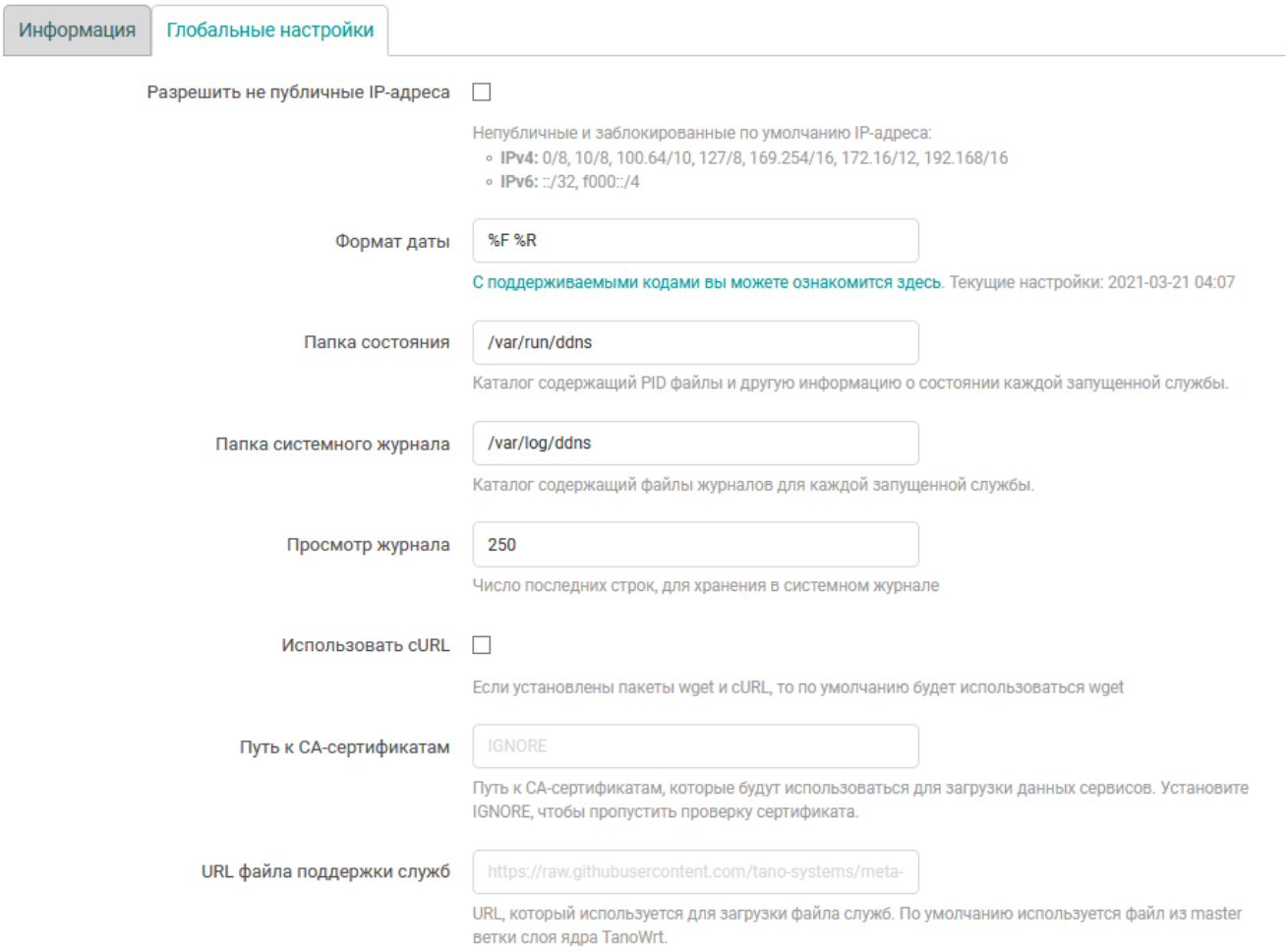


Рис. 6-4: Страница «DDNS». Вкладка «Глобальные настройки»

В данной вкладке расположены следующие глобальные настройки:

- «Разрешить не публичные IP-адреса» — разрешить использование непубличных IP-адресов (по умолчанию запрещены):
  - для IPv4:
    - 0/8
    - 10/8
    - 100.64/10
    - 127/8
    - 169.254/16
    - 172.16/12
    - 192.168/16
  - для IPv6:
    - ::/32
    - f000::/4
- «Формат даты» — строка специальных спецификаторов, определяющая формат вывода даты и времени в таблице сконфигурированных DDNS служб (см. раздел 6.1.3, столбец «Последнее обновление / Следующее обновление»).

С подробным описанием доступных спецификаторов формата можно ознакомится в описании к C++ функции `strftime()` [11].

- «Папка состояния» — путь к папке, в которой хранятся файлы состояний сконфигурированных DDNS служб.
- «Папка системного журнала» — путь к папке, в которой хранятся файлы журналов сконфигурированных DDNS служб.
- «Просмотр журнала» — количество сохраняемых строк в системных журналах DDNS служб.
- «Использовать cURL» — настройка позволяет включить использование утилиты curl вместо wget в том случае, если в системе установлены обе утилиты. По умолчанию, если в системе установлены и curl и wget, будет использоваться утилита wget.
- «Путь к CA-сертификатам» — путь к CA-сертификатам, которые будут использоваться для загрузки данных сервисов. Установите значение «IGNORE», чтобы пропустить проверку сертификата.
- «URL файла поддержки служб» — URL, который используется для загрузки файла служб. По умолчанию используется файл из master ветки слоя ядра TanoWrt.

6.1.3 Службы

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

- «Состояние» — текущее состояние DDNS службы. Может принимать следующие значения:
  - «Не работает» — данная DDNS служба не работает (остановлена);
  - «Работает» — DDNS служба работает. В этом случае, во второй строке под надписью «Работает» будет отображён идентификатор процесса (PID) данной службы.
- «Название» — произвольное имя данной DDNS службы;
- «Поиск имени хоста / Зарегистрированный IP-адрес» — отображает доменное имя данной DDNS службы и определённый для него IP-адрес при последней проверке;
- «Включено» — признак включения соответствующей DDNS службы. Если данная опция отключена, для данной службы скрипт обновления не запускается;
- «Последнее обновление / Следующее обновление» — дата и время последнего и следующего планового обновления информации данной DDNS службы. По умолчанию дата и время отображаются в формате:

  ```
  ГГГГ-ММ-ДД чч:мм
  ```

  где
  - ГГГГ — год;
  - ММ — месяц (от 01 до 12);
  - ДД — день (от 01 до 31);
  - чч — часы (от 00 до 23);
  - мм — минуты (от 00 до 59);

  Формат отображения даты и времени можно настроить в подразделе «Глобальные настройки» при помощи настройки «Формат даты» (см. раздел 6.1.2);
- В последнем столбце расположены следующие кнопки управления DDNS службами:
  - «Остановить» — предназначена для остановки работы соответствующей DDNS службы. Если DDNS служба в текущий момент не запущена, данная кнопка не активна.
  - «Перезапустить» — предназначена для перезапуска соответствующей DDNS службы. Если DDNS службы в текущий момент не запущена, данная кнопка не активна.
  - «Изменить» — предназначена для редактирования параметров (настроек) соответствующей DDNS службы (см. раздел 6.1.3.1).
  - «Удалить» — предназначена для удаления DDNS службы (см. раздел 6.1.3.3).

6.1.3.1 Редактирование настроек DDNS службы

Для редактирования настроек DDNS службы необходимо нажать кнопку «Изменить» для соответствующей службы в таблице подраздела «Службы» на странице «DDNS» (см. рисунок 6-5).

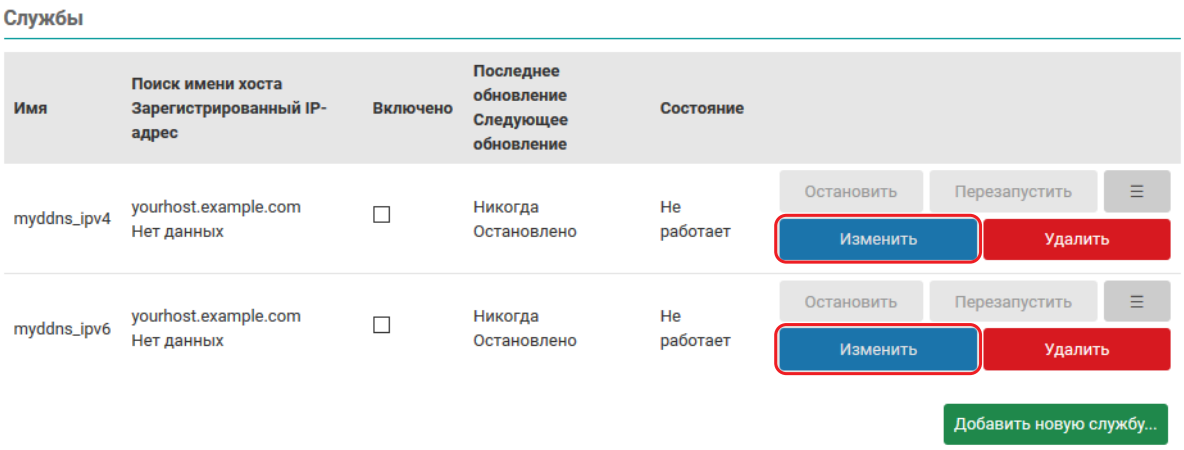


Рис. 6-5: Страница «DDNS». Кнопки изменения настроек службы

При нажатии кнопки «Изменить» будет открыто всплывающее окно редактирования настроек соответствующей DDNS службы, как показано на рисунке 6-6.

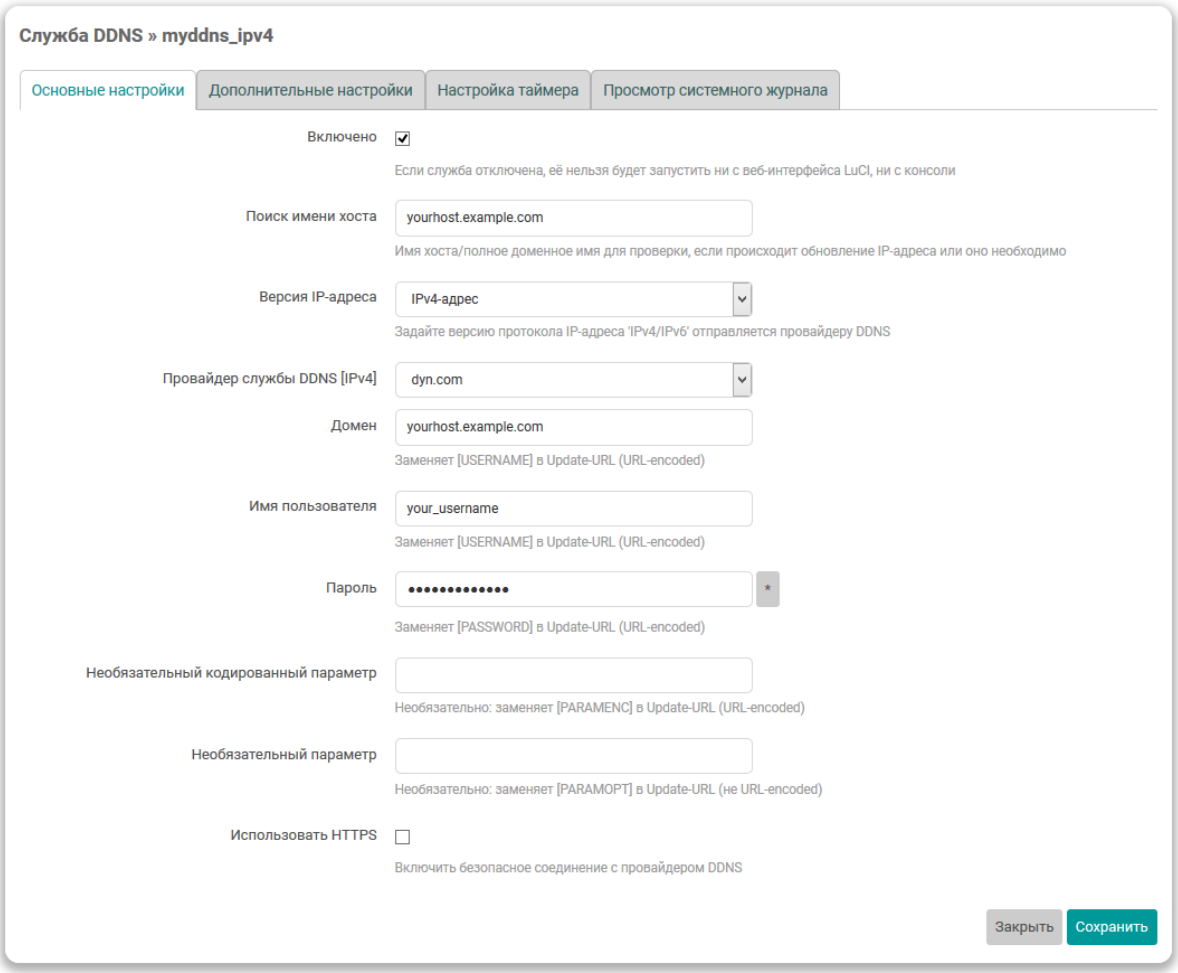


Рис. 6-6: Окно редактирования настроек DDNS службы

Настройки DDNS службы распределены по четырём вкладкам:

- «Основные настройки» (см. раздел 6.1.3.1.1);
- «Дополнительные настройки» (см. раздел 6.1.3.1.2);
- «Настройка таймера» (см. раздел 6.1.3.1.3);
- «Просмотр системного журнала» (см. раздел 6.1.3.1.4).

6.1.3.1.1 Вкладка «Основные настройки»

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

На вкладке размещены основные настройки DDNS службы:

- «Включено» — глобальный флаг активации редактируемой службы DDNS. Если эта опция отключена, то скрипт обновления для данной DDNS службы 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 службы;
- «Версия IP-адреса» — выбор версии IP протокола DDNS службы;
- «Провайдер службы DDNS» — выбор провайдера службы DDNS.

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

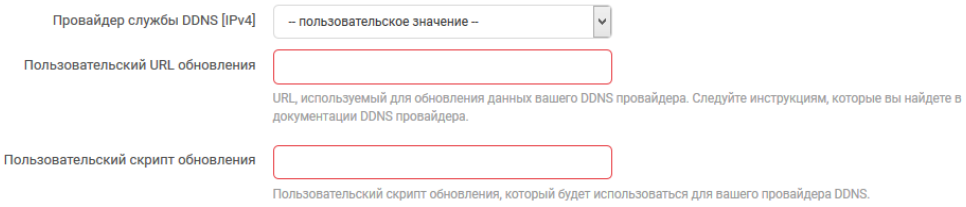


Рис. 6-7: Настройки пользовательского DDNS провайдера

  В поле «Пользовательский URL обновления» указывается URL адрес обновления DDNS службы, 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 информации DDNS службы;
- «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.

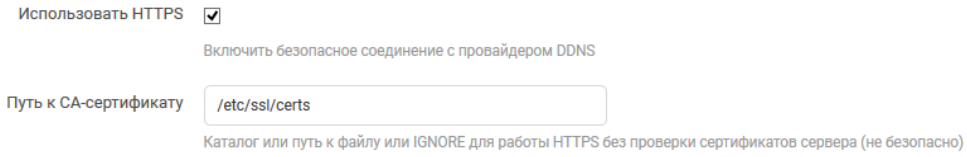


Рис. 6-8: Настройка «Путь к CA-сертификату» DDNS службы

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

6.1.3.1.2 Вкладка «Дополнительные настройки»

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

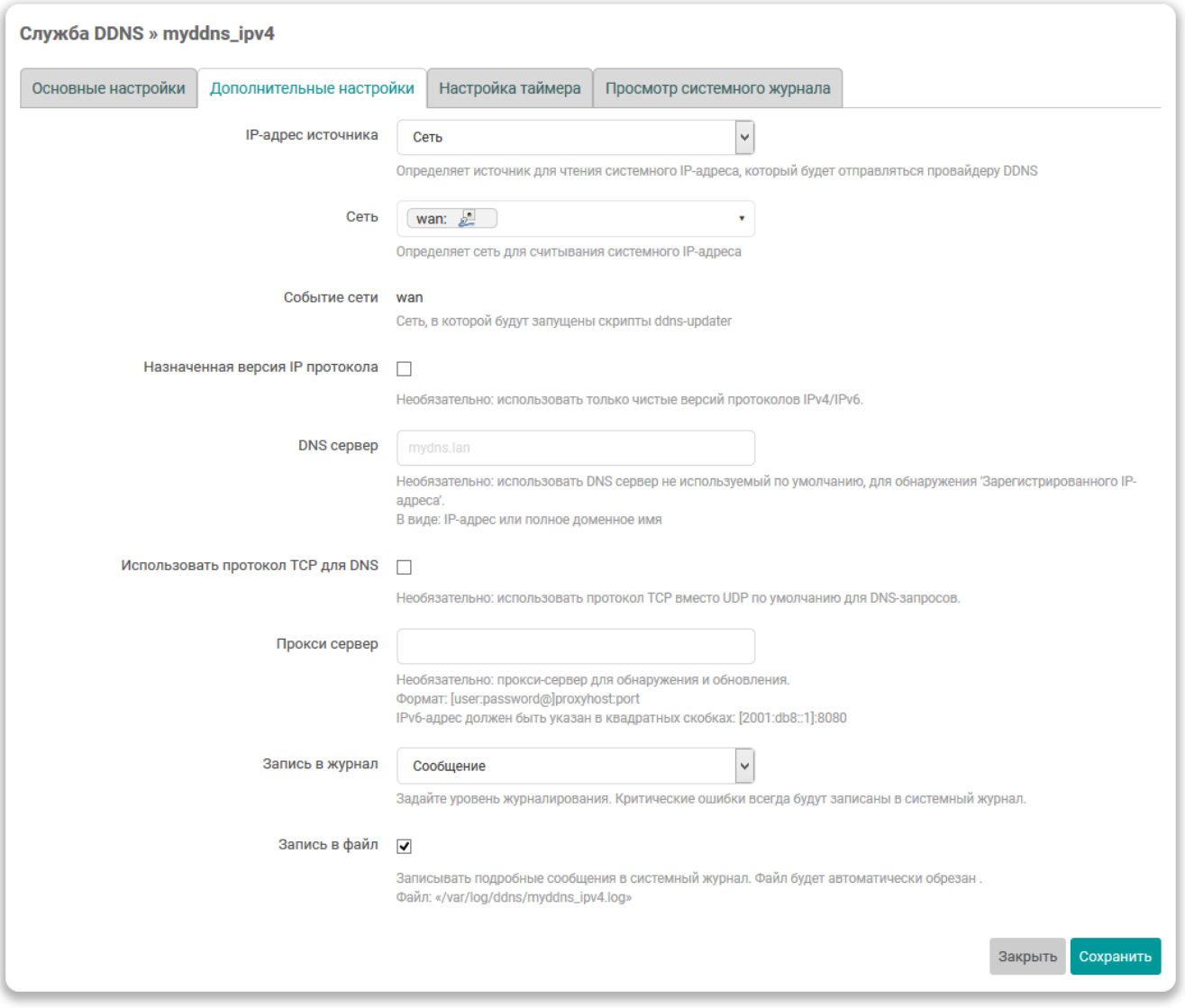


Рис. 6-9: Вкладка «Дополнительные настройки» окна редактирования DDNS службы

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

- «IP-адрес источника» — выбор источника для определения IP-адреса домена данной DDNS службы. Возможен выбор одного из следующих источников:
  - «Сеть» — источником IP-адреса выступает сеть, выбранная в выпадающем списке «Сеть» (см. рисунок 6-10).

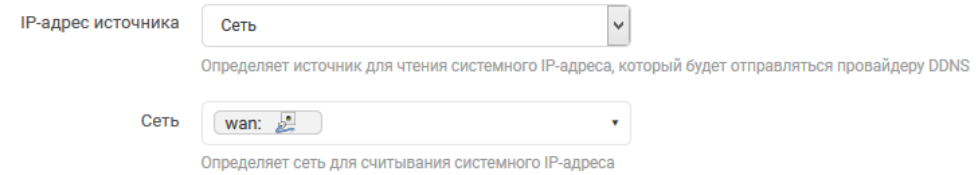


Рис. 6-10: Настройки DDNS службы для источника IP-адреса «Сеть»

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

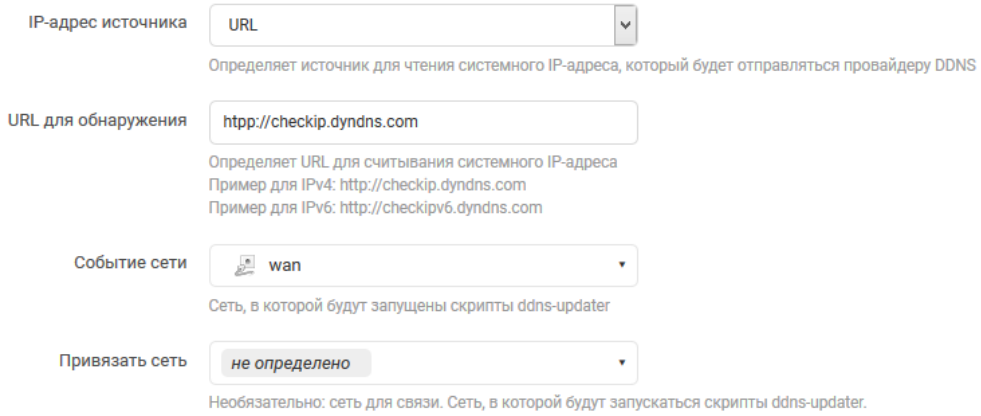


Рис. 6-11: Настройки DDNS службы для источника IP-адреса «URL»

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

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);

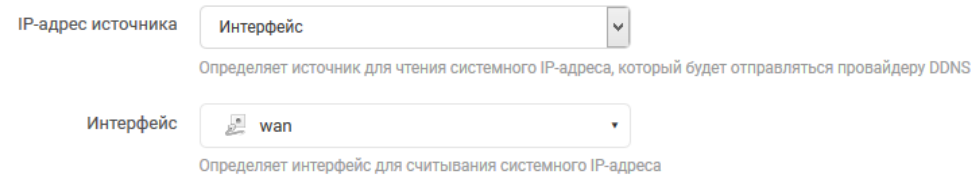


Рис. 6-12: Настройки DDNS службы для источника IP-адреса «Интерфейс»

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

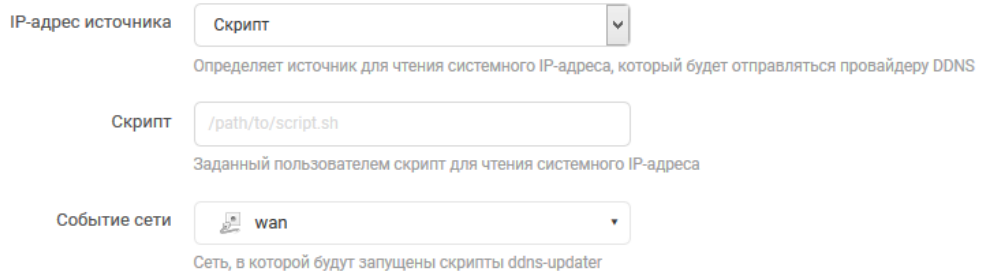


Рис. 6-13: Настройки DDNS службы для источника IP-адреса «Скрипт»

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

- «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 6.1.3.1.1);
- «DNS сервер» — адрес DNS-сервера для определения зарегистрированного IP адреса для данной DDNS службы. Если не задано, то будет использован DNS сервер по умолчанию;
- «Использовать протокол TCP для DNS» — установка данной опции включает использование TCP вместо UDP для DNS запросов;
- «Прокси сервер» — адрес прокси сервера для обнаружения и обновления информации DDNS службы. 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 службы в файл.

6.1.3.1.3 Вкладка «Настройка таймера»

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

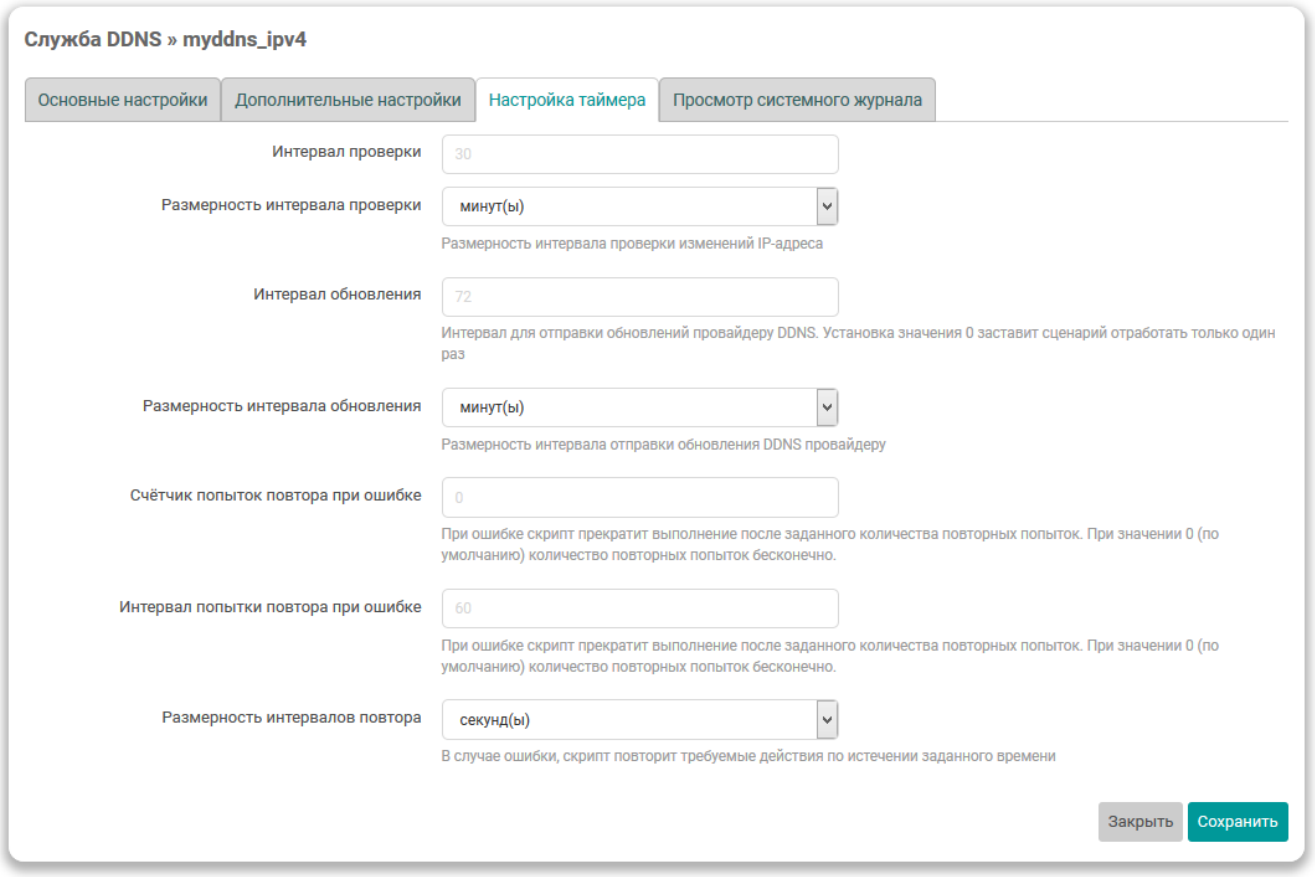


Рис. 6-14: Вкладка «Настройки таймера» окна редактирования DDNS службы

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

- «Интервал проверки» — интервал проверки изменения IP-адреса DDNS службы. Интервал проверки не должен быть менее 5 минут;
- «Размерность интервала проверки» — размерность значения интервала проверки, указанного в поле «Интервал проверки». Данный интервал может указываться в секундах (значение «секунд(ы)»), минутах (значение «минут(ы)») или часах (значение «часа(ов)»);
- «Интервал обновления» — интервал для отправки обновлений провайдеру DDNS. При установке значения «0», провайдеру DDNS будет отправлено обновление только один раз;
- «Размерность интервала обновления» — размерность значения интервала обновления, указанного в поле «Интервал обновления». Данный интервал может указываться в минутах (значение «минут(ы)»), часах (значение «часа(ов)») или днях (значение «дни»);
- «Счётчик 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.
- «Размерность интервалов повтора» — размерность значения интервала попыток повтора при ошибки, указанного в поле «Интервал попытки повтора при ошибке». Данный интервал может указываться в секундах (значение «секунд(ы)») или минутах (значение «минут(ы)»).

6.1.3.1.4 Вкладка «Просмотр системного журнала»

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

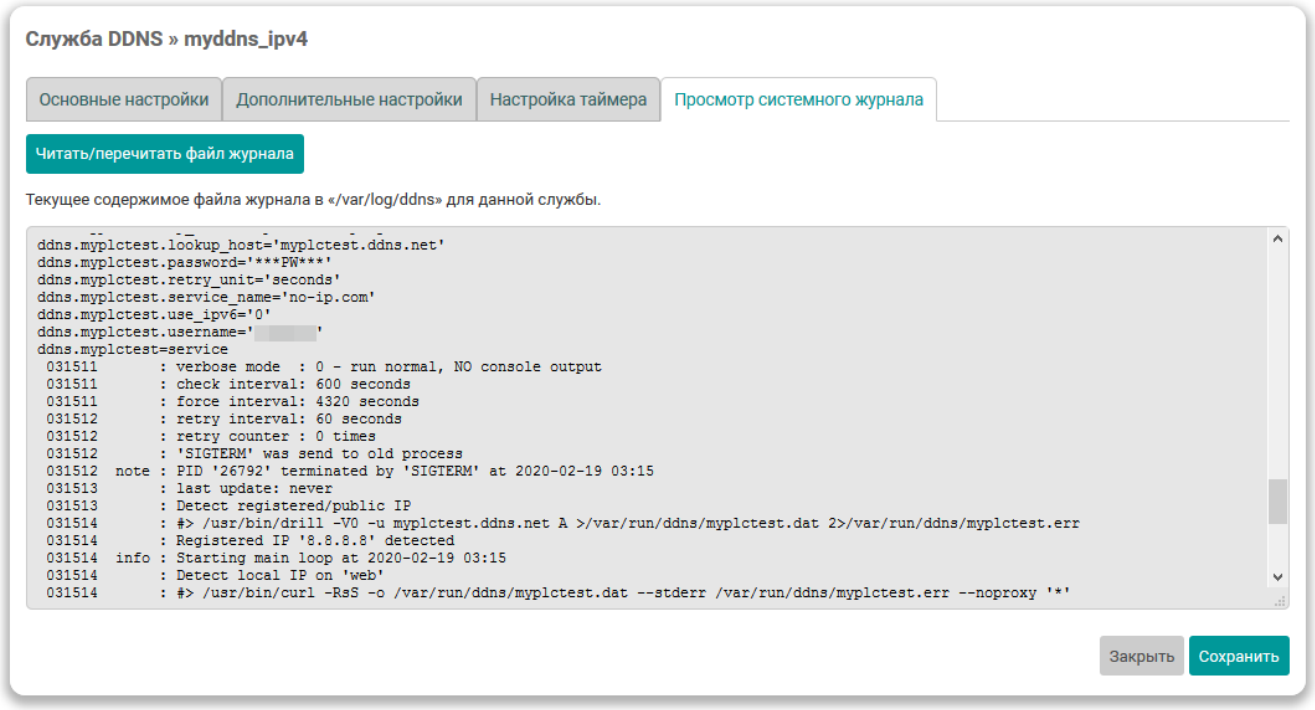


Рис. 6-15: Вкладка «Просмотр системного журнала» окна редактирования DDNS службы

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

Кнопка «Читать/перечитать системный журнал» предназначена для первичного чтения или перечитывания содержимого файла системного журнала.

6.1.3.2 Добавление новой DDNS службы

Для добавления новой DDNS службы необходимо нажать кнопку «Добавить новую службу...», расположенную под таблицей DDNS служб подраздела «Службы» страницы «DDNS» (см. рисунок 6-16).

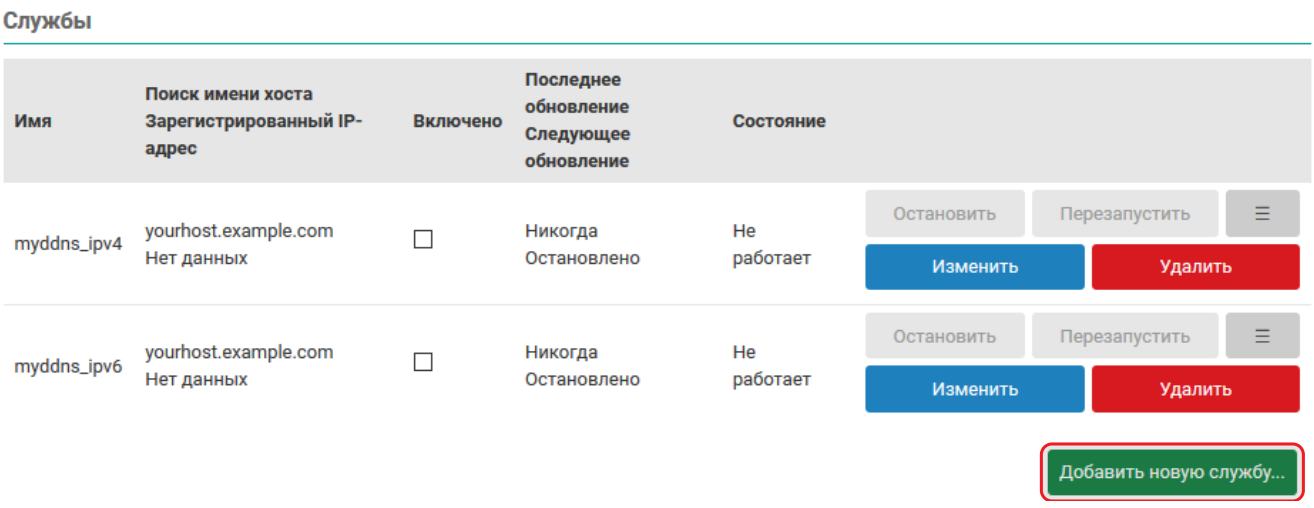


Рис. 6-16: Страница «DDNS». Кнопка добавления службы

После нажатия кнопки «Добавить новую службу...» откроется всплывающее окно, в котором необходимо ввести имя новой DDNS службы и нажать кнопку «Создать службу» (см. рисунок 6-17).

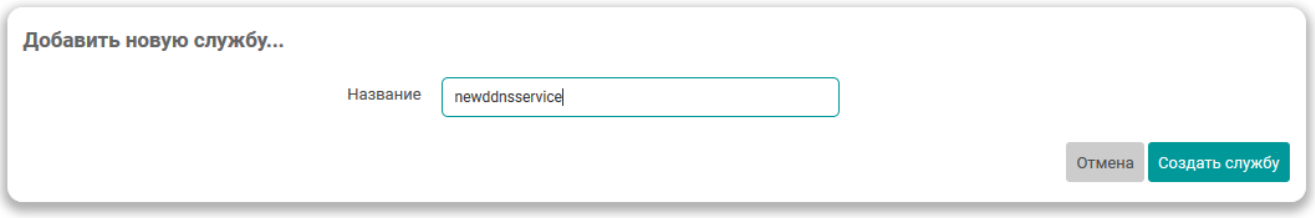


Рис. 6-17: Страница «DDNS». Окно добавления новой службы

После нажатия кнопки «Создать службу» откроется окно редактирования настроек новой DDNS службы, которое подробно рассмотрено в разделе 6.1.3.1.

6.1.3.3 Удаление DDNS службы

Для удаления DDNS службы необходимо нажать кнопку «Удалить» для соответствующей службы в таблице подраздела «Службы» на странице «DDNS» (см. рисунок 6-18).

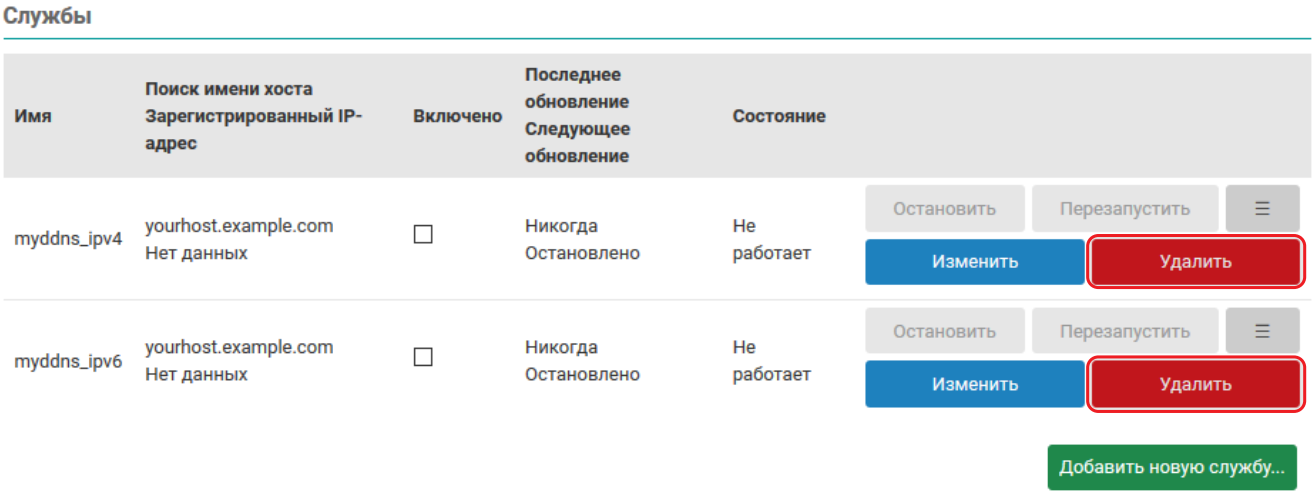


Рис. 6-18: Страница «DDNS». Кнопки удаления службы

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 6-19.

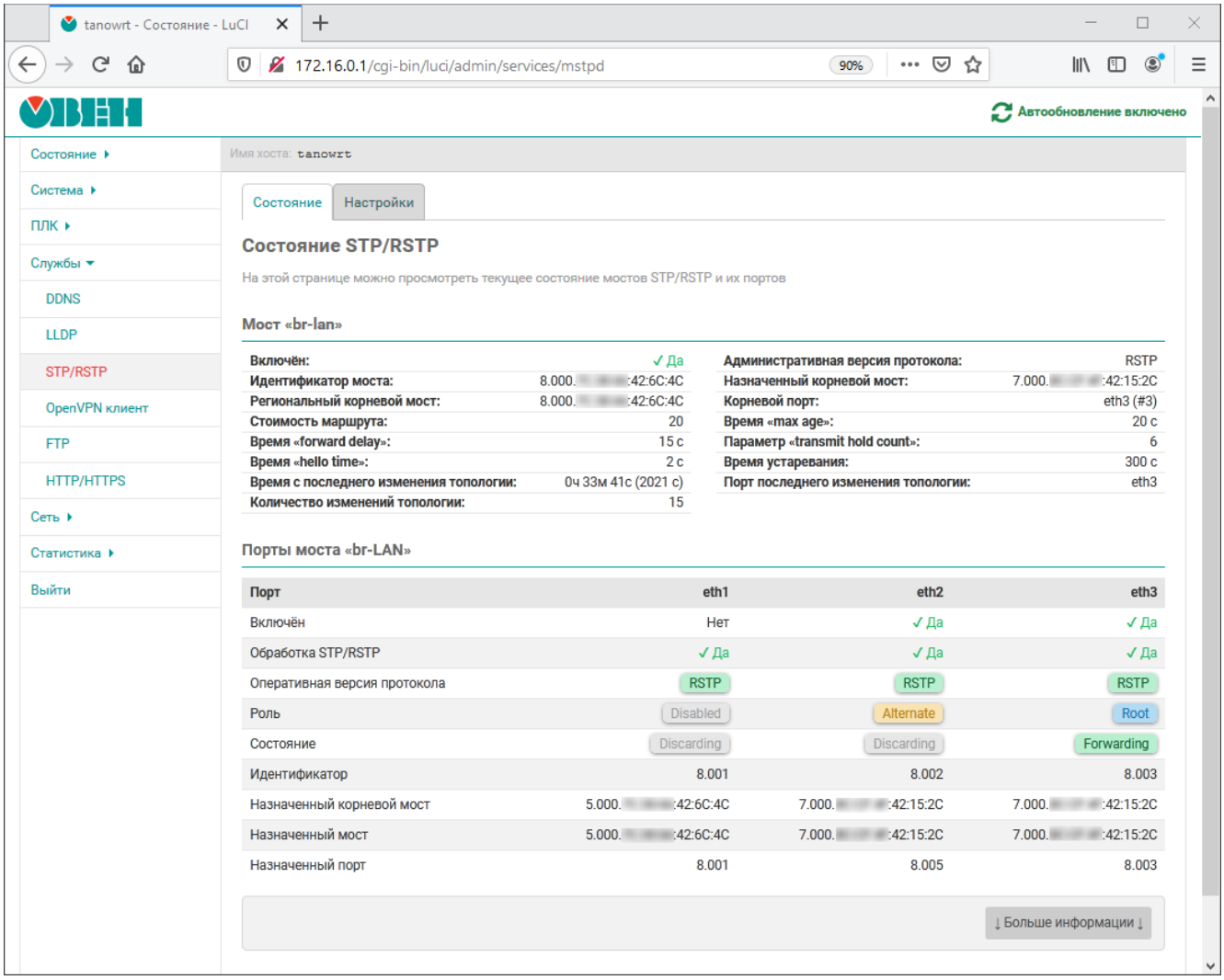


Рис. 6-19: Страница «STP/RSTP»

Состояние и настройки службы STP/RSTP разделены на соответствующие вкладки, расположенные в верхней части страницы (см. рисунок 6-19):

- «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 6-20):

1) вкладки выбора моста, для которого необходимо отобразить информацию о текущем состоянии (если сконфигурирован только один мост с использованием протоколов STP/RSTP, то вкладки выбора моста будут отсутствовать);
2) состояние выбранного моста в виде списка параметров моста и их текущих значений;
3) состояние портов выбранного моста в виде таблицы.

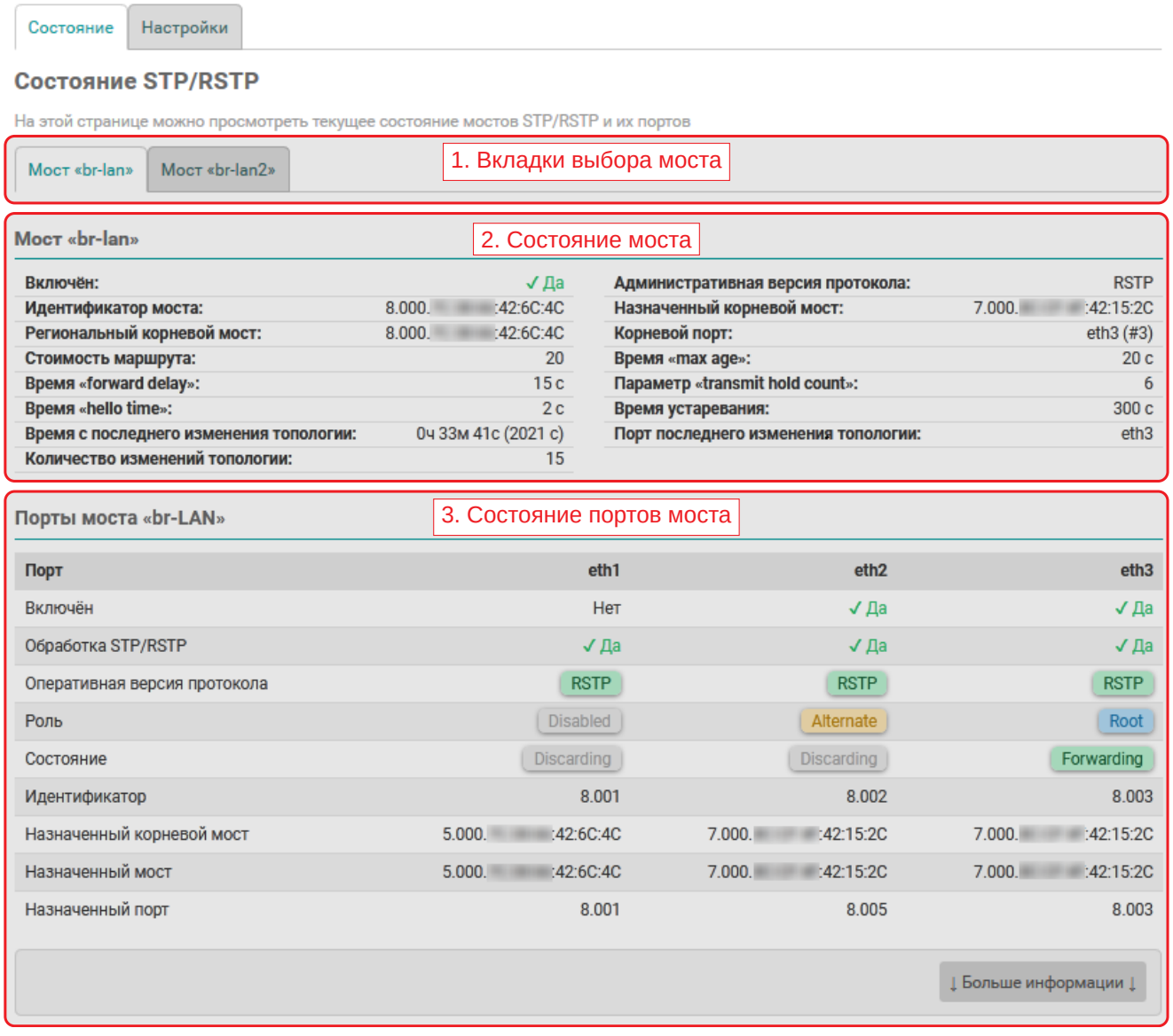


Рис. 6-20: Страница «STP/RSTP». Вкладка «Состояние»

Мост, для которого отображается состояние, выбирается при помощи вкладок с названием моста (позиция 1 на рисунке 6-20).

В области состояния моста (позиция 2 на рисунке 6-20) отображаются следующие параметры:

- «Включён» — состояние включения моста (да или нет);
- «Идентификатор моста» — идентификатор моста, состоящий из приоритета моста и собственного MAC-адреса моста. Отображается в формате:

  ```
  8.000.7C:38:66:42:6C:4C
  ```

  где:

    - `8.000` — приоритет моста;
    - `7C:38:66:42:6C:4C` — MAC-адрес моста.
- «Региональный корневой мост» — идентификатор текущего регионального корневого моста. Формат отображаемого значения соответствует формату параметра «Идентификатор моста»;
- «Стоимость маршрута» — текущая стоимость маршрута до корневого моста;
- «Время „forward delay“» — текущее значение параметра «forward delay». Параметр определяет время перехода корневых (Root) и назначенных (Designated) портов моста в состояние Forwarding;
- «Время „hello time“» — текущее значение времени «hello time». Определяет интервал времени между периодическими отправками конфигурационных сообщений BPDU в назначенные (Designated) порты;
- «Время с последнего изменения топологии» — время, прошедшее с последнего изменения топологии;
- «Количество изменений топологии» — количество изменений топологии;
- «Административная версия протокола» — сконфигурированная администратором версия протокола:
    - STP;
    - RSTP;
- «Назначенный корневой мост» — идентификатор текущего назначенного 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;
- «Параметр „max age“» — текущее значение параметра «max age». Определяет максимальный возраст информации, передаваемой через мост тогда, когда он является корневым;
- «Параметр „transmit hold count“» — текущее значение параметра «transmit hold delay»;
- «Время устаревания» — текущее значение времени устаревания для моста (ageing time). Определяет время жизни записей (в секундах) в динамической таблице MAC-адресов;
- «Порт последнего изменения топологии» — имя порта, инициировавшего последнее изменение топологии.

В области состояния портов моста (позиция 3 на рисунке 6-20) расположена таблица, столбцы которой представляют собой порты моста, а в строках перечислены отображаемые параметры:

- «Включён» — состояние порта (да или нет);
- «Обработка STP/RSTP» — включена ли обработка STP/RSTP пакетов на порту (да или нет). Данный параметр управляется конфигурируемой опцией порта «Фильтр BPDU» (см. раздел 6.2.2.2);
- «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 6-21(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 6-21(б));

(а) Оперативное состояние совпадает с административным

(б) Оперативное состояние отличается от административного

Рис. 6-21: Отображение оперативной версии протокола порта моста

- «Роль» — текущая STP/RSTP роль порта. Порт может иметь одну из следующих ролей:
    - Designated — назначенный порт (рисунок 6-22(а));
    - Alternate — альтернативный порт (рисунок 6-22(б));
    - Root — корневой порт (рисунок 6-22(в));
    - Backup — резервный порт (рисунок 6-22(г));
    - Disabled — порт отключён (рисунок 6-22(д)).

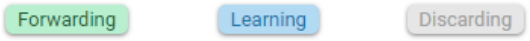
  Каждая роль порта отображается своим цветом, как показано на рисунке 6-22.

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

Рис. 6-22: 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 6-23.



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

Рис. 6-23: 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 «Больше информации», 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;
- «Защита BPDU» — при обнаружении BPDU на порту, порт блокируется (да или нет);
- «Срабатывание защиты BPDU» — количество срабатываний защиты BPDU;
- «Отправлено BPDU» — количество отправленных BPDU пакетов в данный порт;
- «Получено BPDU» — количество полученных BPDU пакетов на данном порту;
- «Получено BPDU (отфильтровано)» — количество полученных BPDU пакетов на данном порту, которые были отфильтрованы;
- «Отправлено TCN» — количество отправленных TCN пакетов в данный порт;
- «Получено TCN» — количество полученных TCN пакетов на данном порту.

На рисунке 6-24 приведён пример внешнего вида таблицы состояния портов моста с включёнными дополнительными параметрами.

Порты моста «br-lan»

Порт	eth1	eth2	eth3
Включён	Нет	✓ Да	✓ Да
Обработка STP/RSTP	✓ Да	✓ Да	✓ Да
Оперативная версия протокола	RSTP	RSTP	RSTP
Роль	Disabled	Alternate	Root
Состояние	Discarding	Discarding	Forwarding
Идентификатор	8.001	8.002	8.003
Назначенный корневой мост	5.000.[redacted]:42:6C:4C	7.000.[redacted]:42:15:2C	7.000.[redacted]:42:15:2C
Назначенный мост	5.000.[redacted]:42:6C:4C	7.000.[redacted]:42:15:2C	7.000.[redacted]:42:15:2C
Назначенный порт	8.001	8.005	8.003
Стоимость маршрута порта	200000	30	20
Административное пограничнное состояние	✓ Да	✓ Да	✓ Да
Автоматическое пограничное состояние	✓ Да	✓ Да	✓ Да
Оперативное пограничное состояние	✓ Да	Нет	Нет
Административное P2P состояние	Автоматически	Автоматически	Автоматически
Оперативное P2P состояние	✓ Да	✓ Да	✓ Да
Защита BPDU	Нет	Нет	Нет
Срабатывание защиты BPDU	Нет	Нет	Нет
Отправлено BPDU	2398	2650	3721
Получено BPDU	4	1486	1493
Получено BPDU (отфильтровано)	–	–	–
Отправлено TCN	3	8	24
Получено TCN	4	14	18

↑ Меньше информации ↑

Рис. 6-24: 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 6-25.

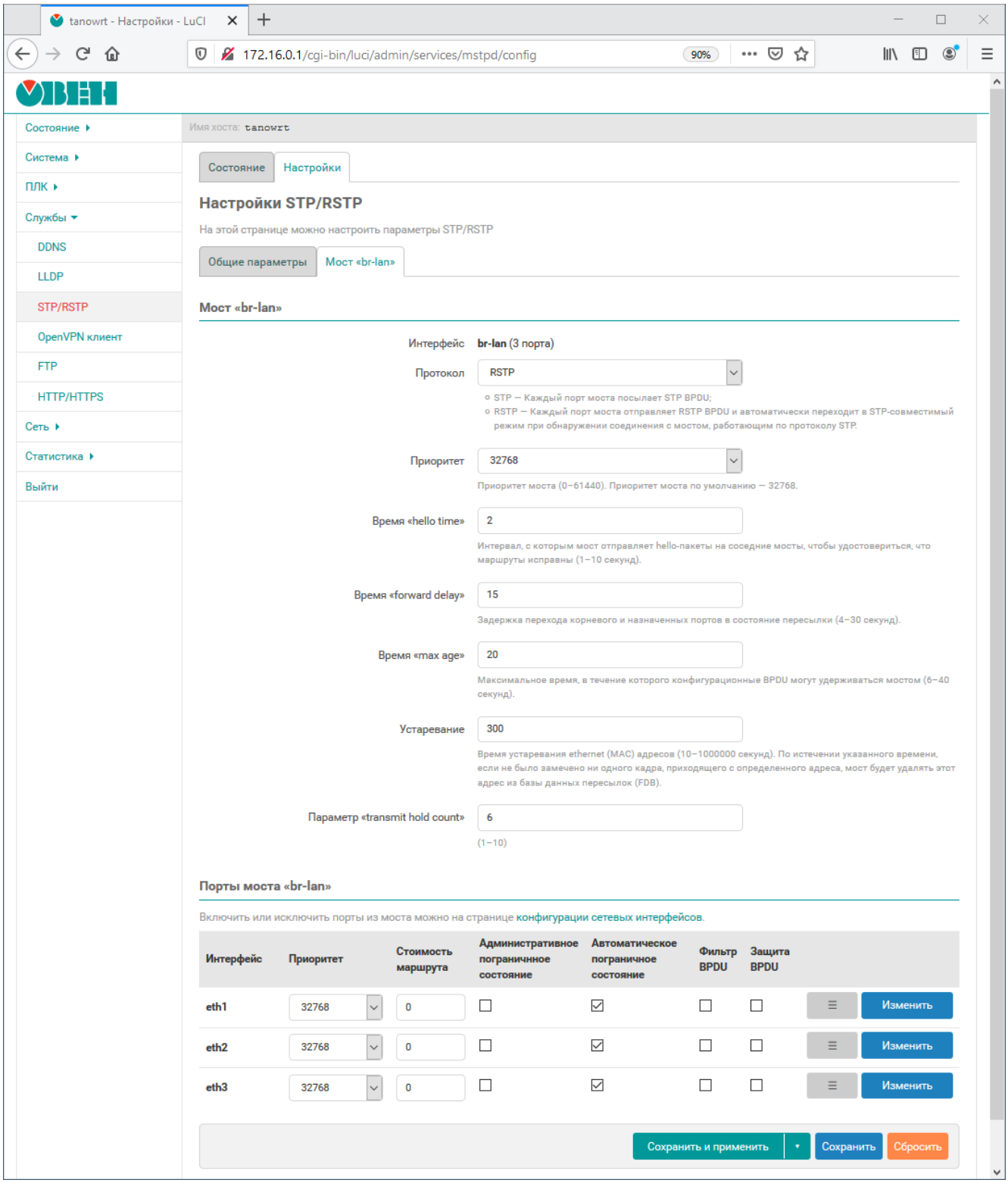


Рис. 6-25: Страница «STP/RSTP». Вкладка «Настройки»

На странице настроек представлены несколько вкладок: «Общие параметры» и вкладки настроек мостов, которые контролируются службой STP/RSTP. Вкладки настроек мостов имеют названия соответствующие названиям сетевых интерфейсов мостов.

6.2.2.1 Общие настройки

Общие настройки расположены во вкладке «Общие настройки» страницы настроек службы STP/RSTP (см. рисунок 6-26).

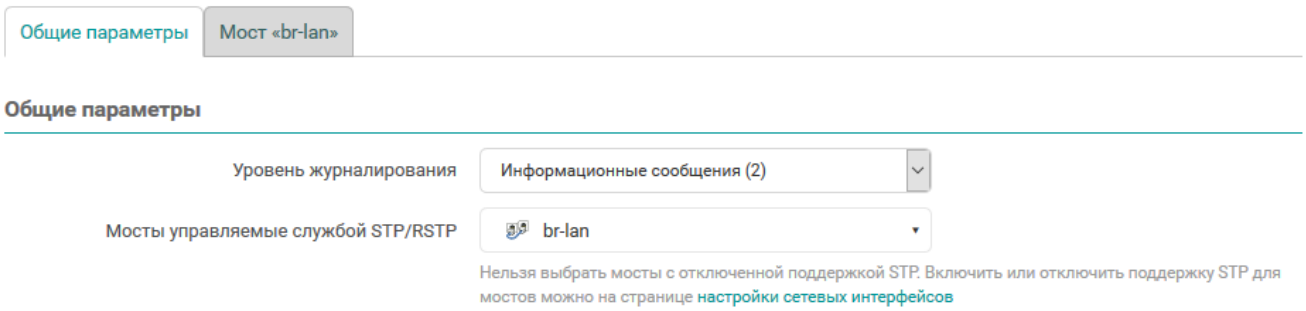


Рис. 6-26: Общие настройки службы STP/RSTP

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;
- «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

На вкладках настроек мостов располагаются 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 разделены на два подраздела:

- подраздел с названием «Мост „имя-моста“» — настройки моста (см. рисунок 6-27);
- подраздел с названием «Порты моста „имя-моста“» — настройки портов моста (см. рисунок 6-28).

В подразделе настроек моста размещены следующие настройки (см. рисунок 6-27):

- «Интерфейс» — имя системного сетевого устройства моста и количество портов (в скобках);
- «Протокол» — выбор административной версии протокола. Поддерживаемые протоколы:
  - STP;
  - RSTP;
- «Приоритет» — выбор приоритета моста;

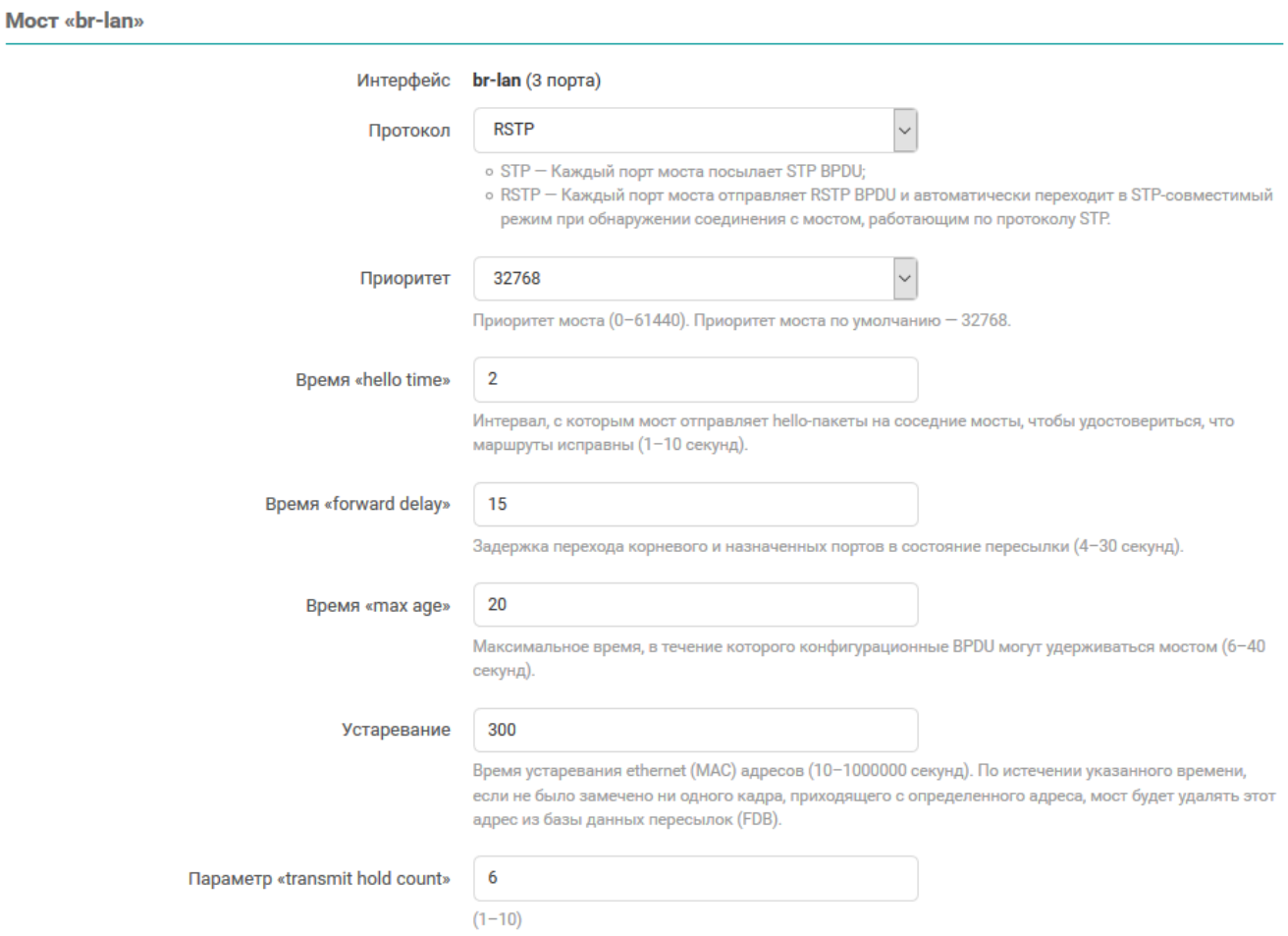


Рис. 6-27: Настройки моста, управляемого службой STP/RSTP

- «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».

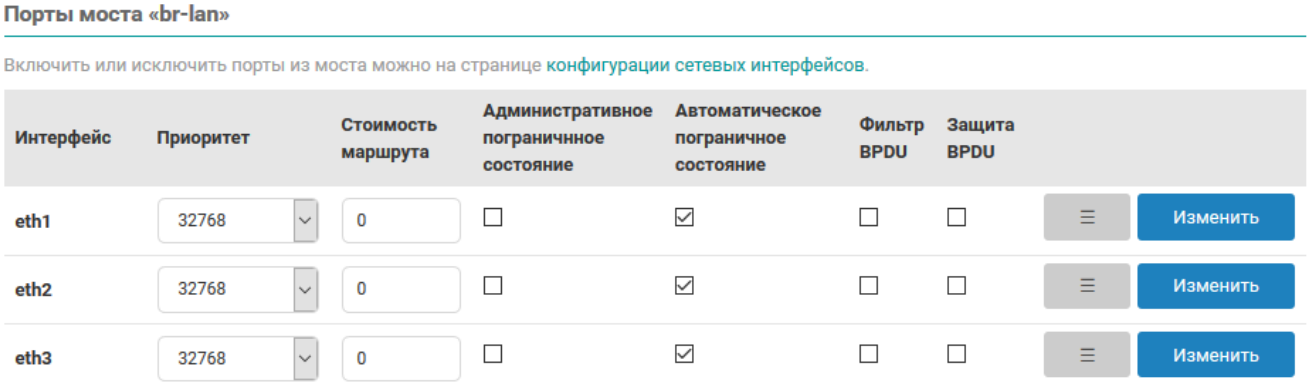


Рис. 6-28: Настройки портов моста, управляемого службой STP/RSTP

В подразделе настроек портов моста отображается список портов моста в виде таблицы (см. рисунок 6-28). Каждая строка таблицы соответствует одному порту моста. В столбцах таблицы размещены элементы управления, позволяющие выполнить конфигурацию следующих основных параметров портов моста:

- «Интерфейс» — имя системного сетевого устройства порта (не конфигурируется);

- «Приоритет» — выбор приоритета порта;
- «Стоимость маршрута» — установка стоимости маршрута порта. Для автоматического определения используется значение «0»;
- «Административное пограничное состояние» — установка административного режима пограничного порта (Edge Port). Возможные значения:
  - включено;
  - выключено.
- «Автоматическое пограничное состояние» — установка режима автоматического определения пограничного порта (Edge Port). Возможные значения:
  - включено;
  - выключено.
- «Фильтр BPDU» — включение или отключение функции BPDU Filtering на порту. Возможные значения:
  - включено;
  - выключено.
- «Защита BPDU» — включение или отключение функции BPDU Guard на порту. Возможные значения:
  - включено;
  - выключено.

Для конфигурации доступны лишь те порты, которые входят в состав конфигурируемого моста. Конфигурация мостов, в том числе включение и/или исключение портов из состава моста осуществляется в настройках сетевых интерфейсов (см. раздел 7.1.1.2).

В последнем столбце таблицы для каждого порта расположены кнопки управления:

- «≡» — кнопка изменения порядка записей в таблице. Удерживая нажатой данную кнопку можно перемещать строку таблицы, изменяя тем самым её порядок.

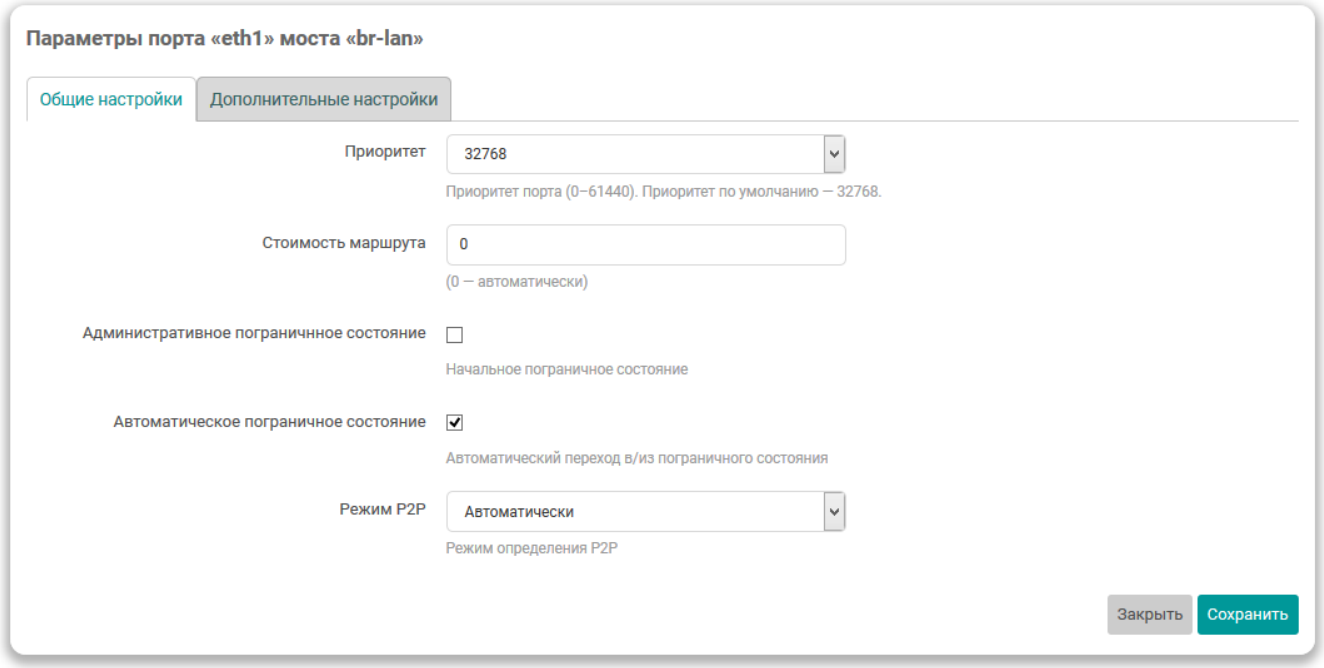
  Порядок расположения портов в таблице не имеет функционального значения и применяется исключительно для удобства и для управления порядком вывода портов моста в таблице состояния (см. раздел 6.2.1).
- «Изменить» — кнопка расширенного редактирования параметров порта.

При нажатии кнопки «Изменить» будет отображено всплывающее окно расширенных настроек соответствующего порта (см. рисунок 6-29).

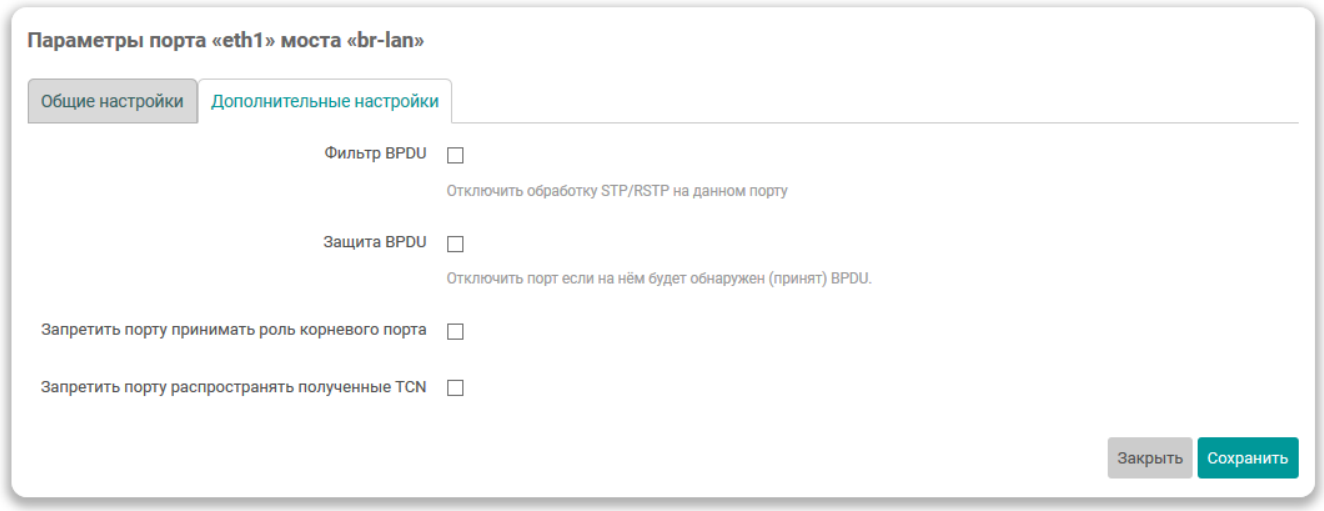
Расширенные настройки разделены на две вкладки — «Общие настройки» (см. рисунок 6-29(а)) и «Дополнительные настройки» (см. рисунок 6-29(б)).

На данных вкладках, помимо уже описанных выше настроек доступных в столбцах таблицы портов моста, расположены следующие дополнительные настройки:

- «Режим 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;
- «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).



(а) Вкладка «Общие настройки»



(б) Вкладка «Дополнительные настройки»

Рис. 6-29: Всплывающее окно расширенных настроек порта моста

6.3 OpenVPN клиент

На странице «OpenVPN клиент» можно выполнить настройку экземпляров OpenVPN клиента и отслеживать текущее состояние активных OpenVPN клиентов. Внешний вид страницы «OpenVPN клиент» показан на рисунке 6-30.

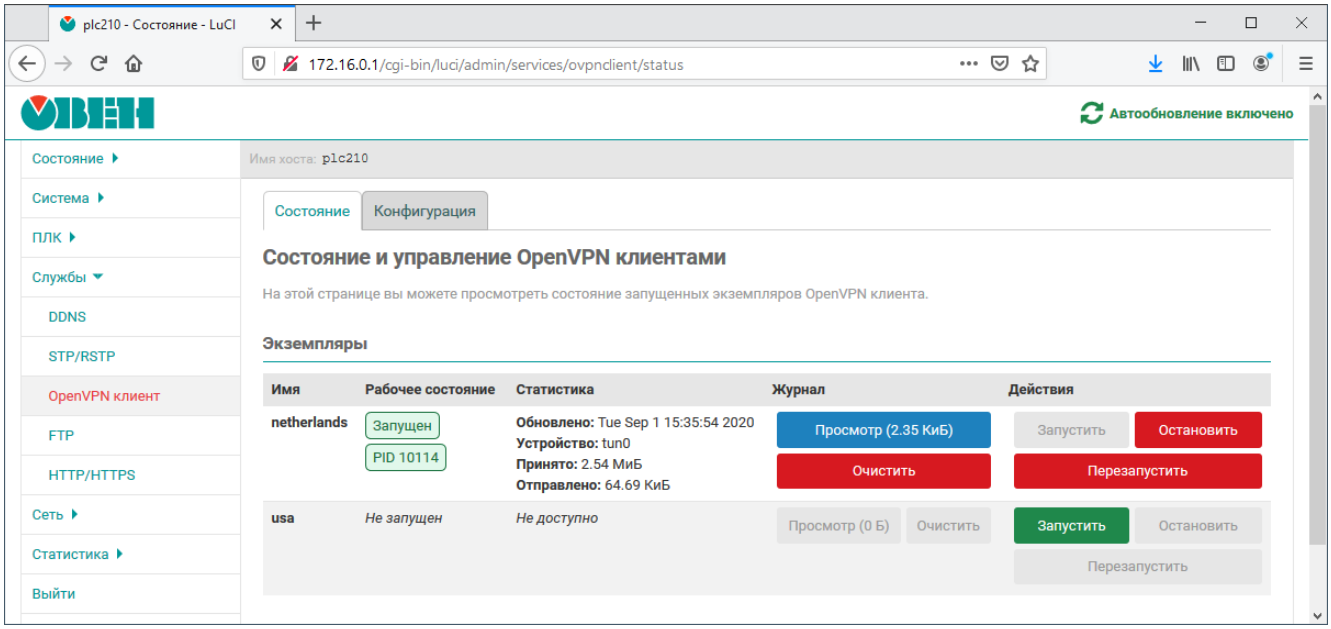


Рис. 6-30: Страница «OpenVPN клиент»

Состояние и настройка экземпляров OpenVPN клиентов разделены на соответствующие вкладки (см. рисунок 6-30):

- «Состояние» (см. раздел 6.3.1);
- «Конфигурация» (см. раздел 6.3.2).

6.3.1 Состояние

На вкладке «Состояние» страницы «OpenVPN клиент» в виде таблицы отображается текущее состояние всех включённых экземпляров OpenVPN клиента (см. рисунок 6-31). Помимо отображения состояния на данной странице можно производить ручной запуск и остановку настроенных экземпляров OpenVPN клиента.

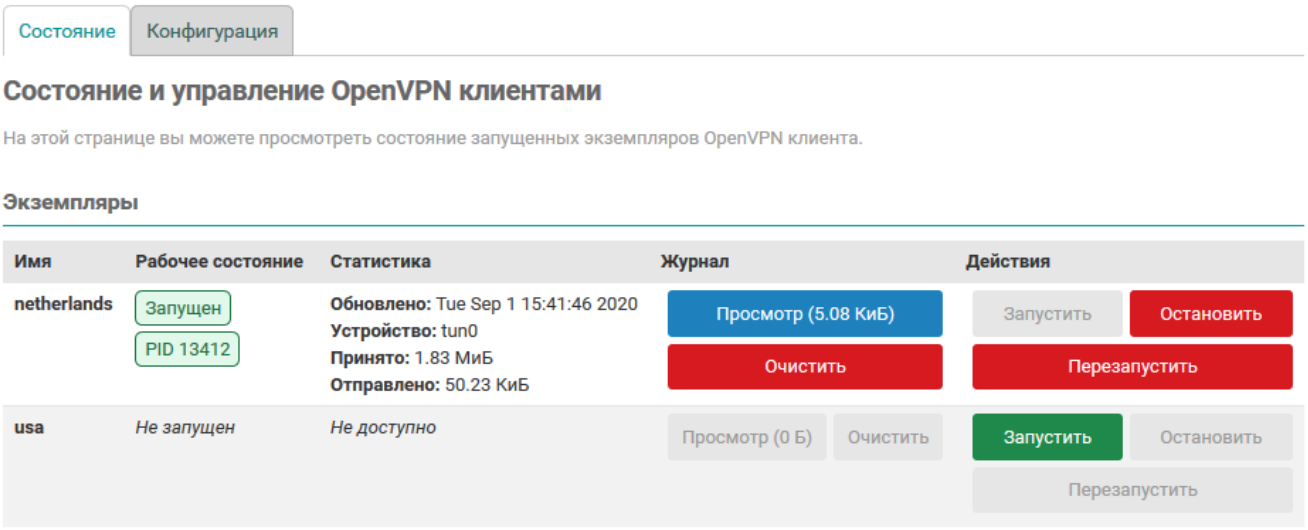


Рис. 6-31: Страница «OpenVPN клиент». Вкладка «Состояние»

Каждая строка таблицы соответствует одному экземпляру OpenVPN клиента. В столбцах таблицы отображается следующая информация:

- «Имя» — уникальное имя экземпляра OpenVPN клиента.
- «Рабочее состояние» — текущее рабочее состояние экземпляра OpenVPN клиента. Может принимать одно из двух значений:
  - «Не запущен» — экземпляр OpenVPN клиента не запущен;
  - «Запущен» — экземпляр OpenVPN клиента запущен. Идентификатор процесса (PID) данного экземпляра будет отображаться в формате «`PID <идентификатор>`», как показано на рисунке 6-32;
- «Статистика» — статистика виртуального интерфейса экземпляра OpenVPN клиента. Включает в себя следующие параметры:
  - «Обновлено» — дата и время последнего обновления данных статистики;
  - «Устройство» — имя устройства виртуального интерфейса подключения. В случае невозможности определения имени устройство отображается значение «неизвестно»;
  - «Принято» — количество принятых данных через интерфейс OpenVPN подключения;
  - «Отправлено» — количество отправленных данных через интерфейс OpenVPN подключения.

  Если данные статистики не доступны (например, экземпляр ещё не запускался), то в данном столбце отображается сообщение «Не доступно».
- «Журнал» — кнопки просмотра и очистки файла журнала экземпляра OpenVPN клиента (см. раздел 6.3.1.1);
- «Действия» — кнопки действий для экземпляра OpenVPN клиента (см. раздел 6.3.1.2).

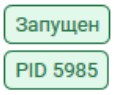


Рис. 6-32: Отображение запущенного состояния экземпляра OpenVPN клиента

6.3.1.1 Просмотр и очистка файла журнала экземпляра OpenVPN клиента

Для просмотра содержимого файла журнала экземпляра OpenVPN клиента предназначена кнопка «Просмотр», расположенная в столбце «Журнал» таблицы состояния экземпляров OpenVPN клиентов (см. рисунок 6-31).

Дополнительно, в названии кнопки в скобках отображается текущий размер файла журнала для соответствующего экземпляра OpenVPN клиента. Кнопка «Просмотр» активна только если размер файла журнала больше 0.

При нажатии кнопки «Просмотр» отображается всплывающее окно с содержимым файла журнала, как показано на рисунке 6-33.

Для очистки журнала экземпляра OpenVPN клиента предназначена кнопка «Очистка», расположенная в столбце «Журнал» таблицы состояния экземпляров OpenVPN клиентов (см. рисунок 6-31). Кнопка активна только если размер файла журнала больше 0. При нажатии кнопки «Очистка» будет выполнена очистка содержимого файла журнала для соответствующего OpenVPN клиента.

Для экземпляров OpenVPN клиента, в которых используется автоматическое назначение имени устройства, реальное имя устройства определяется путём анализа содержимого файла журнала. Для таких экземпляров OpenVPN клиента после очистки журнала невозможно определить имя устройства виртуального интерфейса подключения. В этом случае в столбце «Статистика» таблицы состояния в параметре «Устройство» будет отображаться значение «неизвестно».

6.3.1.2 Ручной запуск и остановка экземпляра OpenVPN клиента

Для выполнения ручного управления (запуск, остановка или перезапуск) экземпляром OpenVPN клиента предназначены кнопки, расположенные в столбце «Действия» таблицы состояния экземпляров OpenVPN клиентов (см. рисунок 6-31):

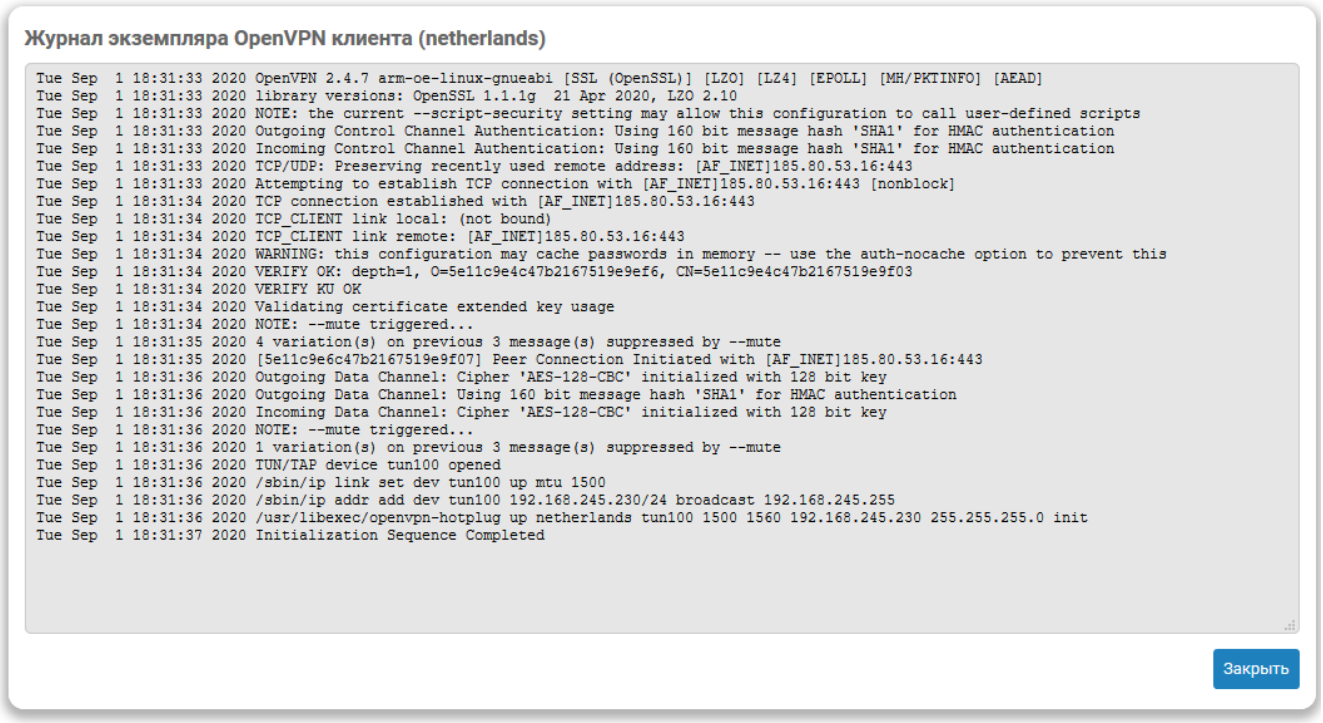


Рис. 6-33: Всплывающее окно просмотра журнала экземпляра OpenVPN клиента

- «Запустить» — выполняет запуск экземпляра OpenVPN клиента. Если экземпляр OpenVPN клиента уже запущен, то кнопка не активна;
- «Остановить» — выполняет остановку экземпляра OpenVPN клиента. Если экземпляр OpenVPN клиента не запущен, то кнопка не активна;
- «Перезапустить» — выполняет перезапуск экземпляра OpenVPN клиента. Если экземпляр OpenVPN клиента не запущен, то кнопка не активна.

6.3.2 Конфигурация

В приложении Г приведено описание процедуры настройки экземпляра OpenVPN клиента с использованием сервиса бесплатного VPN доступа freeopenvpn.org[a].

[a] https://www.freeopenvpn.org/

На вкладке «Конфигурация» страницы «OpenVPN клиент» расположены настройки службы OpenVPN и настройки экземпляров OpenVPN клиентов. Внешний вид вкладки «Конфигурация» показан на рисунке 6-34.

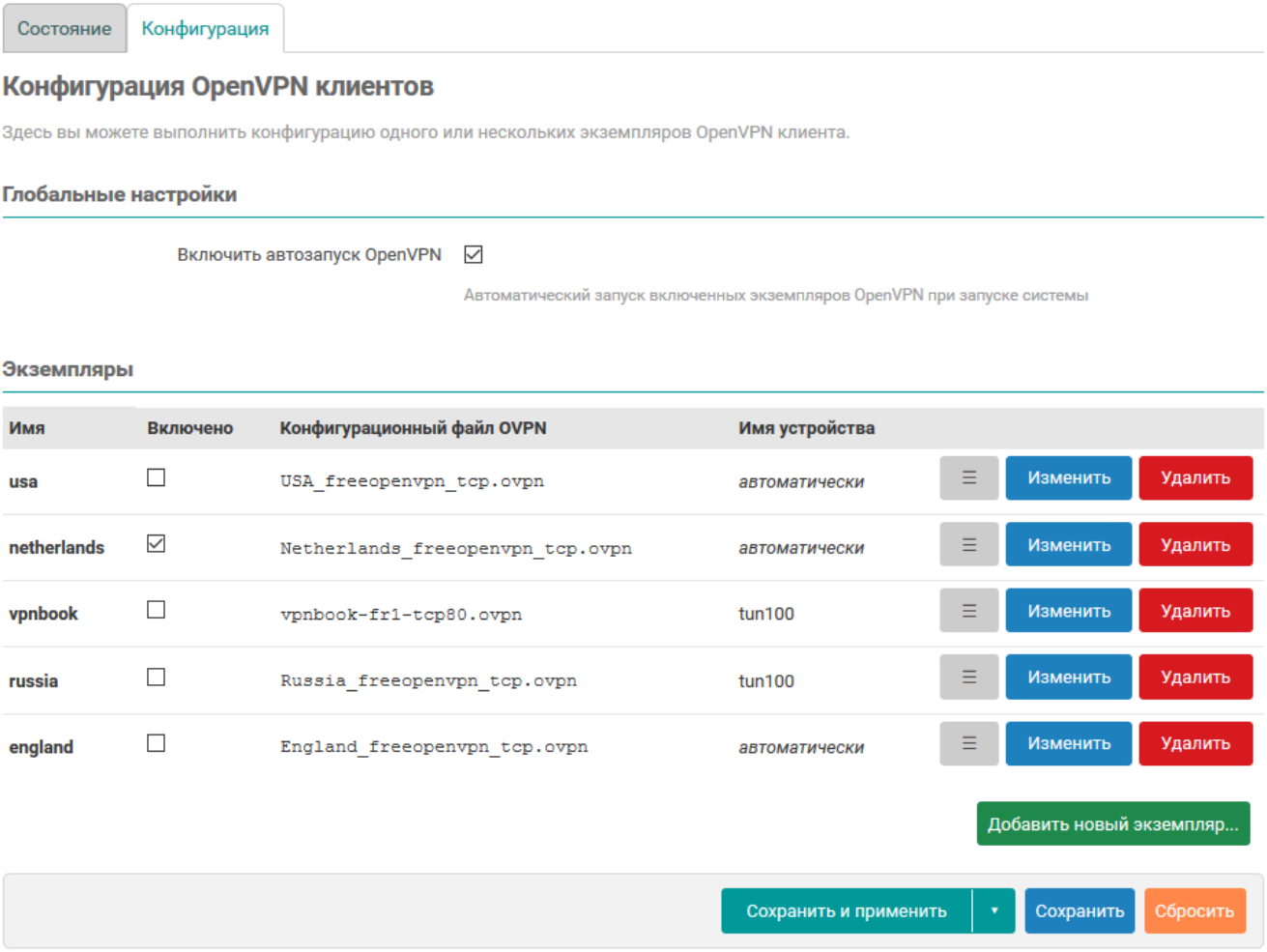


Рис. 6-34: Страница «OpenVPN клиент». Вкладка «Конфигурация»

Страница конфигурации разделена на подраздел глобальных настроек и подраздел конфигурации экземпляров OpenVPN клиентов.

В подразделе глобальных настроек расположена только одна настройка — «Включить автозапуск OpenVPN». Данная настройка позволяет включить автоматический запуск службы OpenVPN при запуске системы. Если автоматический запуск включён, то все настроенные и включённые экземпляры OpenVPN клиента (для которых включена настройка «Включено») также будут автоматически запускаться при запуске системы.

Настройки экземпляров OpenVPN клиентов отображаются в виде таблицы в подразделе «Экземпляры» (см. рисунок 6-35).

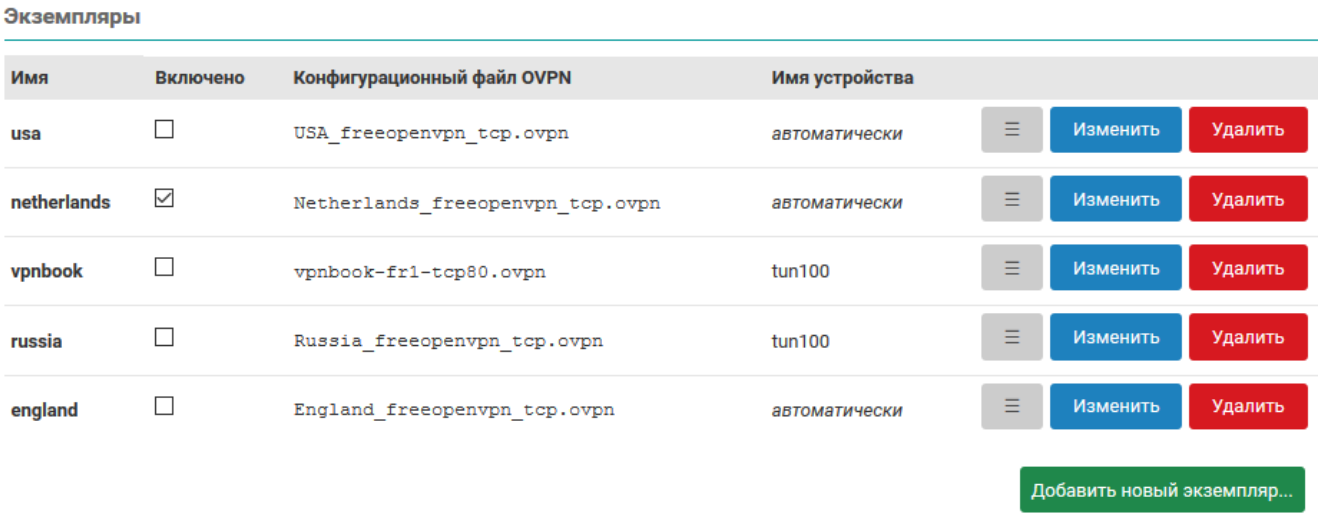


Рис. 6-35: Страница «OpenVPN клиент». Таблица настроек экземпляров OpenVPN клиентов

Таблица имеет следующие основные столбцы:

- «Имя» — уникальное имя экземпляра OpenVPN клиента;
- «Включено» — включён или выключен соответствующий экземпляр OpenVPN клиента;
- «Конфигурационный файл OVPN» — имя конфигурационного файла экземпляра OpenVPN клиента в формате OVPN (см. подробное описание параметра в разделе 6.3.2.1);
- «Имя устройства» — имя устройства (см. подробное описание параметра в разделе 6.3.2.1).

В последнем столбце таблицы расположены кнопки управления записями конфигурации экземпляров OpenVPN клиентов:

- «≡» — кнопка изменения порядка записей в таблице. Удерживая нажатой данную кнопку можно перемещать строку таблицы, изменяя тем самым её порядок. Применяется исключительно для визуальной группировки конфигураций. Функционального значения порядок записей конфигураций в таблице не имеет;
- «Изменить» — кнопка редактирования конфигурации соответствующего экземпляра OpenVPN клиента (см. раздел 6.3.2.1);
- «Удалить» — кнопка удаления конфигурации соответствующего экземпляра OpenVPN клиента (см. раздел 6.3.2.3).

Под таблицей настроек экземпляров OpenVPN клиентов расположена кнопка «Добавить новый экземпляр...», предназначенная для добавления конфигурации нового экземпляра OpenVPN клиента (см. раздел 6.3.2.2).

6.3.2.1 Редактирование экземпляра OpenVPN клиента

Для редактирования настроек экземпляра OpenVPN клиента необходимо нажать кнопку «Изменить» (см. рисунок 6-35), расположенную в строке соответствующего экземпляра. При этом будет открыто всплывающее окно настроек экземпляра OpenVPN клиента, как показано на рисунке 6-36.

Для конфигурации доступны следующие параметры экземпляра OpenVPN клиента:

- «Включено» — включён или выключен экземпляр OpenVPN клиента;
- «Конфигурационный файл OVPN» — выбор и загрузка конфигурационного файла экземпляра OpenVPN клиента в формате OVPN [12] (см. раздел 6.3.2.1.1);
- «Имя устройства» — имя устройства для данного экземпляра OpenVPN клиента. Должно быть указано в форме `tunX` или `tapX`, где `X` — номер устройства. Если имя устройства указано, то при подключении будет использовано указанное устройство. Если устройство не указано, то при подключении устройство будет создано автоматически в соответствии с опциями конфигурационного файла.
- «Аутентификация по имени пользователя и паролю» — включение функции дополнительной аутентификации по имени пользователя и паролю. Многие провайдеры OpenVPN требуют отдельной дополнительной аутентификации по имени пользователя и паролю;

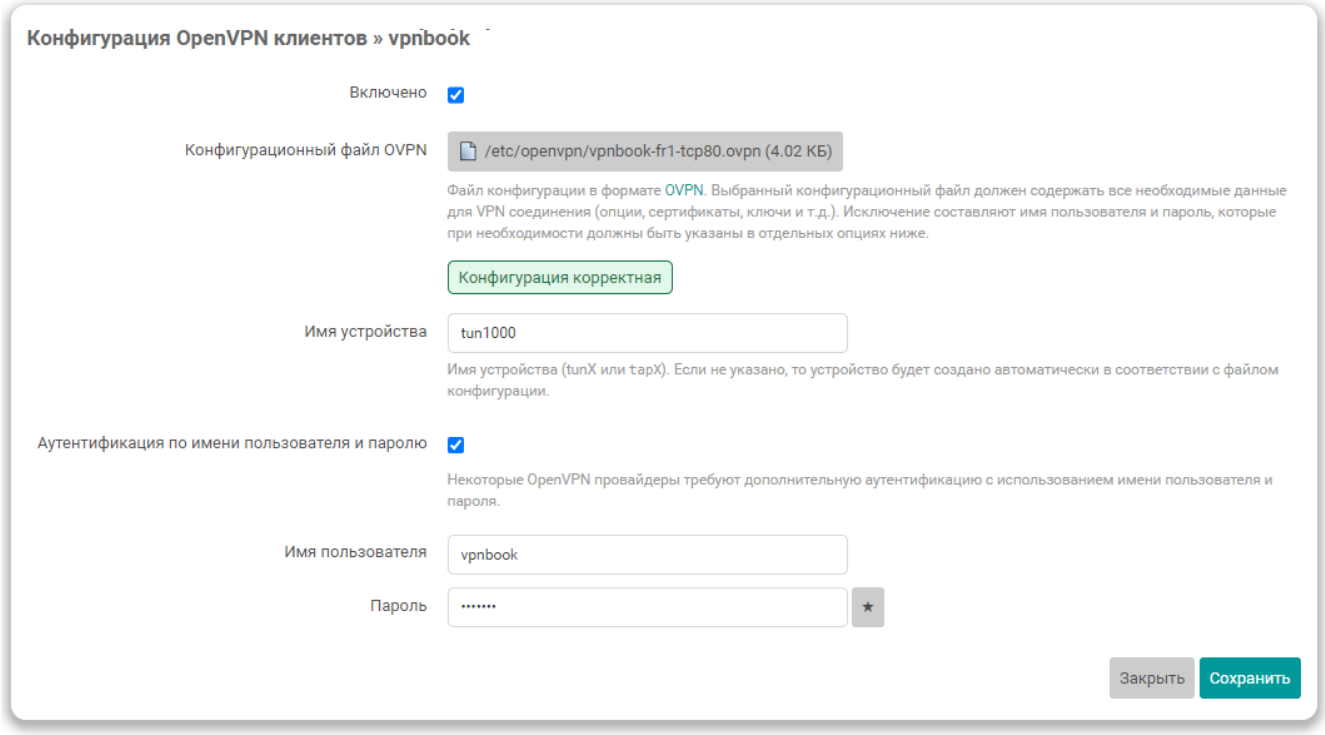


Рис. 6-36: Всплывающее окно редактирования настроек экземпляра OpenVPN клиента

- «Имя пользователя» — имя пользователя для аутентификации по имени пользователя и паролю. Настройка активна только если включена опция «Аутентификация по имени пользователя и паролю»;
- «Пароль» — пароль для аутентификации по имени пользователя и паролю. Настройка активна только если включена опция «Аутентификация по имени пользователя и паролю».

6.3.2.1.1 Выбор и загрузка конфигурационных файлов в OVPN формате

Для выбора и загрузки конфигурационных файлов в формате OVPN [12] предназначена опция «Конфигурационный файл OVPN», отображаемая во всплывающем окне редактирования настроек экземпляра OpenVPN клиента (см. рисунок 6-36).

После создания нового экземпляра OpenVPN клиента конфигурационный файл не выбран и внешний вид опции выглядит, как показано на рисунке 6-37.

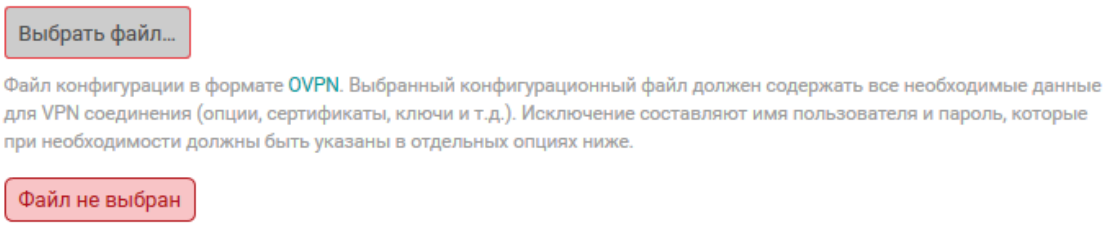


Рис. 6-37: Выбор и загрузка конфигурационного файла в формате OVPN. Файл не выбран

Для выбора (или загрузки нового) файла необходимо нажать кнопку «Выбрать файл...». Нажатие данной кнопки переводит опцию в режим выбора (или загрузки) файла. В режиме выбора файла отображается список уже загруженных файлов, как показано на рисунке 6-38.

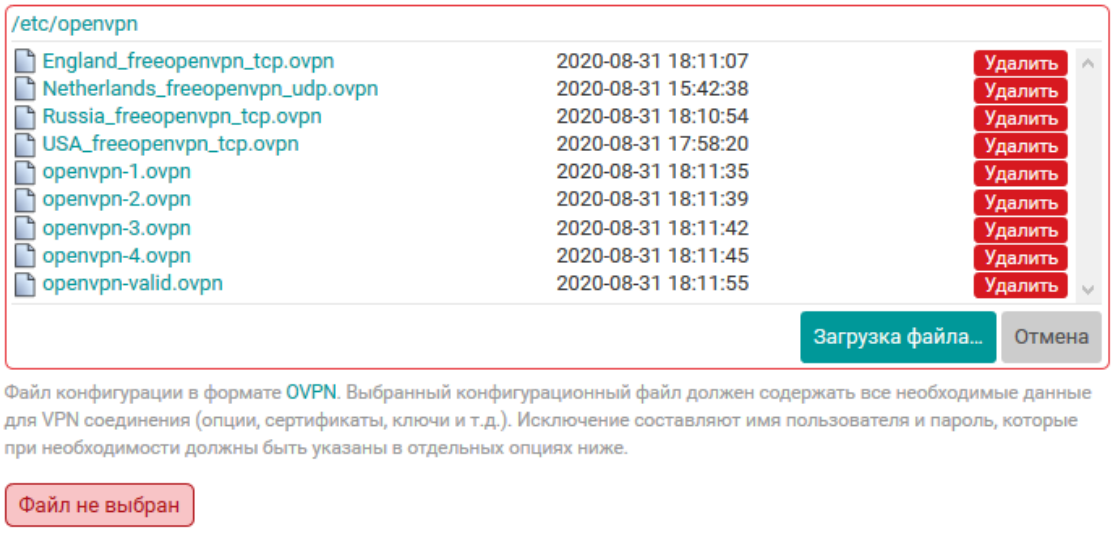


Рис. 6-38: Выбор и загрузка конфигурационного файла в формате OVPN. Список загруженных файлов

Если загруженные файлы отсутствуют, то отображаемый список также будет пуст и внешний вид опции будет выглядеть, как показано на рисунке 6-39.

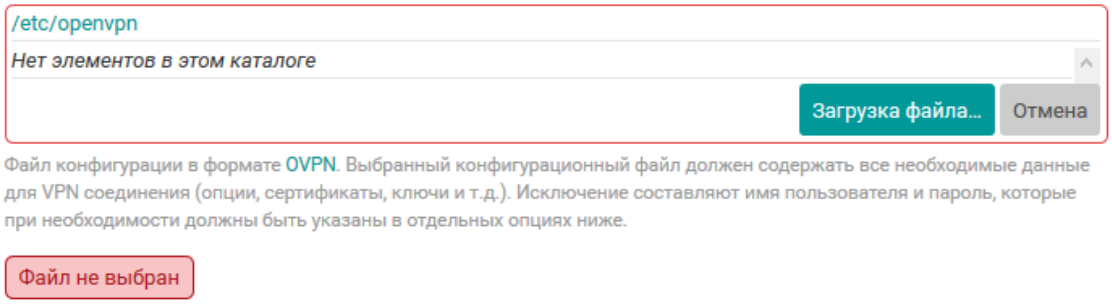


Рис. 6-39: Выбор и загрузка конфигурационного файла в формате OVPN. Отсутствие загруженных файлов

Для загрузки нового файла на устройство необходимо нажать кнопку «Загрузка файла...». В этом случае будет открыто стандартное диалоговое окно выбора файла (см. рисунок 6-40), в котором необходимо выбрать требуемый файл на локальной файловой системе компьютера и нажать кнопку «Открыть» (расположение и название кнопки может отличаться в зависимости от используемого браузера и/или операционной системы).

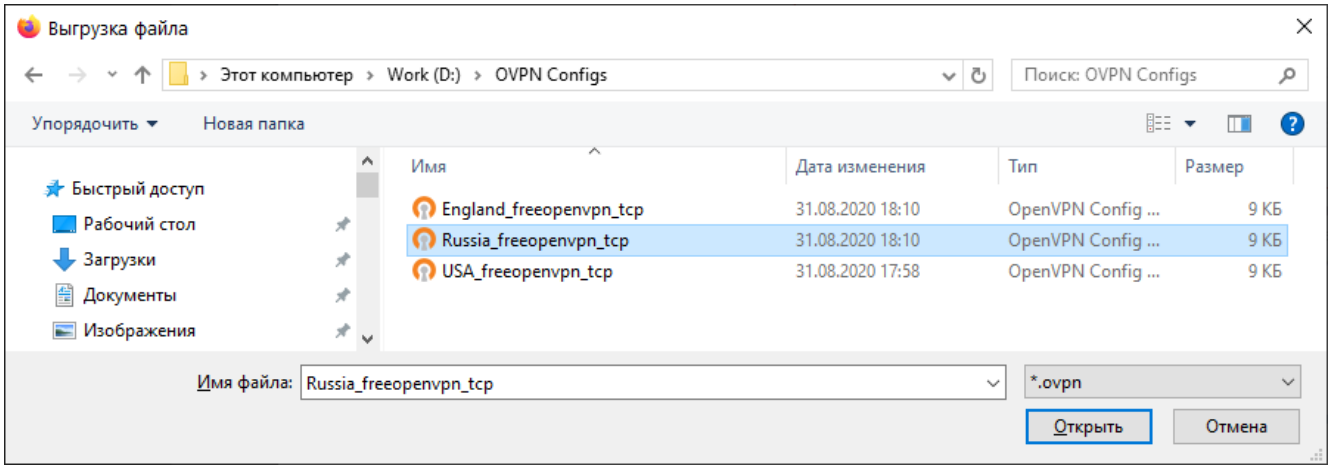


Рис. 6-40: Стандартное диалоговое окно выбора файла для загрузки

Когда требуемый файл будет выбран, внешний вид опции будет выглядеть, как показано на рисунке 6-41 — имя загружаемого файла будет отображаться в поле между кнопками «Обзор...» и «Загрузка файла».

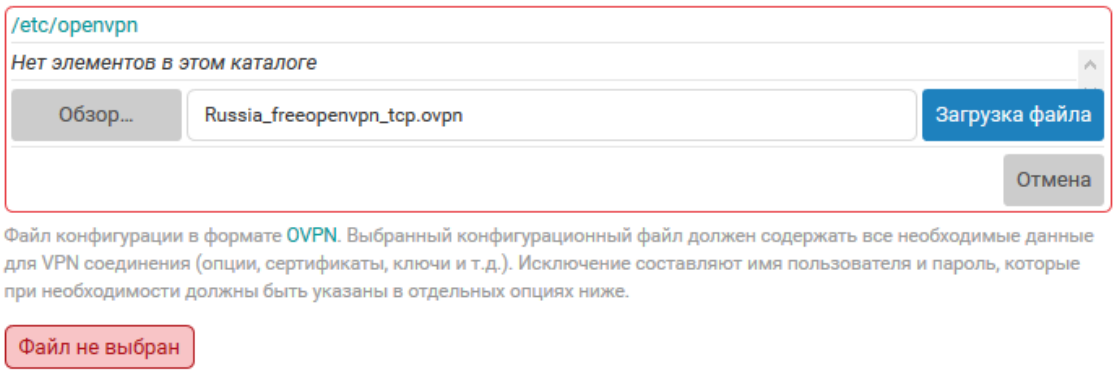


Рис. 6-41: Выбор и загрузка конфигурационного файла в формате OVPN. Выбор файла для загрузки

Если требуется выбрать другой файл для загрузки (например, файл был выбран ошибочно), необходимо нажать кнопку «Обзор...» и повторить выбор файла на локальной файловой системе компьютера.

Нажатие кнопки «Загрузка файла» приведёт к выполнению загрузки выбранного файла на устройство. По окончанию загрузки файла на устройство новый файл будет доступен в списке загруженных файлов для выбора (см. рисунок 6-42).

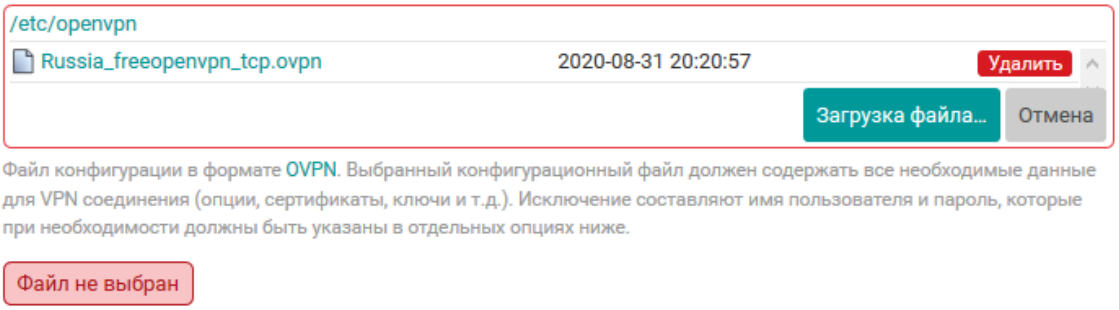


Рис. 6-42: Выбор и загрузка конфигурационного файла в формате OVPN. Файл загружен на устройство

Выбор требуемого файла производится путём однократного нажатия имени файла в списке. При выборе файла опция переходит из режима выбора файлов обратно в обычный режим. В обычном режиме, если файл выбран, название кнопки «Выбрать файл...» (см. рисунок 6-37) будет заменено на имя (путь) текущего выбранного файла (см. рисунок 6-43).

После выбора конфигурационного файла автоматически будет произведена его проверка (валидация). Результат проверки будет отображён под кнопкой выбора файла, как показано на рисунке 6-43.

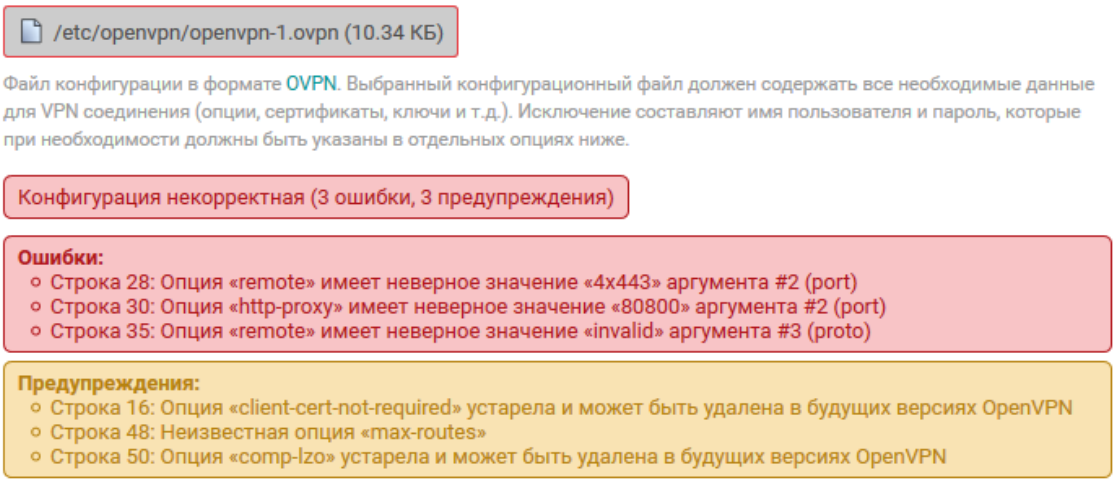


Рис. 6-43: Валидация OVPN конфигурационного файла. Некорректная конфигурация

В случае обнаружения некорректной конфигурации будут выведены сообщения (ошибки и предупреждения) валидатора.

Корректный конфигурационный файл должен удовлетворять следующим требованиям:

- файл должен являться конфигурацией OpenVPN клиента (конфигурационные файлы для OpenVPN сервера не поддерживаются);
- файл должен являться синтаксически корректным конфигурационным файлом в формате OVPN [12] и не должен содержать неизвестных опций;
- конфигурационные опции, предполагающие указание тех или иных файлов в своих аргументах, не должны ссылаться на эти файлы в форме пути к файлу. Подобные опции (ca, cert, key, tls-auth и т.п.) должны быть указаны во встраиваемой (inline) форме с включением содержимого требуемых файлов непосредственно в конфигурационном файле.

Сохранить конфигурацию экземпляра OpenVPN клиента с выбранным некорректным конфигурационным файлом нельзя. Необходимо выбрать корректный конфигурационный файл.

6.3.2.2 Добавление нового экземпляра OpenVPN клиента

Для добавления новой конфигурации экземпляра OpenVPN клиента необходимо нажать кнопку «Добавить новый экземпляр...», расположенную под таблицей экземпляров (см. рисунок 6-35).

При нажатии кнопки будет отображено всплывающее окно с предложением ввода имени нового экземпляра OpenVPN клиента, как показано на рисунке 6-44.

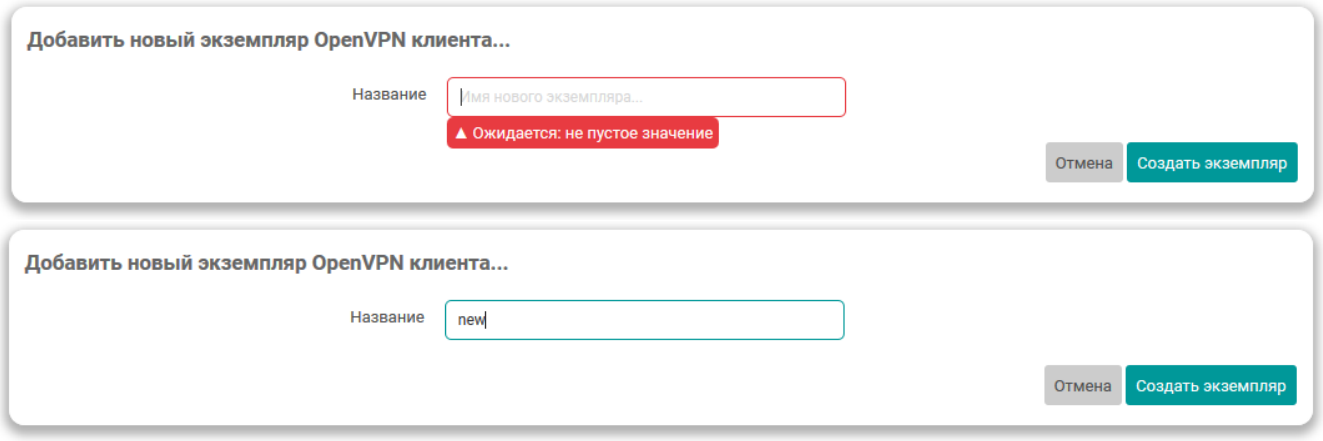


Рис. 6-44: Всплывающее окно ввода имени нового экземпляра OpenVPN клиента

Имя нового экземпляра OpenVPN клиента должно удовлетворять следующим условиям:

- не должно совпадать с именем уже существующих экземпляров OpenVPN клиентов;
- длина имени не должна превышать 24 символа;
- должно состоять из символов латинского алфавита («a–z», «A–Z»), арабских цифр («0–9») и символа нижнего подчёркивания («_»). Любые другие символы запрещены.

Имя экземпляра OpenVPN клиента после его создания изменить нельзя.

После ввода правильного имени нового экземпляра OpenVPN клиента и нажатия кнопки «Создать экземпляр» (см. рисунок 6-44) будет открыто всплывающее окно настроек нового экземпляра OpenVPN клиента, также как и при изменении (редактировании) настроек уже существующего экземпляра OpenVPN клиента (см. раздел 6.3.2.1).

6.3.2.3 Удаление экземпляра OpenVPN клиента

Для удаления экземпляра OpenVPN клиента предназначена кнопка «Удалить» (см. рисунок 6-35), расположенная в строке соответствующего экземпляра.

6.4 HTTP/HTTPS

На странице «HTTP/HTTPS» раздела «Службы» расположены настройки лёгкого однопоточного Web-сервера «uHTTPd» (см. рисунок 6-45).

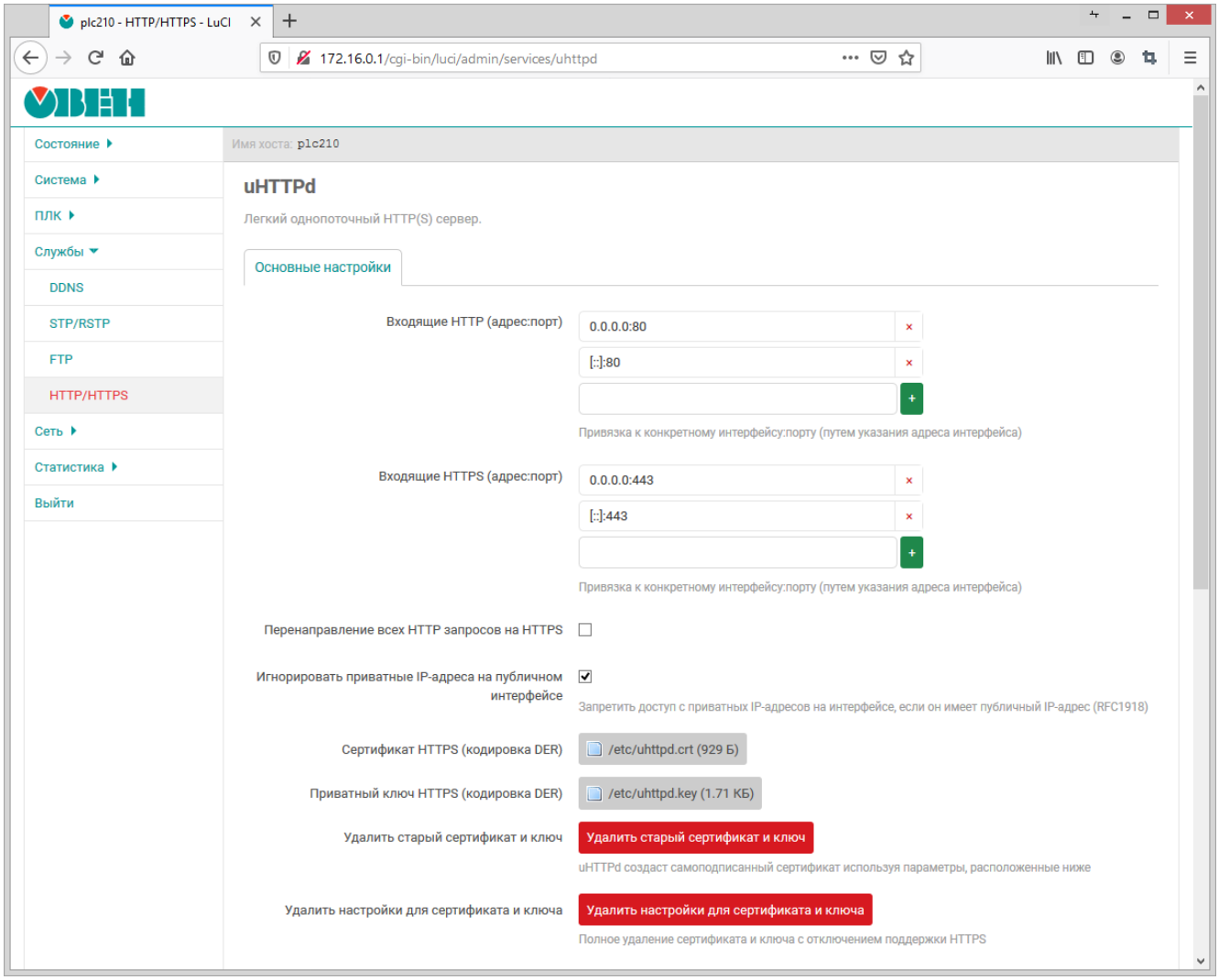


Рис. 6-45: Страница «HTTP/HTTPS»

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 [13]);
- «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 6.4.1);

- «Удалить настройки для сертификата и ключа» — нажатие этой кнопки удаляет существующий сертификат и приватный ключ, а также отключает поддержку протокола HTTPS.

6.4.1 Параметры самоподписанного сертификата

В подразделе «Параметры самоподписанного сертификата» страницы «HTTP/HTTPS» представлены настройки, используемые для генерации самоподписанного сертификата службы HTTP/HTTPS-сервера (см. рисунок 6-46).

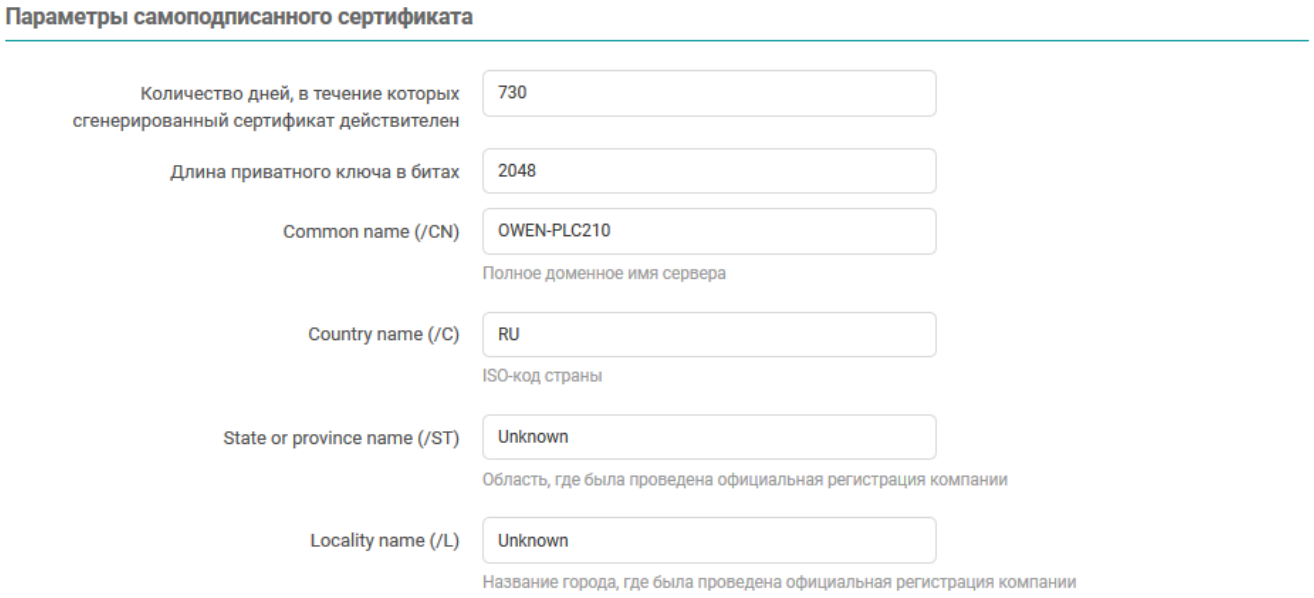


Рис. 6-46: Страница «HTTP/HTTPS». Параметры самоподписанного сертификата

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.

6.5 FTP

На странице «FTP» раздела «Службы» расположены настройки FTP-сервера. Внешний вид страницы «FTP» показан на рисунке 6-47.

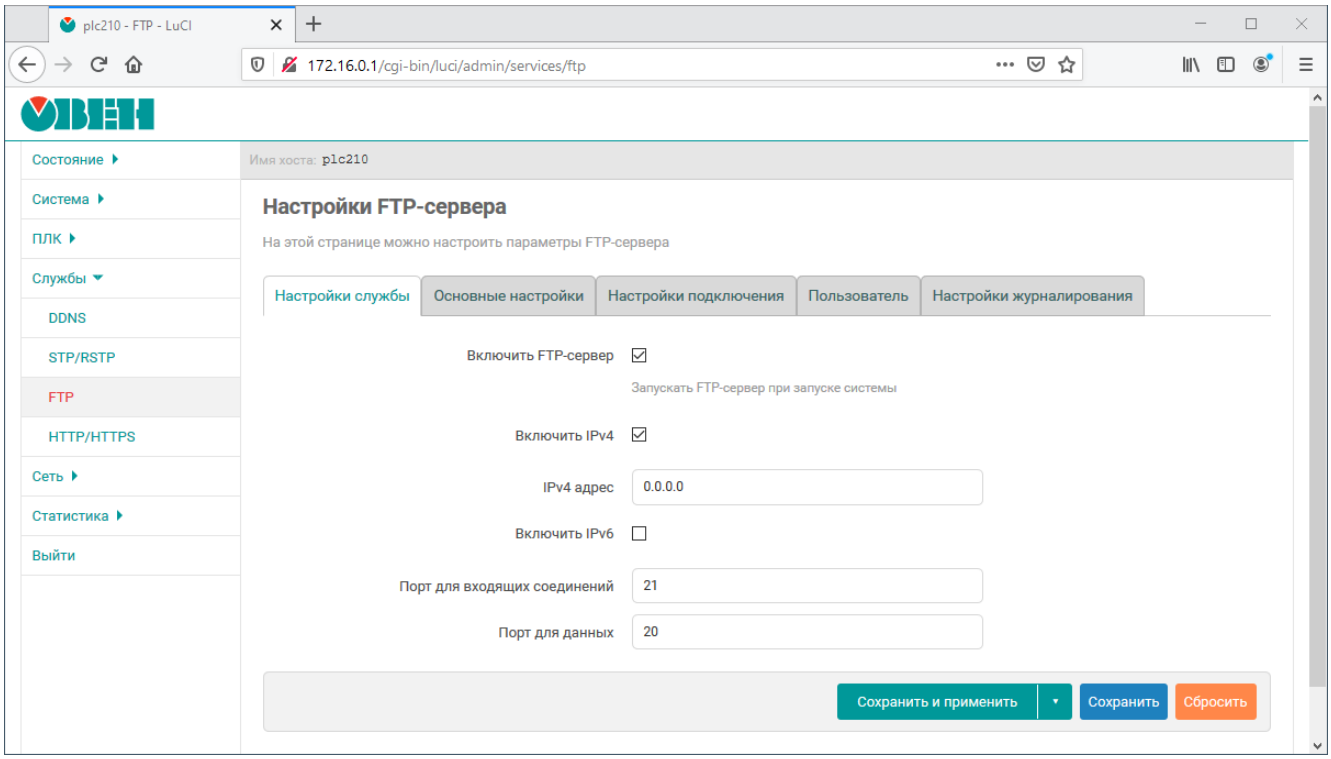


Рис. 6-47: Страница «FTP»

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

Настройки FTP-сервера разделены на пять вкладок:

- «Настройки службы» (см. раздел 6.5.1);
- «Основные настройки» (см. раздел 6.5.2);
- «Настройки подключения» (см. раздел 6.5.3);
- «Пользователь» (см. раздел 6.5.4);
- «Настройки журналирования» (см. раздел 6.5.5).

6.5.1 Настройки службы

Настройки службы FTP-сервера расположены во вкладке «Настройки службы» (см. рисунок 6-48) 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;

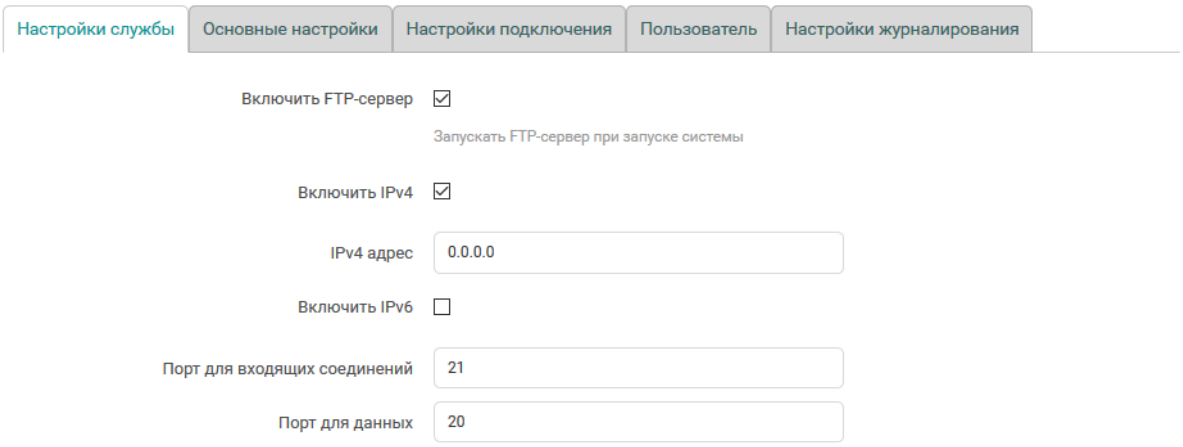


Рис. 6-48: Страница «FTP». Настройки службы

- «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).

6.5.2 Основные настройки

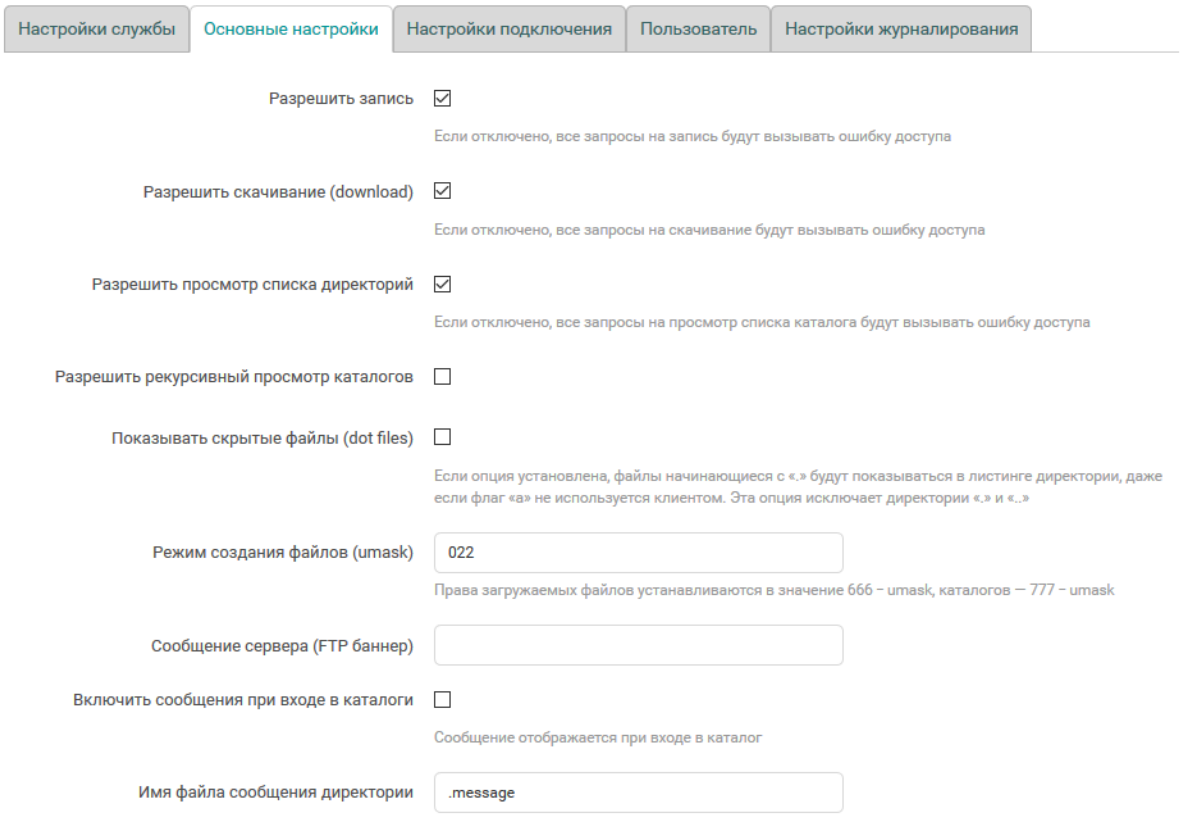


Рис. 6-49: Страница «FTP». Основные настройки

Основные настройки FTP-сервера расположены во вкладке «Основные настройки» (см. рисунок 6-49) 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».

6.5.3 Настройки подключения

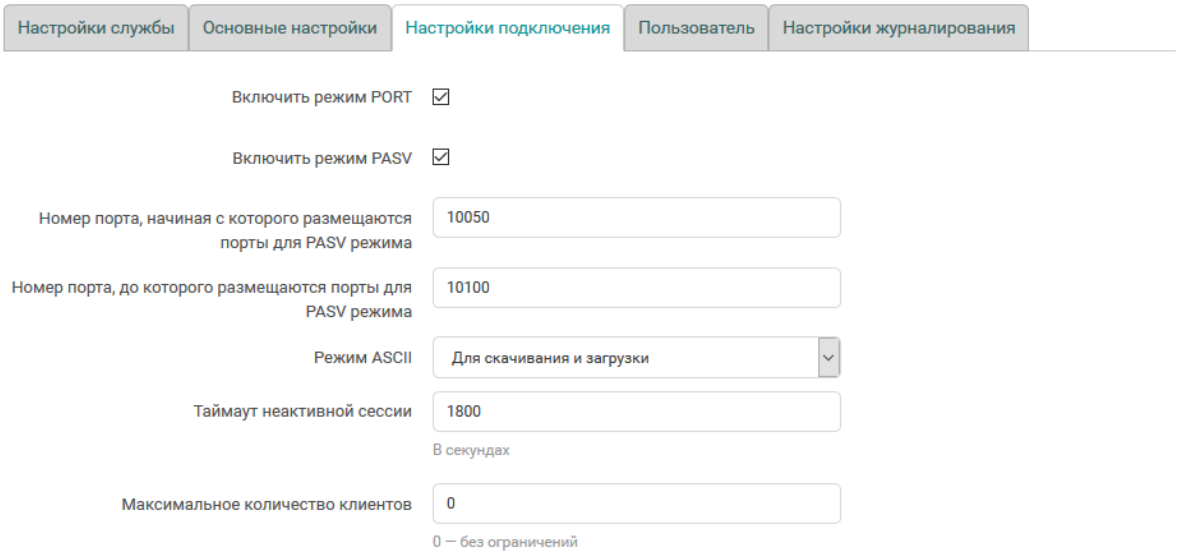


Рис. 6-50: Страница «FTP». Настройки подключения

Настройки подключения FTP-сервера расположены во вкладке «Настройки подключения» (см. рисунок 6-50) 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.

6.5.4 Настройки пользователя

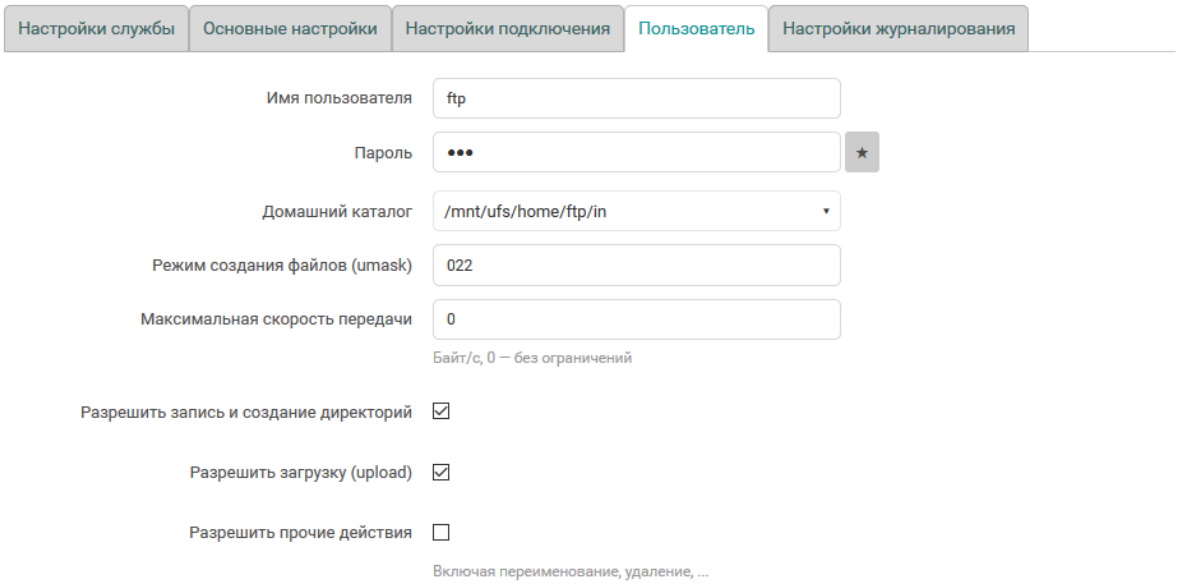


Рис. 6-51: Страница «FTP». Настройки пользователя

Настройки пользователя расположены во вкладке «Пользователь» (см. рисунок 6-51) 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.

6.5.5 Настройки журналирования

Настройки журналирования FTP-сервера расположены во вкладке «Настройки журналирования» (см. рисунок 6-52) 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»;

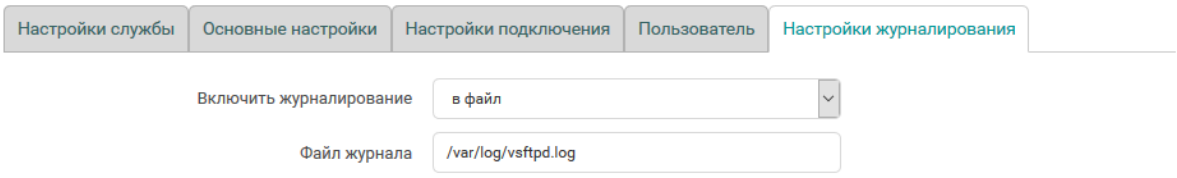


Рис. 6-52: Страница «FTP». Настройки журналирования

- «в syslog» — журналирование выполняется в системный журнал (syslog).

Страница просмотра содержимого системного журнала описана в разделе 3.5.2 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.

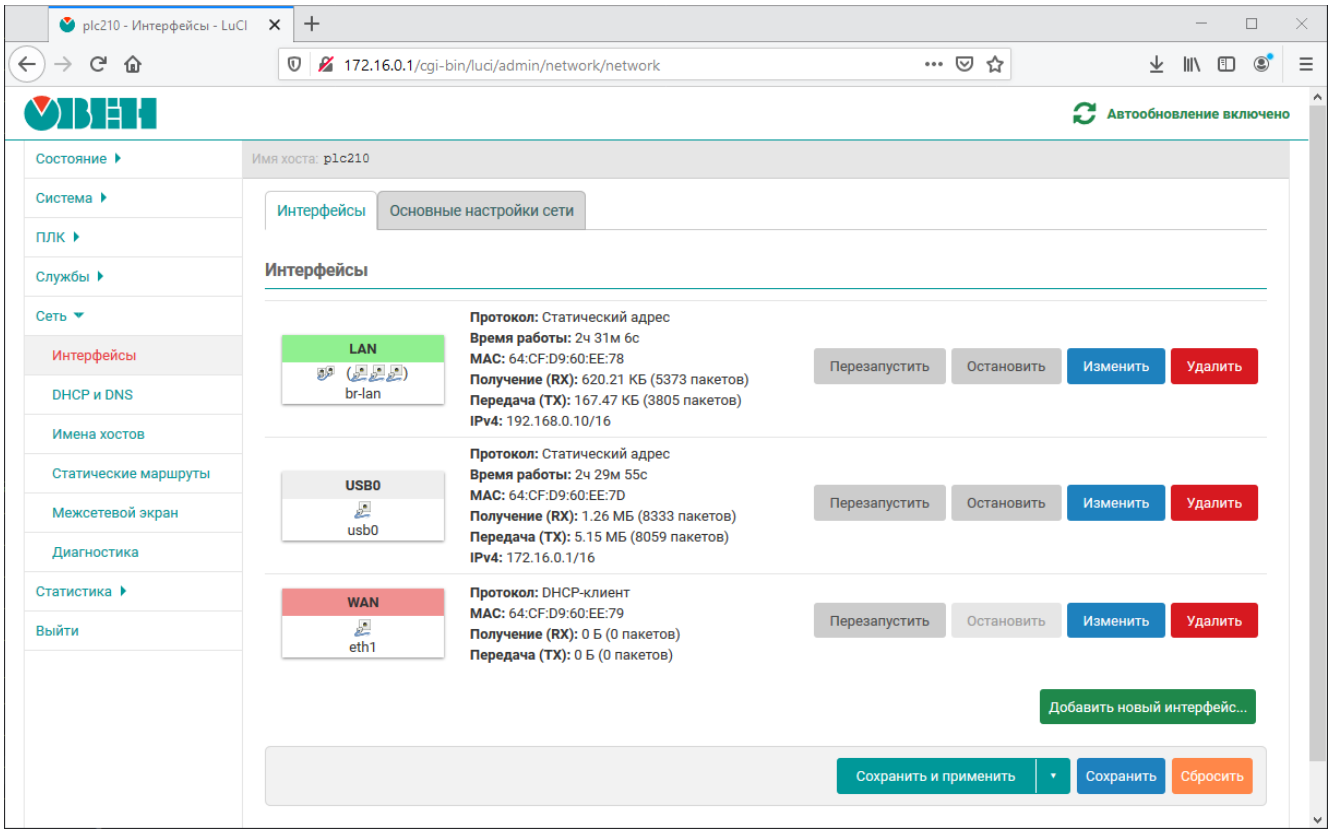


Рис. 7-1: Страница «Интерфейсы». Вкладка «Интерфейсы»

В самом верху страницы расположены две вкладки «Интерфейсы» и «Основные настройки сети». На вкладке «Основные настройки сети» расположена настройка ULA префикса IPv6 (см. рисунок 7-2).

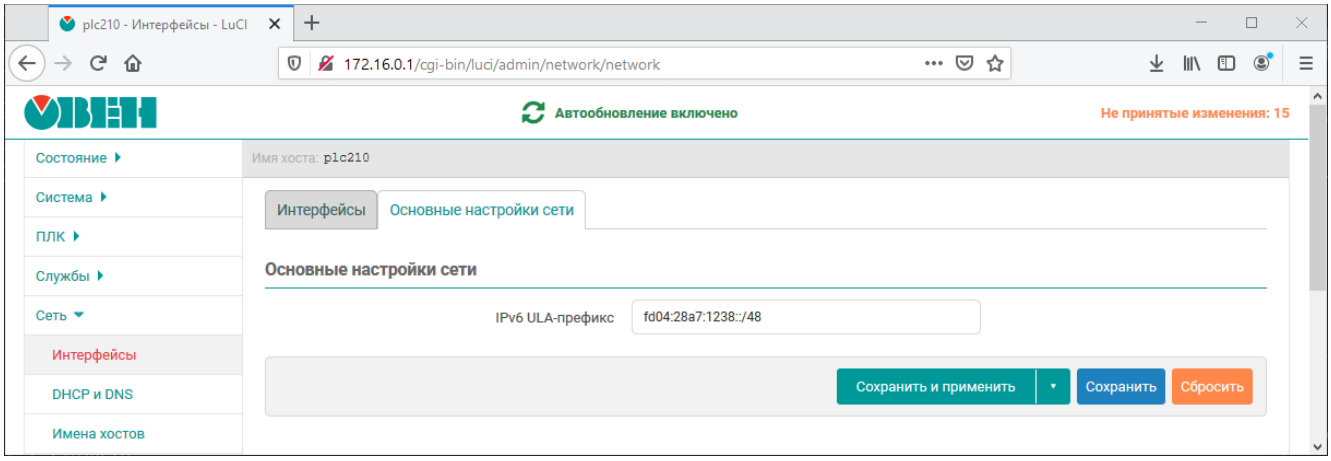
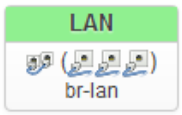


Рис. 7-2: Страница «Интерфейсы». Вкладка «Основные настройки сети»

На вкладке «Интерфейсы» расположена таблица «Интерфейсы», в которой перечислены имеющиеся (сконфигурированные) 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).

На рисунке 7-3 приведены примеры значков сетевых интерфейсов.



(а) Значок интерфейса-моста «LAN»

(б) Значок интерфейса «WAN»

Рис. 7-3: Значки сетевых интерфейсов

На рисунке 7-3(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 7-3(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, обновляемая 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 всплывающее окно редактирования параметров интерфейса (см. раздел 7.1.1).
- «Удалить» — удаляет соответствующий интерфейс.

7.1.1 Редактирование интерфейсов

Внешний вид всплывающего окна редактирования сетевого интерфейса показан на рисунке 7-4.

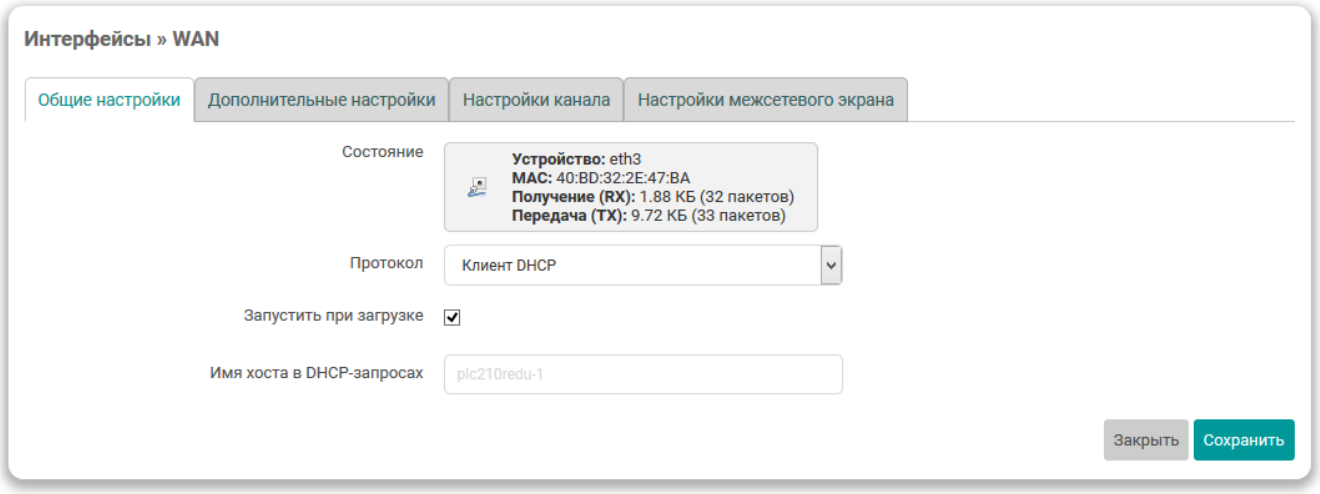


Рис. 7-4: Окно редактирования параметров сетевого интерфейса

Окно редактирования сетевого интерфейса разделено 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.

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.

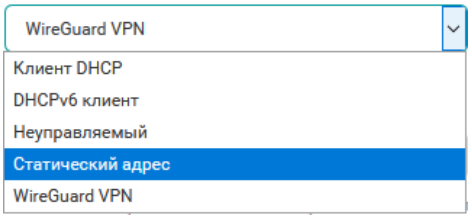


Рис. 7-5: Выпадающий список выбора протокола интерфейса

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

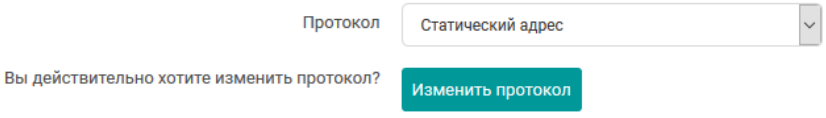


Рис. 7-6: Кнопка смены протокола сетевого интерфейса

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 «Общие настройки»:

- «Запустить при загрузке» — включает или отключает автоматический запуск интерфейса при загрузке системы.

На вкладке «Дополнительные настройки» содержатся следующие общие для всех протоколов настройки:

- «Использовать встроенный IPv6-менеджмент» — включает или отключает использование встроенного IPv6 менеджмента для данного интерфейса;
- «Принудительное подключение (Force link)» — устанавливать параметры интерфейсу независимо от состояния подключения. Если опция включена, изменение состояния подключения (например, подключение или отключение кабеля) не будет вызывать hotplug обработчики.

  Данная опция по умолчанию включена для протокола «Статический адрес» (см. раздел 7.1.2.2) и выключена для всех остальных протоколов.

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

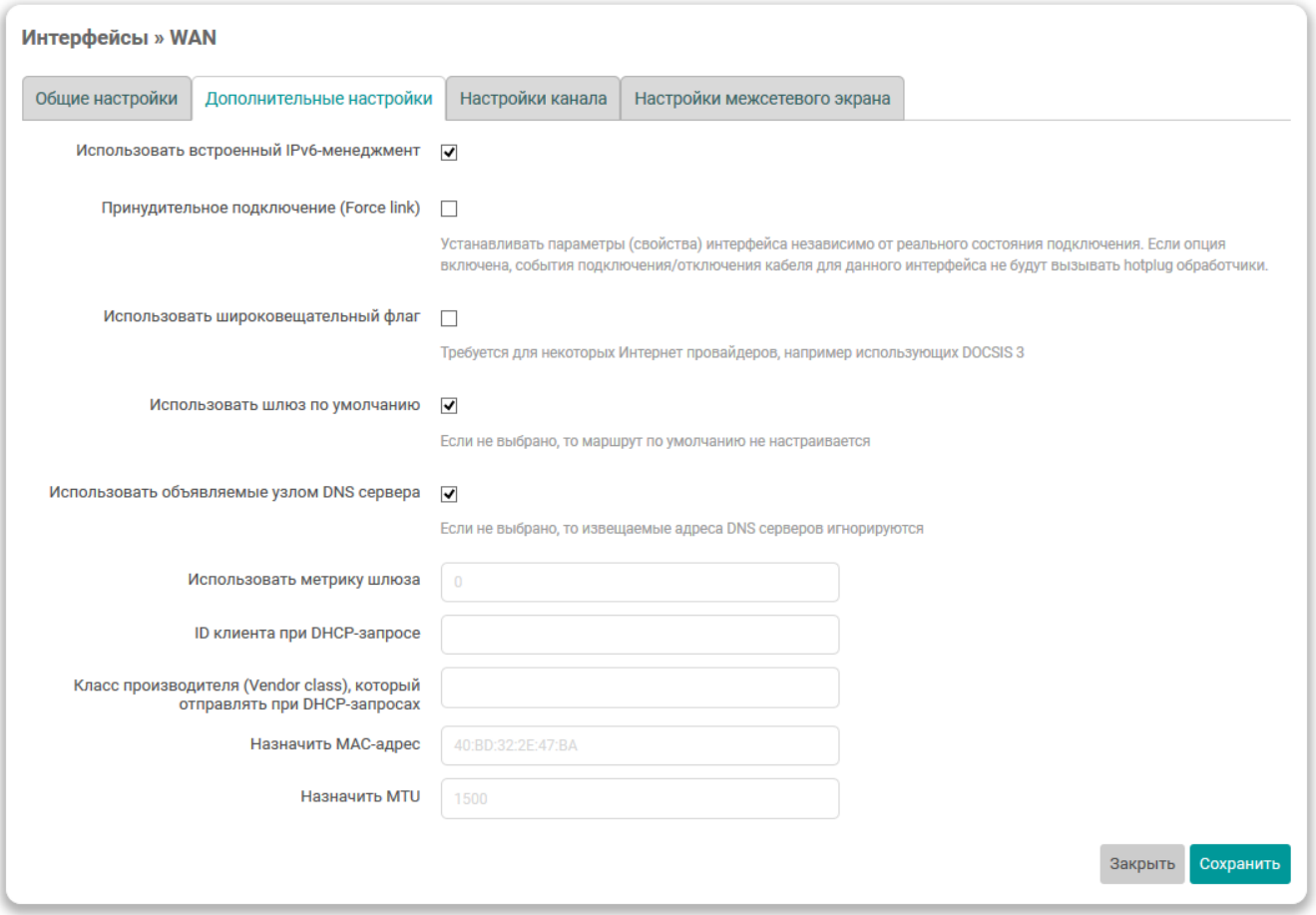


Рис. 7-7: Дополнительные настройки сетевого интерфейса для протокола «DHCP-клиент»

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».

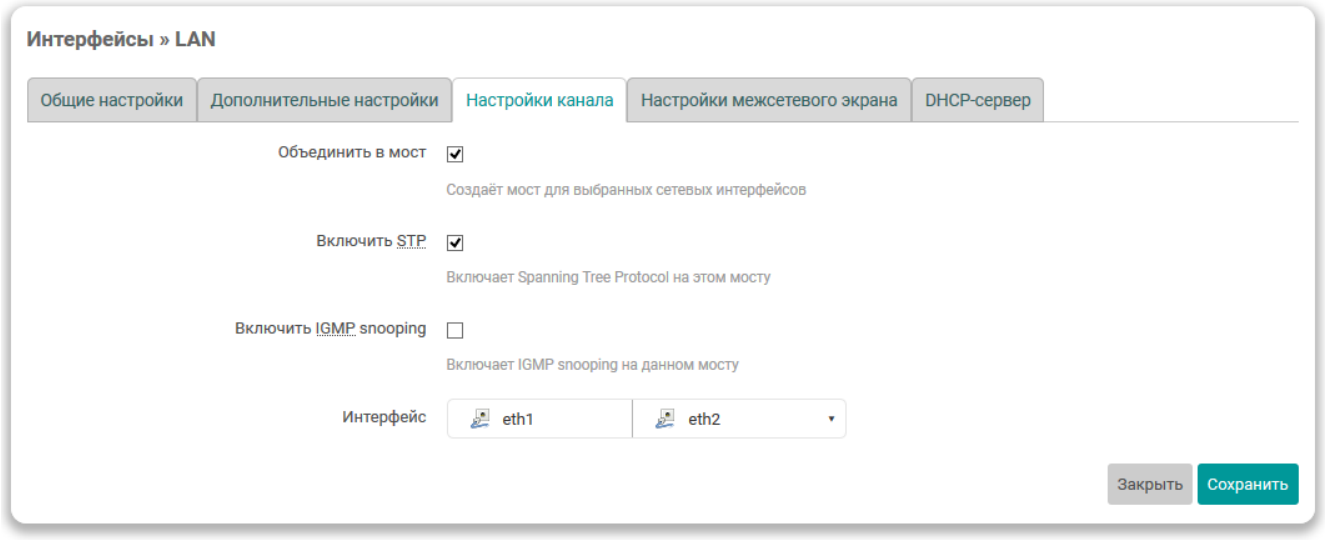


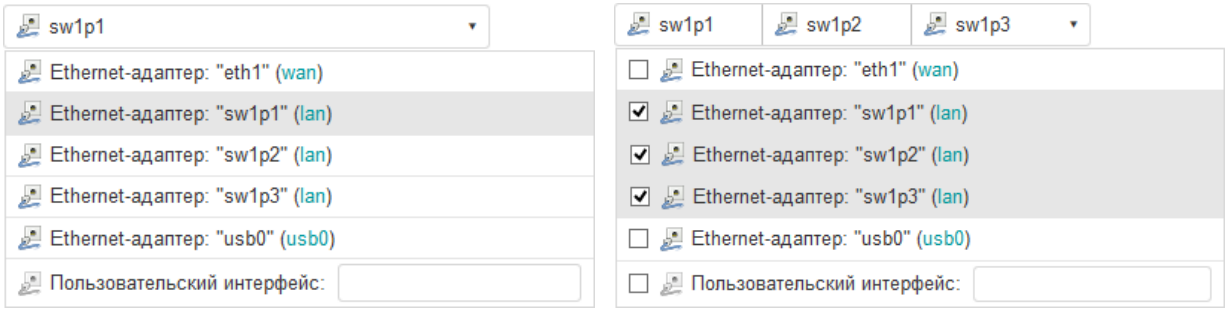
Рис. 7-8: Настройки канала сетевого интерфейса

На данной вкладке представлены следующие настройки сетевого интерфейса:

- «Объединить в мост» — настройка позволяет выполнить объединение нескольких системных сетевых интерфейсов в сетевой мост [14]. В этом случае становятся доступны дополнительные настройки:
  - «Включить STP» — включает или отключает протокол STP [15] 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 [16] 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.

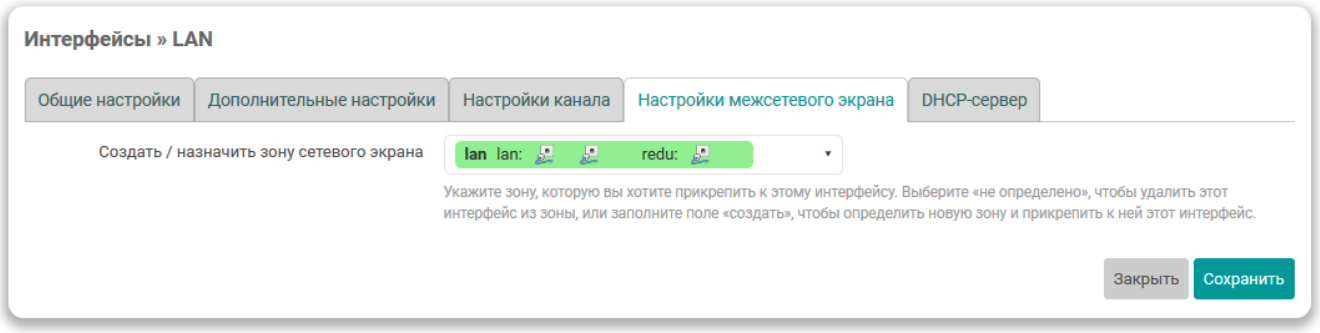


Рис. 7-10: Настройки межсетевого экрана сетевого интерфейса

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

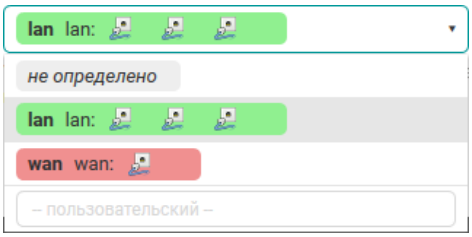


Рис. 7-11: Выпадающий список выбора зоны межсетевого экрана

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 дополнительные 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 доступны во вкладке «DHCP-сервер» окна редактирования настроек сетевого интерфейса (см. рисунок 7-12).

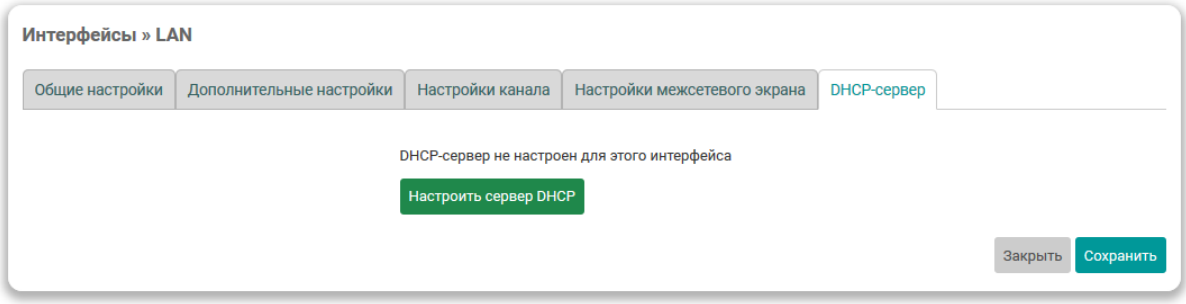


Рис. 7-12: Вкладка настроек DHCP-сервера

Для включения DHCP-сервера на интерфейсе (если он еще не включен), необходимо нажать кнопку «Настроить сервер DHCP».

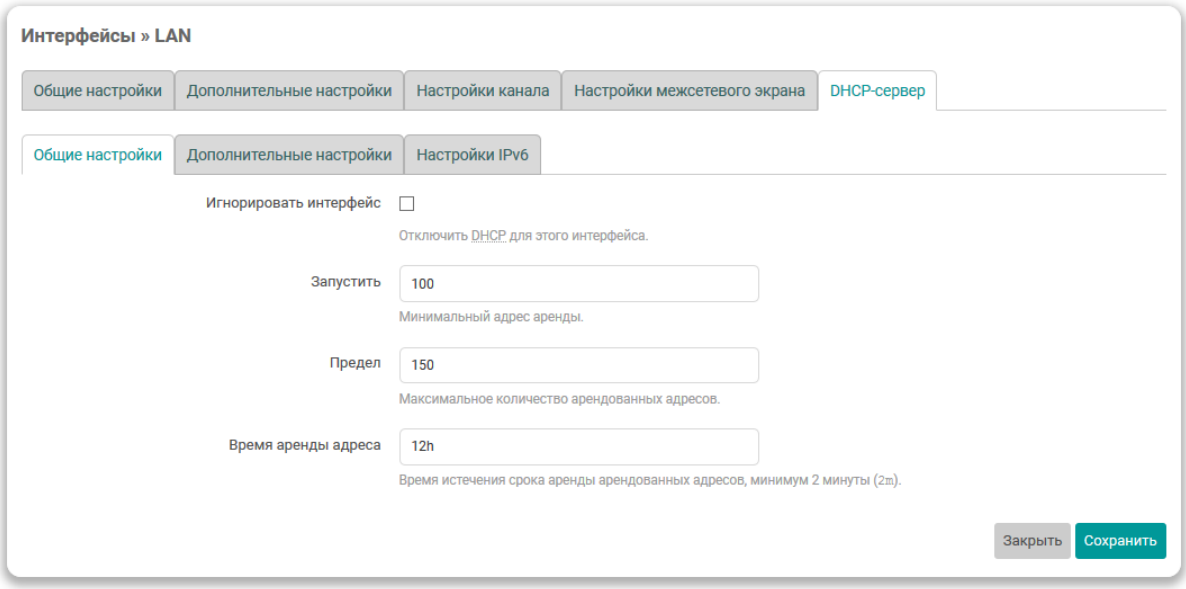


Рис. 7-13: Общие настройки DHCP-сервера сетевого интерфейса

Общие настройки DHCP-сервера представлены во вкладке «Общие настройки» (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).

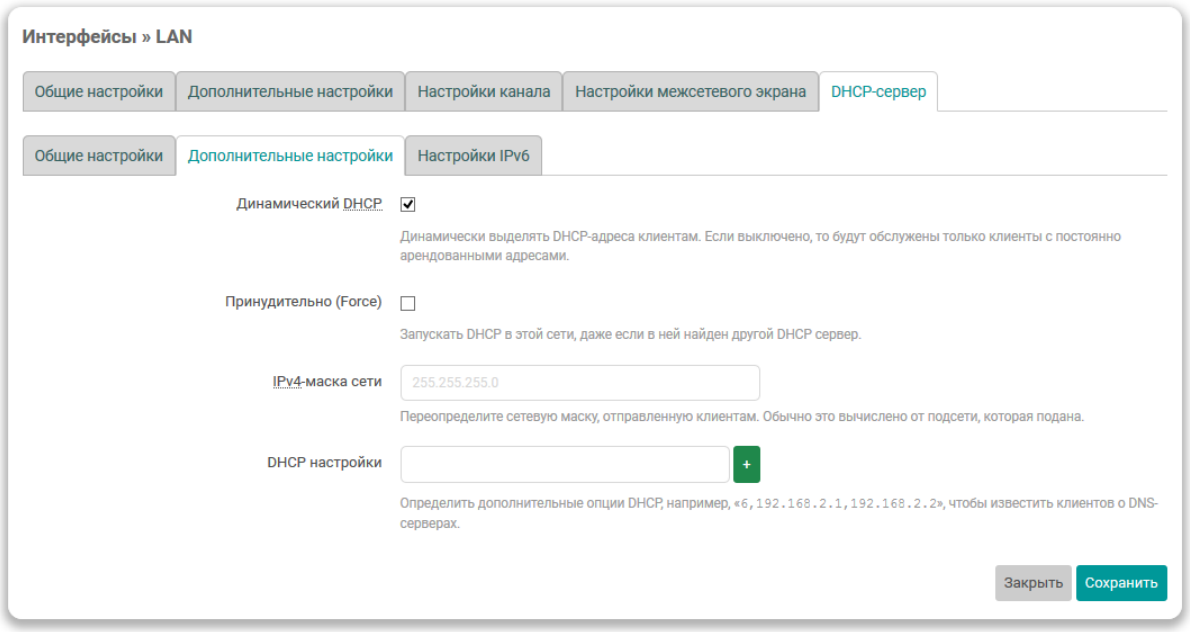


Рис. 7-14: Дополнительные настройки DHCP-сервера сетевого интерфейса

Если DHCP-сервер на интерфейсе включён, то во вкладке «Дополнительные настройки» (см. рисунок 7-14) будут 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.

- «Принудительно (Force)» — запускать DHCP-сервер на данном интерфейсе, даже если обнаружен другой DHCP-сервер в этой же сети.

  По умолчанию, если опция «Принудительно (Force)» отключена, то перед запуском DHCP-сервера на интерфейсе, в сеть будет отправлен DHCP-запрос. Если на отправленный запрос будет получен ответ, то DHCP-сервер запущен не будет. При этом, в системном журнале (см. раздел 3.5.2) можно будет обнаружить записи следующего вида:

  ```
  found already running DHCP-server on interface 'eth1' refusing to start, use 'option
      ← force 1' to override
  ```

- «IPv4-маска сети» — переопределение маски подсети, которая отдаётся клиентам.
- «DHCP настройки» — настройка позволяет определить произвольные DHCP опции [17], 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.

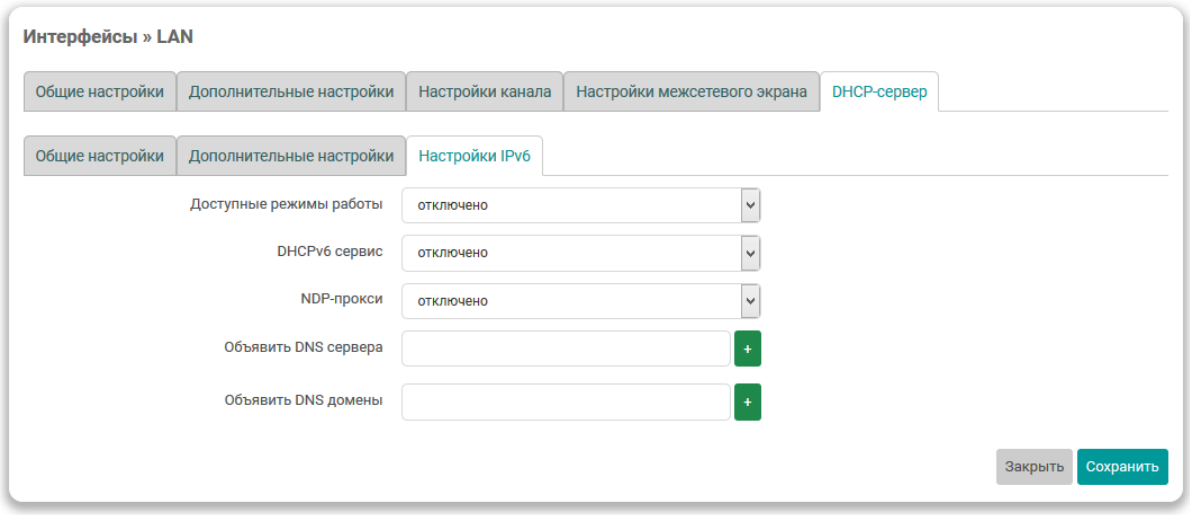


Рис. 7-15: IPv6 настройки DHCP-сервера сетевого интерфейса

Во вкладке «Настройки IPv6» 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].

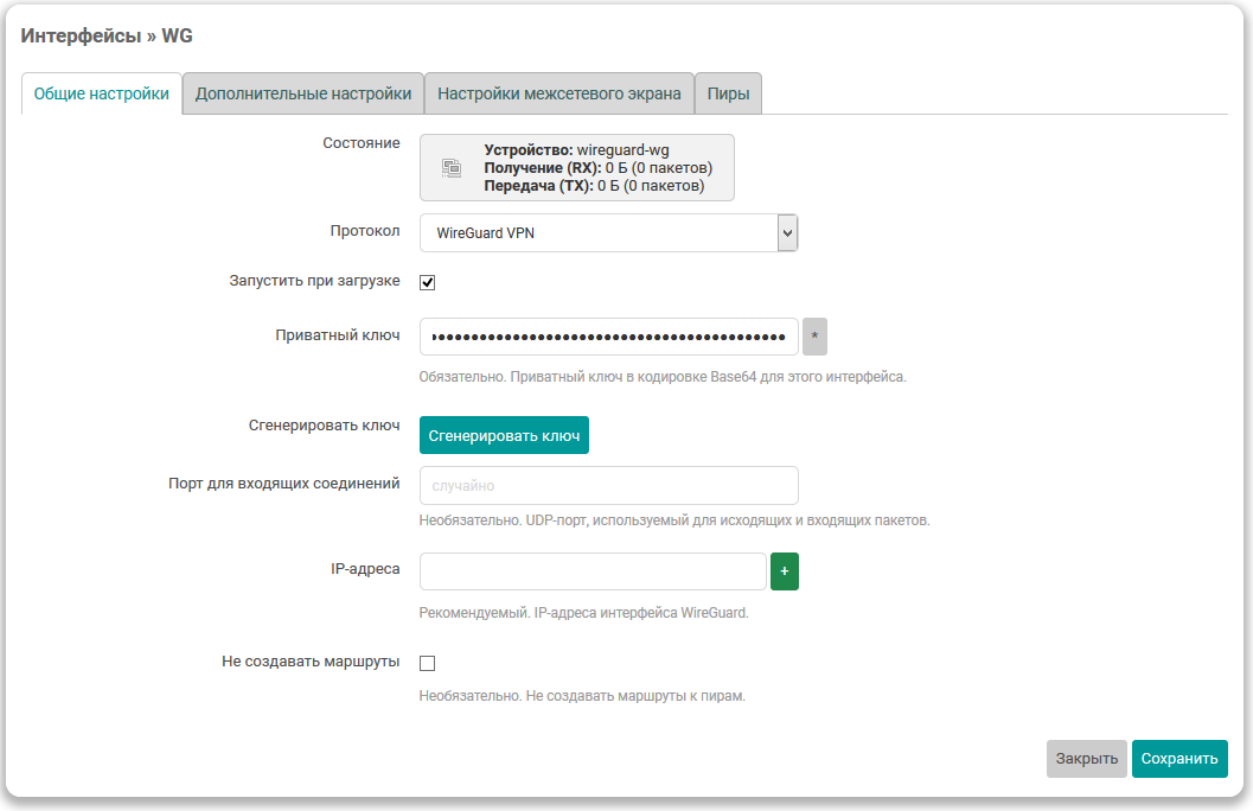


Рис. 7-16: Общие настройки интерфейса «WireGuard VPN»

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.
- «Сгенерировать ключ» — кнопка генерации нового случайного приватного ключа. Нажатие этой кнопки приведёт к генерации нового случайного приватного ключа, значение которого будет автоматически вставлено в поле ввода «Приватный ключ».
- «Порт для входящих соединений» — UDP-порт для входящих пакетов. По умолчанию, 51820.
- «IP-адреса» — разрешенные IP-адреса интерфейса WireGuard.

Во вкладке «Пиры» (см. рисунок 7-17) выполняется настройка удалённых WireGuard-серверов (пиров).

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

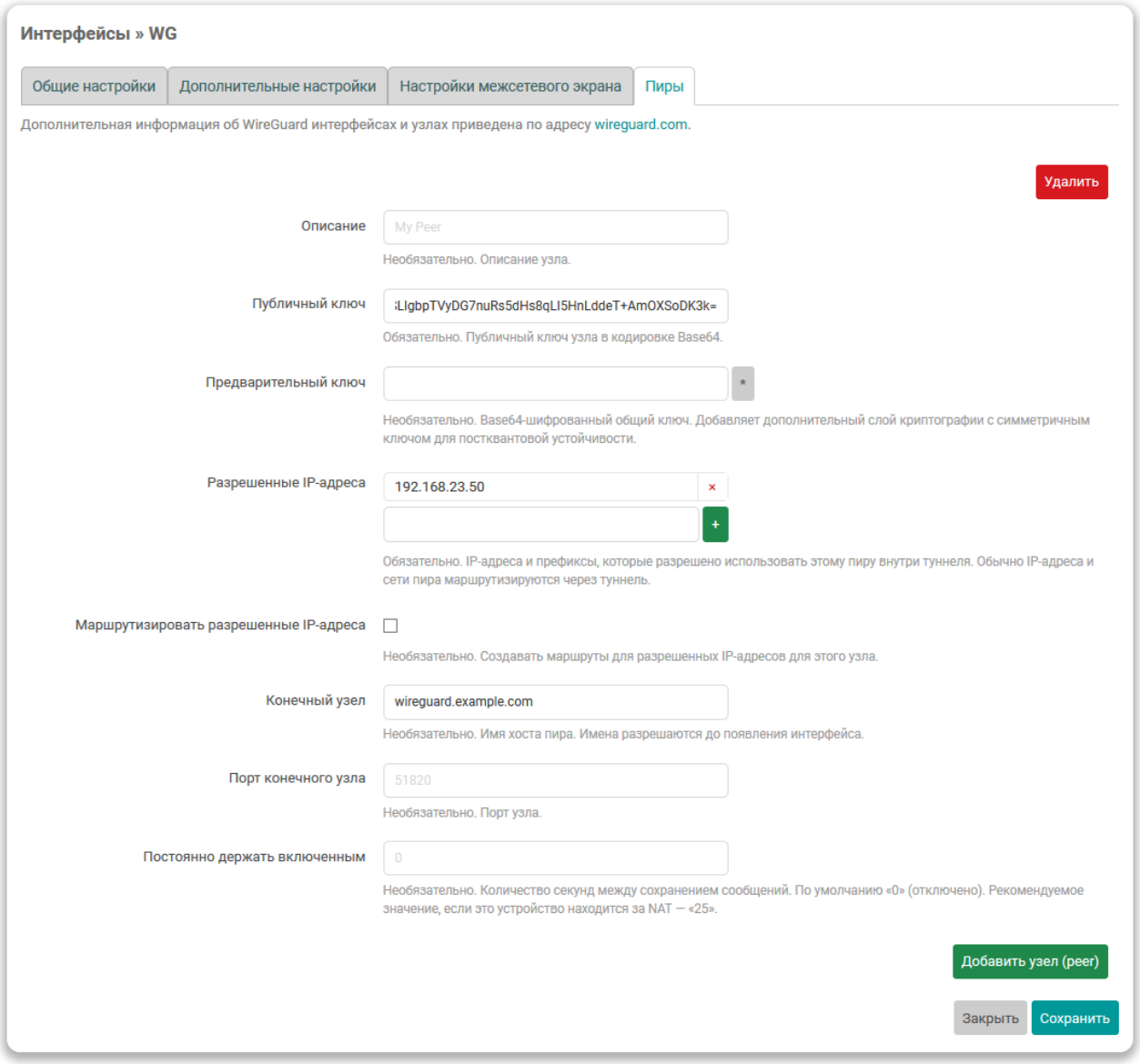


Рис. 7-17: Вкладка «Пиры» интерфейса «WireGuard VPN»

Для каждого WireGuard-сервера доступны следующие настройки:

- «Описание» — необязательное текстовое описание удалённого WireGuard-сервера.
- «Публичный ключ» — строка, куда вставляется сгенерированный в кодировке Base64 публичный ключ для интерфейса WireGuard.
- «Предварительный ключ» — шифрованный общий ключ, в кодировке Base64, который добавляет дополнительный слой криптографии с симметричным ключом для постквантовой устойчивости.
- «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».

Для добавления дополнительного удалённого WireGuard-сервера необходимо нажать кнопку «Добавить узел (peer)», расположенную внизу окна настроек (см. рисунок 7-16).

Для удаление удалённого WireGuard-сервера необходимо нажать кнопку «Удалить», расположенную перед блоком настроек соответствующего WireGuard-сервера (см. рисунок 7-16).

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 открыто всплывающее окно создания нового сетевого интерфейса, как показано на рисунке 7-18, на которой следует указать основные настройки создаваемого интерфейса, включая символьное имя и протокол интерфейса.

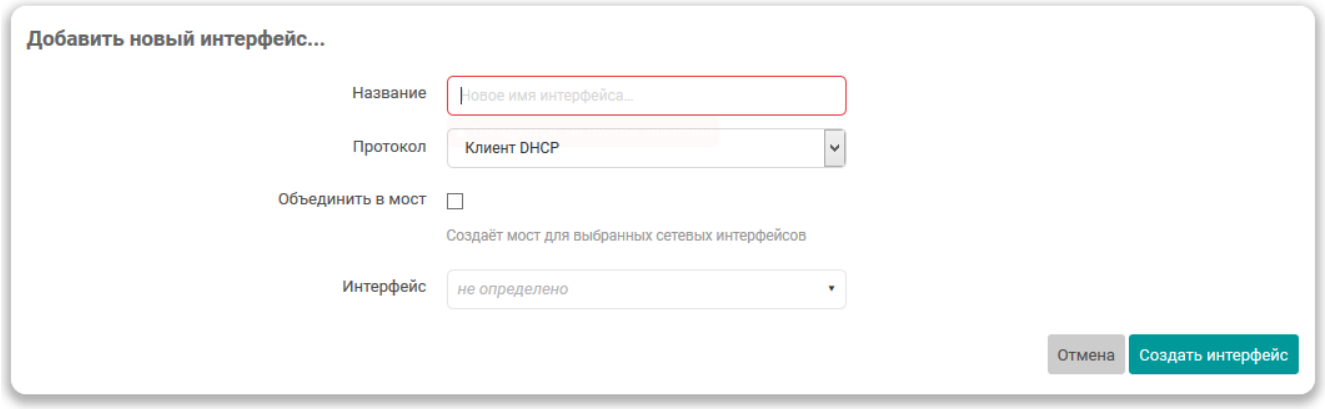


Рис. 7-18: Окно создания нового сетевого интерфейса

После ввода основных параметров интерфейса, для его создания следует нажать кнопку «Создать интерфейс». Если основные параметры создаваемого интерфейса были введены без ошибок, будет отображено окно редактирования нового интерфейса, которое подробно описано 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», интерфейс будет помечен для удаления. Реальное удаление интерфейса произойдёт только после сохранения и применения сделанных настроек (кнопка «Сохранить и применить»).

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 7-19.

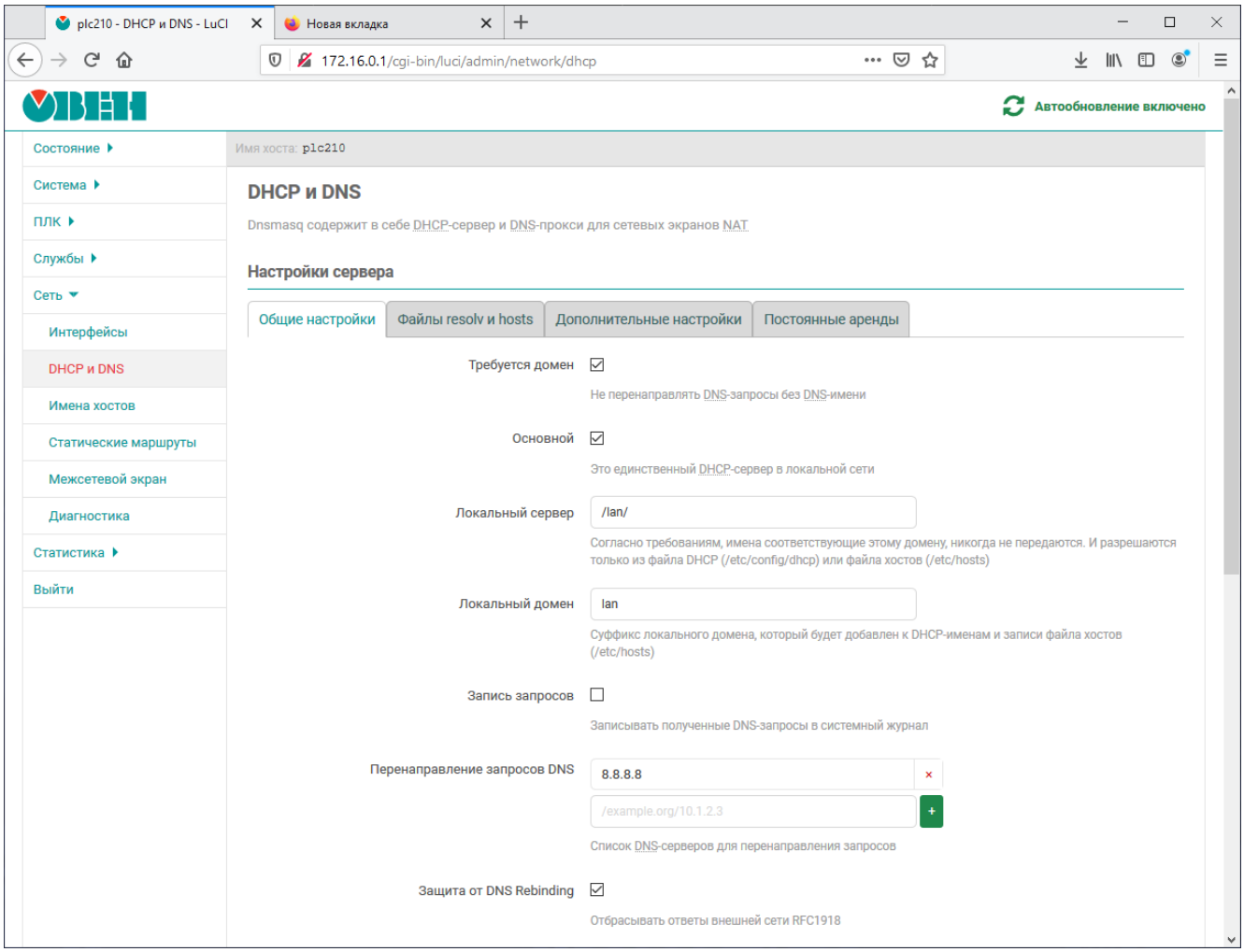


Рис. 7-19: Страница «DHCP и DNS»

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

- «Общие настройки» (см. раздел 7.2.1);
- «Файлы resolv и hosts» (см. раздел 7.2.2);
- «Дополнительные настройки» (см. раздел 7.2.3);
- «Постоянные аренды» (см. раздел 7.2.4).

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 7-20.

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»).

Рис. 7-20: Общие настройки службы dnsmasq

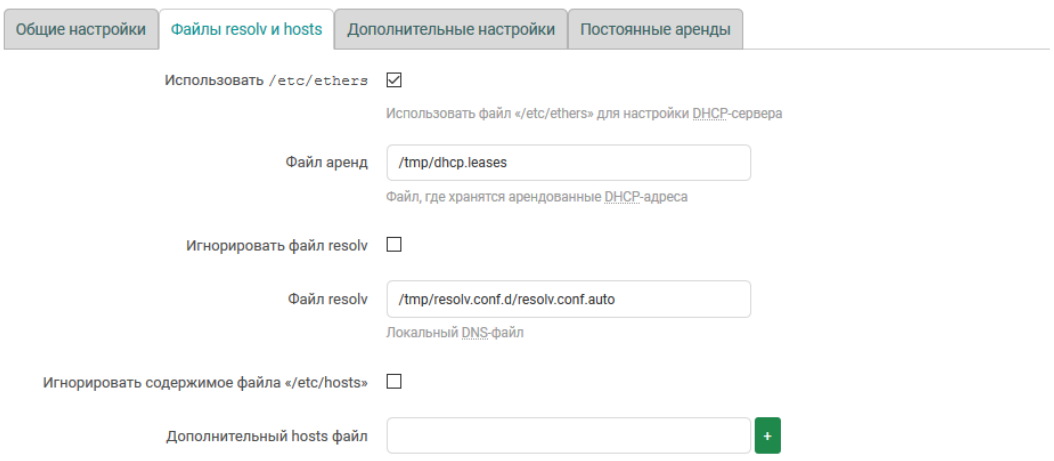


Рис. 7-21: Настройки файлов resolv.conf и hosts службы dnsmasq

- «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 [18].

  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 [13].
- «Разрешить локальный хост» — включает или отключает ответы внешней сети в диапазоне 127.0.0.0/8.
- «Белый список доменов» — Список доменов, для которых разрешены ответы RFC1918 [13].
- «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).
- «Интерфейс для входящих соединений» — список интерфейсов для прослушивания. По умолчанию прослушиваются все интерфейсы. При указании списка интерфейсов для прослушивания, служба будет прослушивать порты указанных интерфейсов а также интерфейса локальной петли (loopback).
- «Исключить интерфейсы» — Список интерфейсов, на которых запрещено прослушивание службы dnsmasq.

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

Во вкладке «Файлы resolv и hosts» страницы «DHCP и DNS» расположены настройки, касающиеся файлов «resolv.conf» [19] и «hosts» [20]. Внешний вид вкладки «Файлы resolv и hosts» показан на рисунке 7-21.

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

- «Использовать /etc/ethers» — указание использовать конфигурационный файл «/etc/ethers» [21] 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 содержимое файла /etc/hosts» — указание службе dnsmasq игнорировать данные файла «/etc/hosts».
- «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».

7.2.3 Дополнительные настройки

Дополнительные настройки службы dnsmasq расположены во вкладке «Дополнительные настройки» страницы «DHCP и DNS». Внешний вид вкладки «Дополнительные настройки» показан на рисунке 7-22.

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.

Рис. 7-22: Дополнительные настройки службы dnsmasq

- «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.
- «Максимальное кол-во DHCP аренд» — максимальное количество активных арендованных DHCP-адресов.
- «Максимальный EDNS0 размер пакета» — максимально допустимый размер EDNS.0 UDP пакетов.
- «Максимальное количество 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.

7.2.4 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 во вкладке «Постоянные аренды» страницы «DHCP и DNS». Внешний вид вкладки «Постоянные аренды» показан на рисунке 7-23.

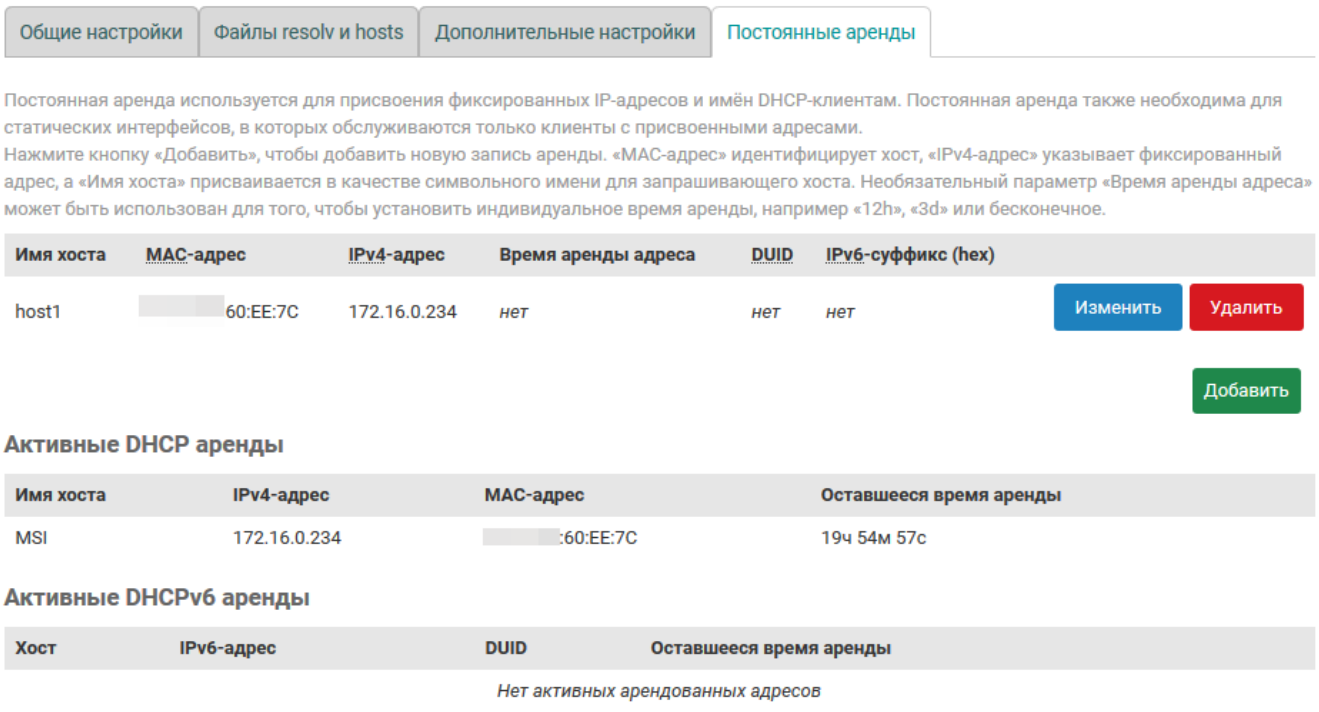


Рис. 7-23: Настройка постоянных аренд службы dnsmasq

Добавление новой постоянной аренды осуществляется нажатием кнопки «Добавить» с последующим указанием параметров постоянной аренды в открывшемся всплывающем окне настроек постоянной аренды (см. рисунок 7-24).

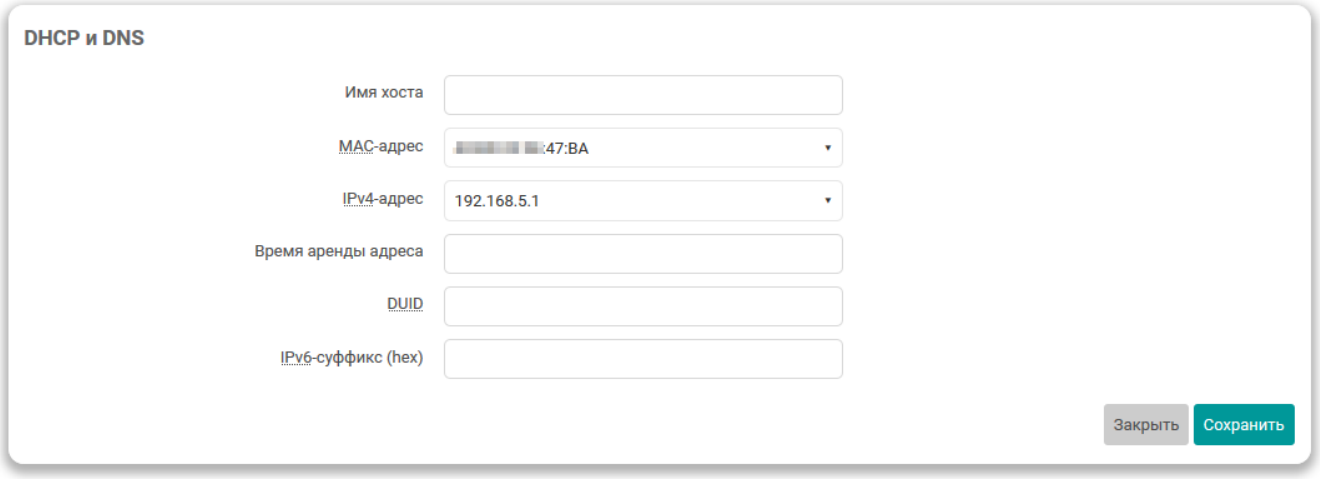


Рис. 7-24: Добавление записи постоянной аренды DHCP-сервера

Изменение существующих записей статических адресов осуществляется при помощи кнопки «Изменить», расположенной в самом правом столбце таблицы статических адресов для каждой из записей (см. рисунок 7-23).

Удалить существующую постоянную аренду можно при помощи кнопки «Удалить», расположенной в строке соответствующей записи (см. рисунок 7-23).

Дополнительно, на вкладке «Постоянные аренды» в подразделах «Активные DHCP аренды» и «Активные DHCPv6 аренды» приводятся таблицы текущих арендованных адресов для IP протоколов версий 4 и 6 (см. рисунок 7-25).

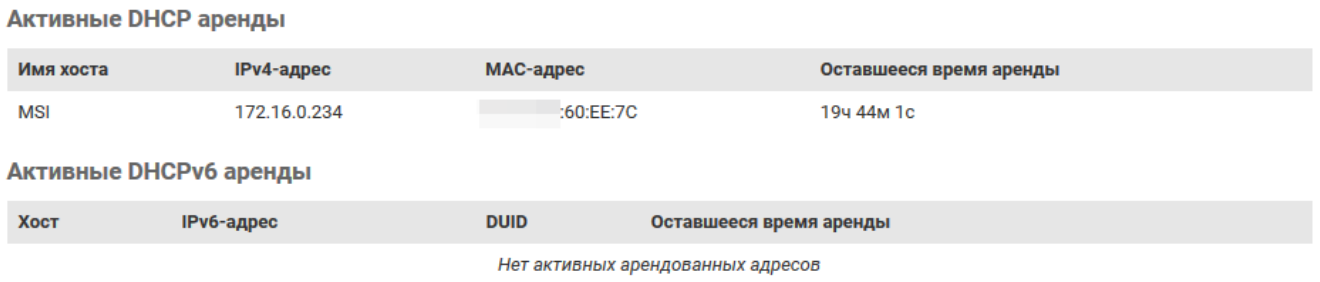


Рис. 7-25: Активные аренды DHCP-сервера

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).

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 7-26.

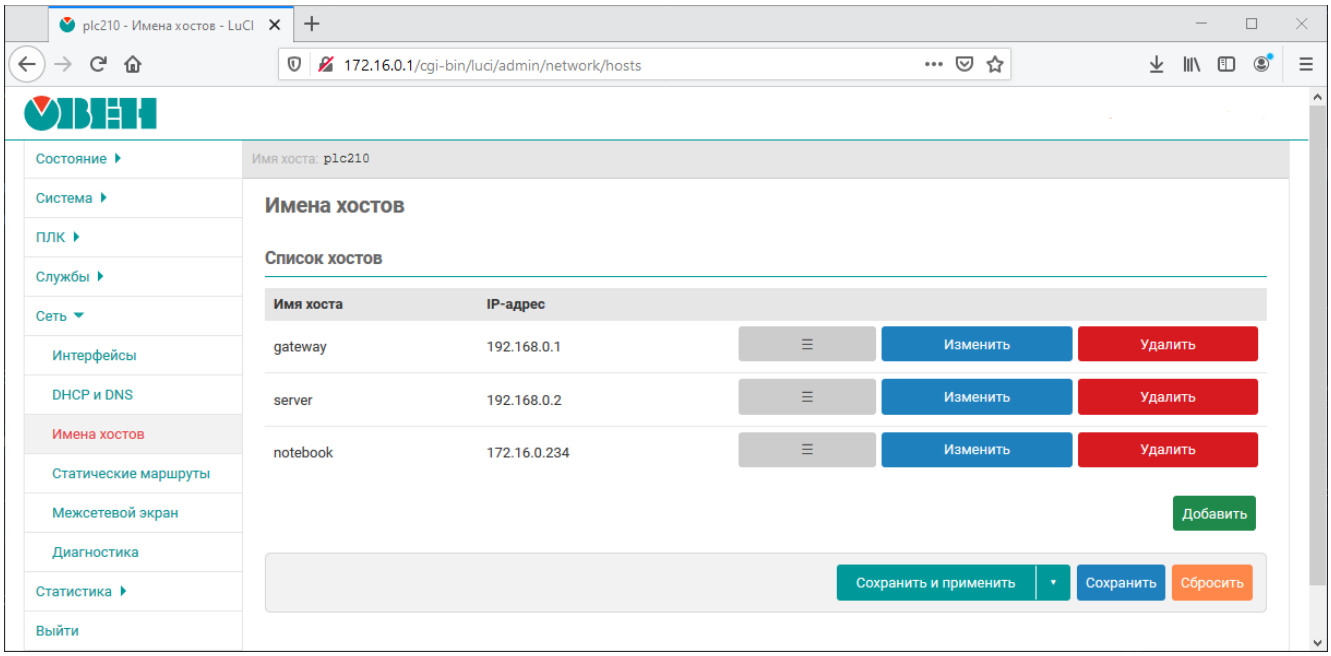


Рис. 7-26: Страница «Имена хостов»

Добавление нового имени хоста осуществляется нажатием кнопки «Добавить» с последующим указанием имени хоста и соответствующего ему IP-адреса в открывшемся всплывающем окне настроек записи, как показано на рисунке 7-27).

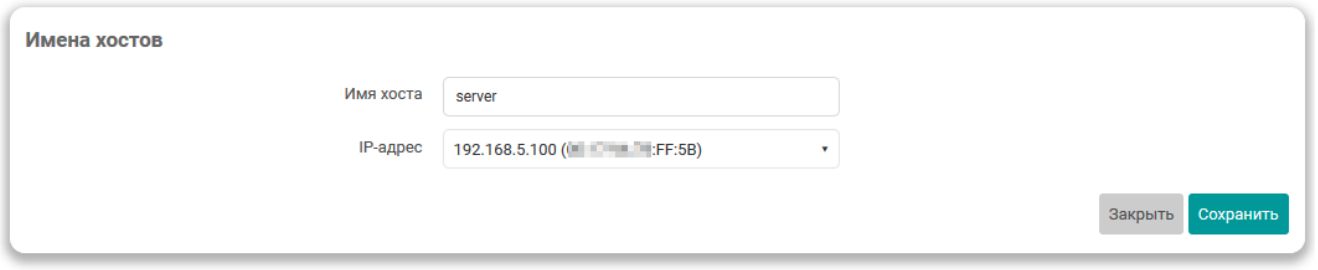


Рис. 7-27: Страница «Имена хостов». Окно настроек записи

Для редактирования уже существующей записи предназначена кнопка «Изменить» в правой части таблицы хостов. При нажатии кнопки «Изменить» будет открыто всплывающее окно с редактирования параметров соответствующей записи полностью аналогичное окну при добавлении новой записи (см. рисунок 7-27).

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 7-28.

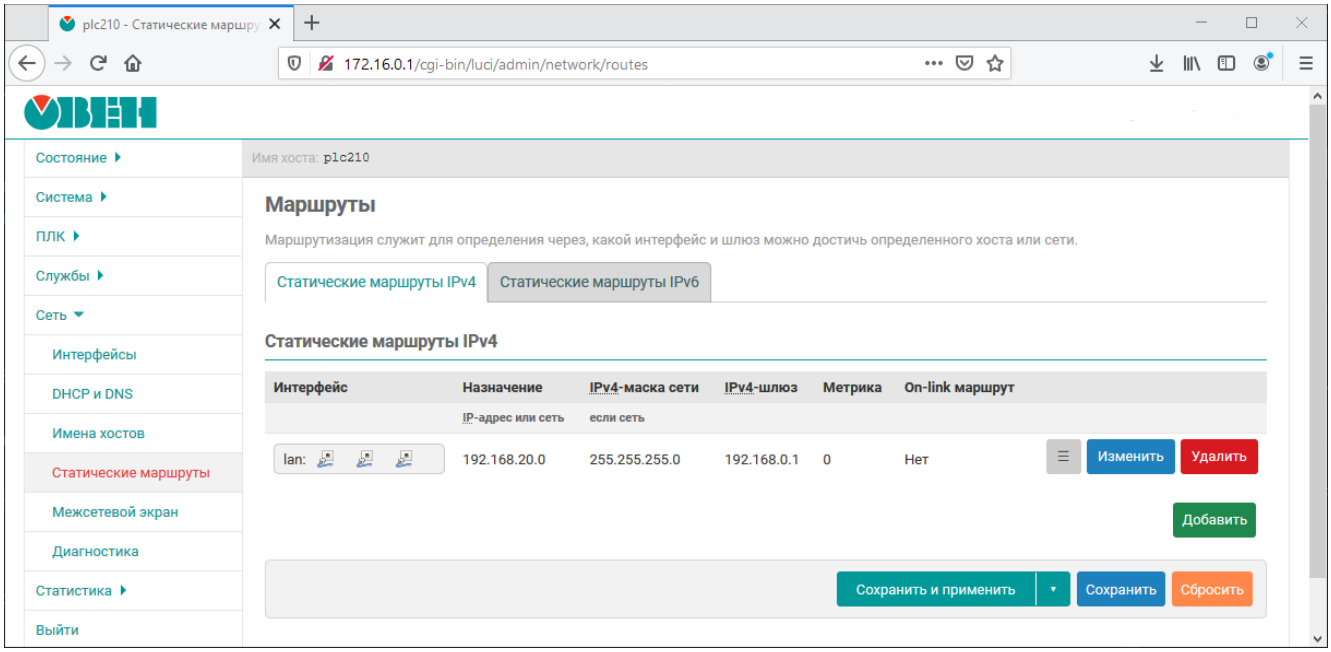


Рис. 7-28: Страница «Статические маршруты»

Страница «Статические маршруты» разделена на две вкладки «Статические маршруты IPv4» и «Статические маршруты IPv6» предназначенные для управления статическими маршрутами для IPv4 и IPv6 соответственно.

Далее рассмотрено управление статическими маршрутами только для IPv4, так как для IPv6 все действия и настройки маршрутов полностью совпадают.

Добавление нового статического маршрута осуществляется нажатием кнопки «Добавить». При нажатии кнопки «Добавить» будет открыто всплывающее окно настроек добавляемого маршрута, как показано на рисунке 7-30.

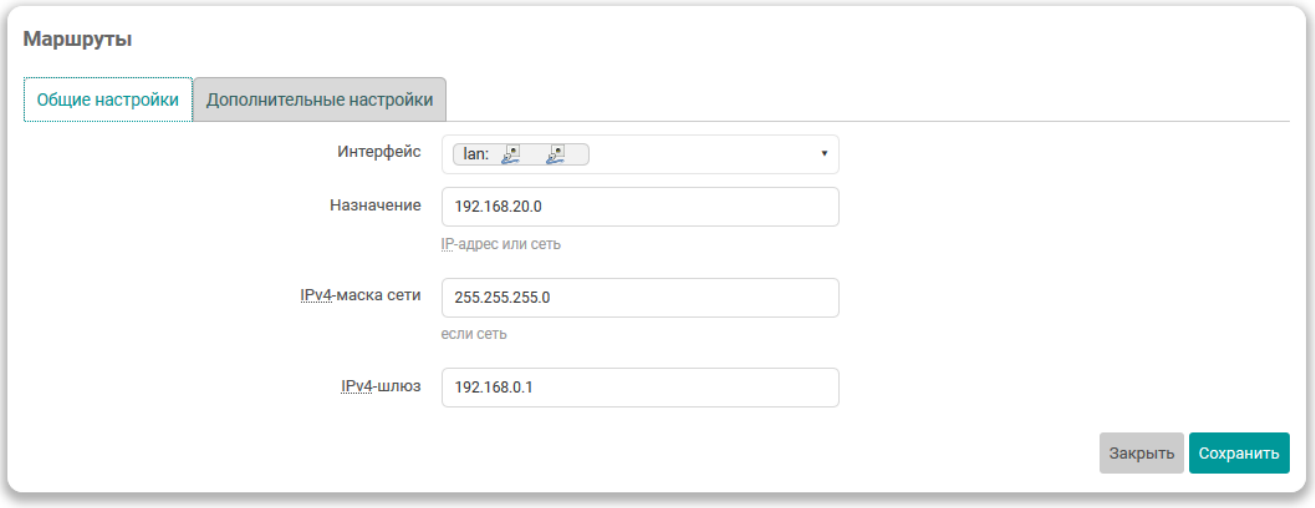


Рис. 7-29: Страница «Статические маршруты». Окно настроек маршрута

Для редактирования уже существующего маршрута предназначена кнопка «Изменить» в правой части таблицы маршрутов. При нажатии кнопки «Изменить» будет открыто всплывающее окно с редактирования

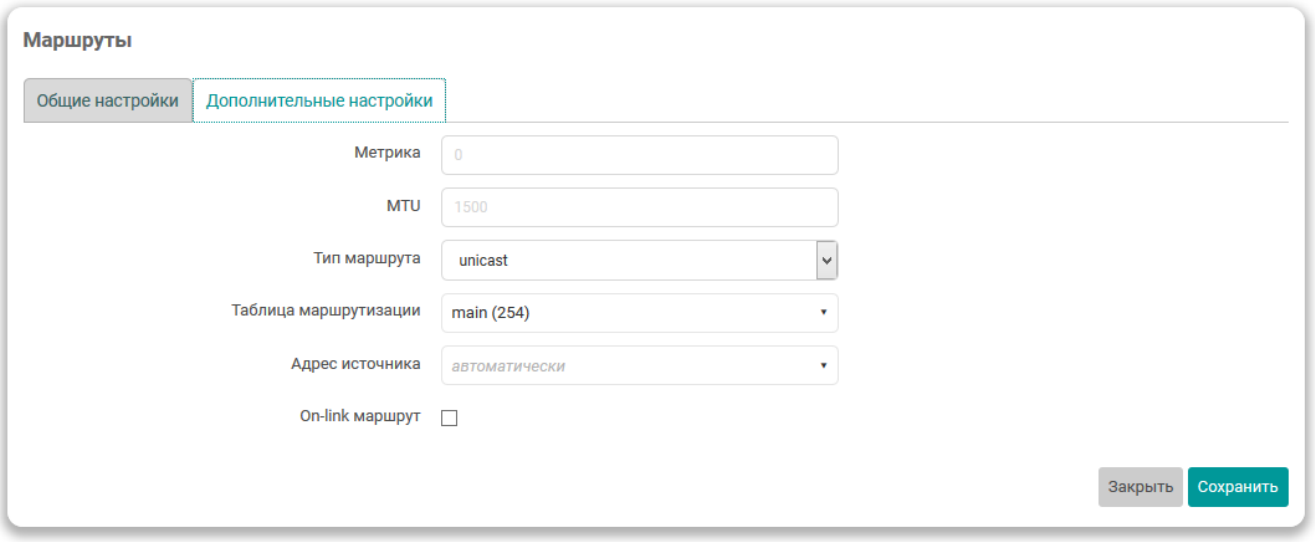


Рис. 7-30: Страница «Статические маршруты». Дополнительные настройки маршрута

параметров соответствующего маршрута полностью аналогичное окну при добавлении нового маршрута (см. рисунок 7-27).

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).
- «Правила NAT» — настройка правил NAT межсетевого экрана (см. раздел 7.5.5).
- «Пользовательские правила» — настройка пользовательских правил межсетевого экрана (см. раздел 7.5.6).

7.5.1 Общие настройки

Внешний вид страницы «Межсетевой экран» с открытой вкладкой «Общие настройки» показан на рисунке 7-31.

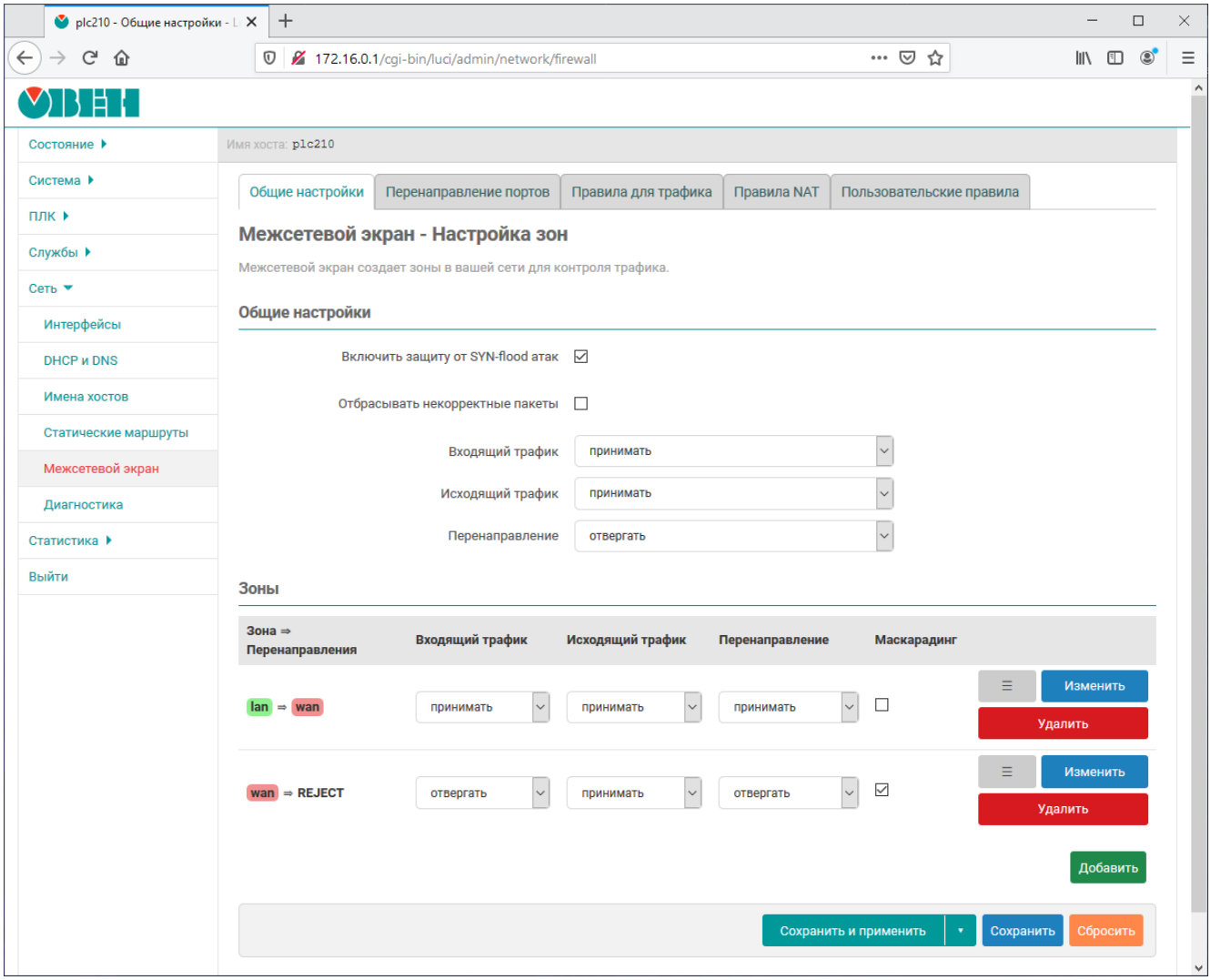


Рис. 7-31: Общие настройки межсетевого экрана

На данной вкладке содержатся следующие настройки межсетевого экрана:

- «Включить защиту от SYN-flood атак» — управление функцией защиты от SYN-flood атак [22].
- «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 настройки» страницы «Межсетевой экран») перечислены существующие зоны в виде таблицы с их основными параметрами в столбцах (см. рисунок 7-32):

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

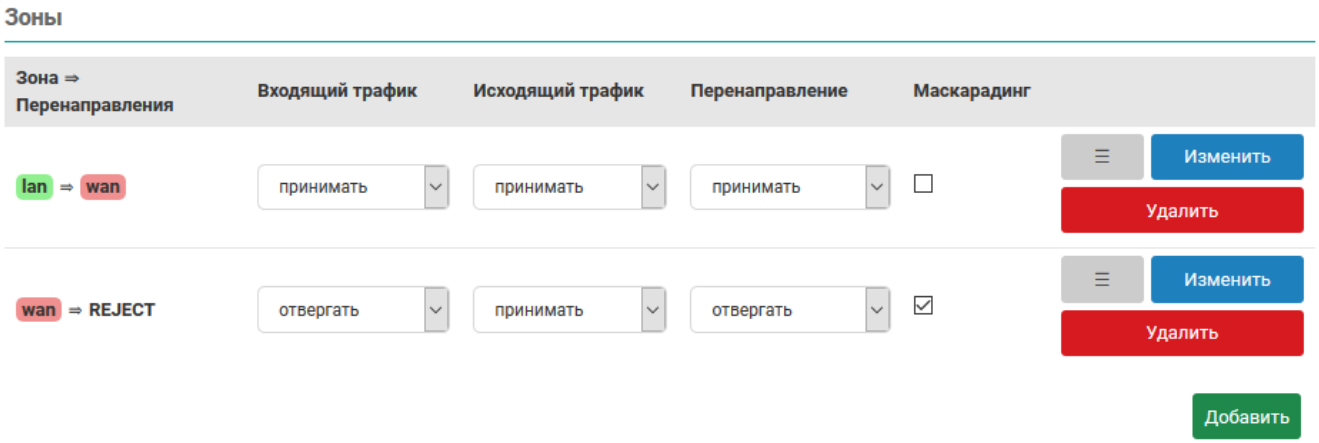


Рис. 7-32: Настройка зон межсетевого экрана. Таблица зон

В последнем столбце таблицы для каждой зоны расположены кнопки управления:

- «☰» — кнопка изменения порядка записей в таблице. Удерживая нажатой данную кнопку можно перемещать строку таблицы, изменяя тем самым её порядок.
- «Изменить» — кнопка редактирования параметров зоны (см. раздел 7.5.2.1).
- «Удалить» — кнопка удаления зоны (см. раздел 7.5.2.3).

7.5.2.1 Редактирование зон

Основные параметры зоны можно изменить в строке таблицы зон при помощи соответствующих элементов управления (см. рисунок 7-32). Для изменения дополнительных параметров зоны необходимо нажать кнопку «Изменить» в строке соответствующей зоны. При этом откроется всплывающее окно редактирования параметров зоны с вкладками:

- «Общие настройки» (см. раздел 7.5.2.1.1);
- «Дополнительные настройки» (см. раздел 7.5.2.1.2);
- «Отслеживание соединений (conntrack)» (см. раздел 7.5.2.1.3);
- «Дополнительные аргументы iptables» (см. раздел 7.5.2.1.4).

7.5.2.1.1 Вкладка «Общие настройки»

Внешний вид окна редактирования параметров зоны межсетевого экрана с открытой вкладкой «Общие настройки» показан на рисунке 7-33

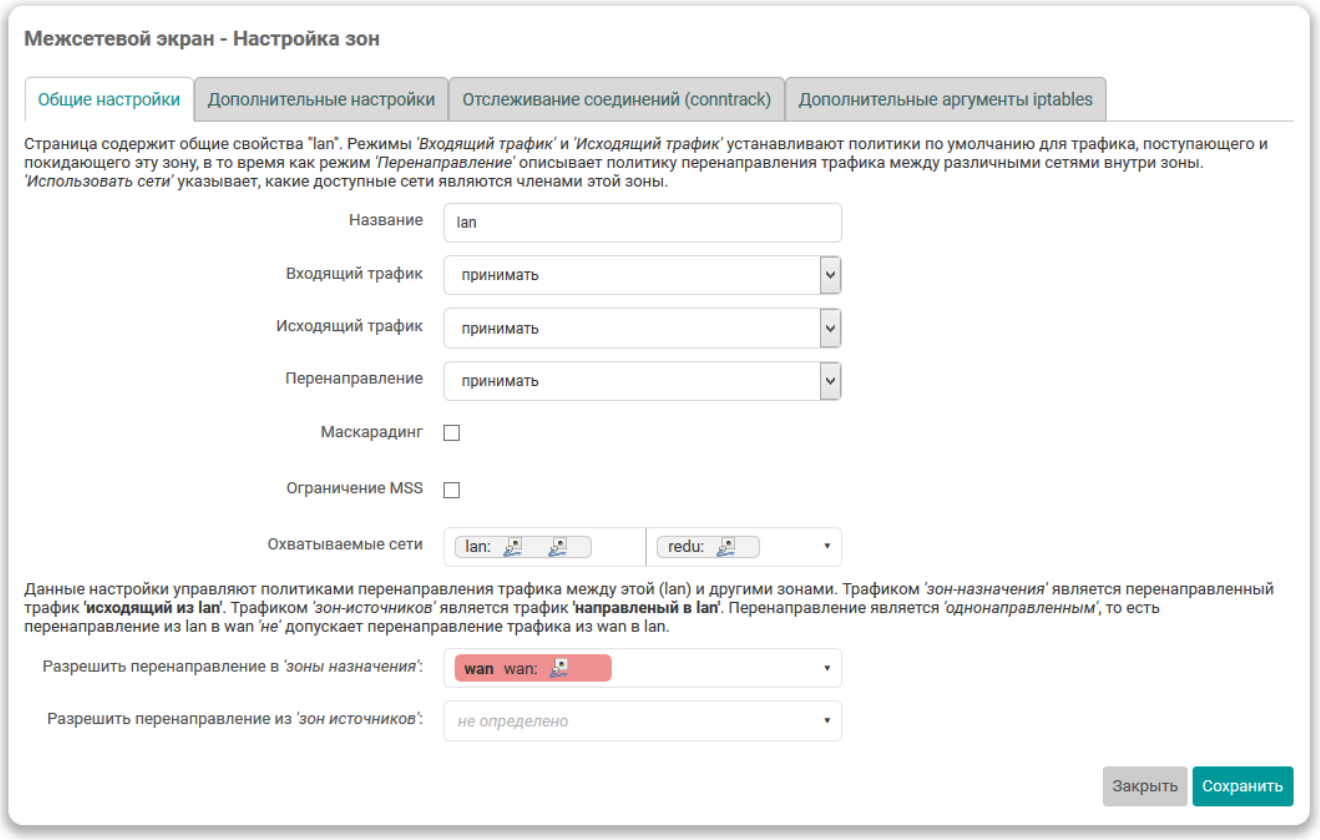


Рис. 7-33: Окно настроек зоны межсетевого экрана. Вкладка «Общие настройки»

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.
- «Ограничение MSS» — включает или отключает ограничение MSS при передаче для данной зоны.
- «Использовать сети» — выбор сетевых интерфейсов, входящих в указанную зону.
- «Охватываемые сети» — список сетей, входящих в настраиваемую зону.

Дополнительно, на вкладке «Общие настройки», для каждой зоны указывается политика перенаправления между зонами при помощи следующих настроек:

- «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.

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.

7.5.2.1.2 Вкладка «Дополнительные настройки»

Внешний вид вкладки «Дополнительные настройки» показан на рисунке 7-34

На вкладке «Дополнительные настройки» доступны следующие настройки:

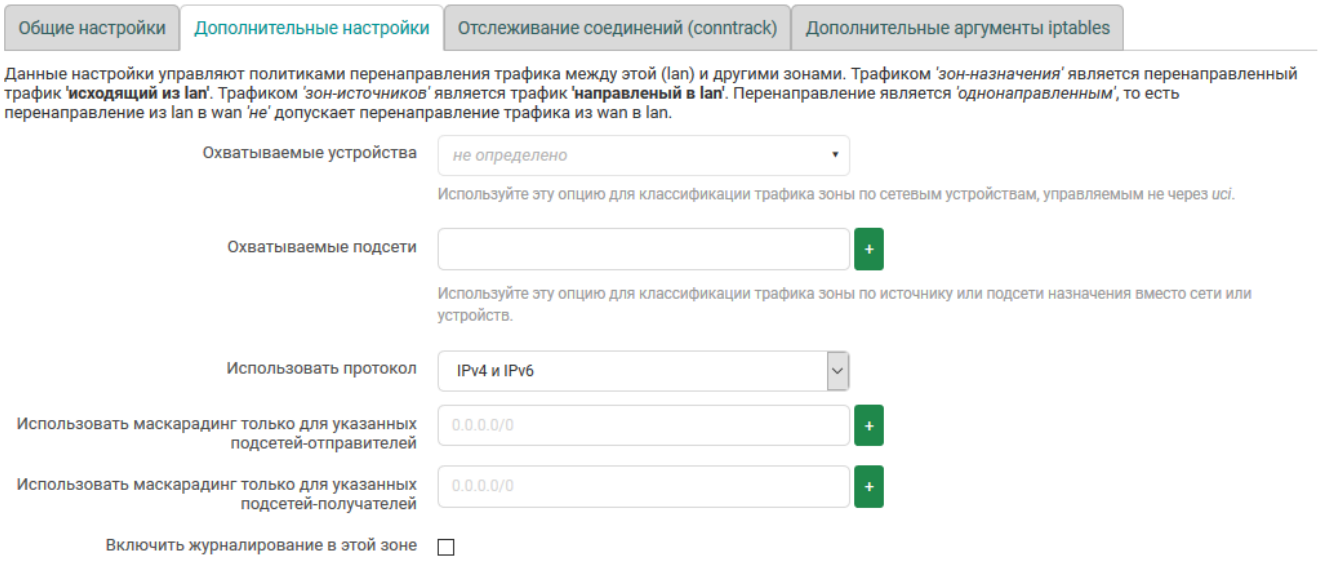


Рис. 7-34: Окно настроек зоны межсетевого экрана. Вкладка «Дополнительные настройки»

- «Охватываемые устройства» — настройка позволяет классифицировать трафик зоны по сетевым устройствам (в том числе сетевые устройства не управляемые через веб-интерфейс).
- «Охватываемые подсети» — настройка позволяет классифицировать трафик зоны по истонику или подсети назначения вместо сети или устройства.
- «Использовать протокол» — выбор версии используемого IP-протокола в указанной зоне. Возможен выбор из вариантов:
  - «только IPv4»;
  - «только IPv6»;
  - «IPv4 и IPv6».
- «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 журналирование в этой зоне» — включает или отключает запись срабатывания правил межсетевого экрана для данной зоны в системный журнал

7.5.2.1.3 Вкладка «Отслеживание соединений (conntrack)»

Внешний вид вкладки «Отслеживание соединений (conntrack)» показан на рисунке 7-35

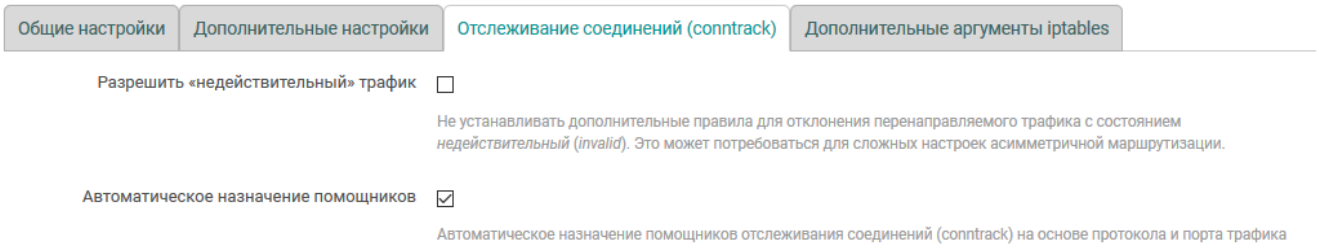


Рис. 7-35: Окно настроек зоны межсетевого экрана. Вкладка «Отслеживание соединений (conntrack)»

На вкладке «Отслеживание соединений (conntrack)» доступны следующие настройки:

- «Разрешить „недействительный“ трафик» — настройка позволяет не устанавливать дополнительные правила для отклонения перенаправляемого трафика с состоянием недействительный (invalid). Это может потребоваться, например, для сложных настроек асимметричной маршрутизации.
- «Автоматическое назначение помощников» — управляет автоматическим назначением помощников отслеживания соединений (conntrack) на основе протокола и порта трафика для редактируемой зоны.

7.5.2.1.4 Вкладка «Дополнительные аргументы iptables»

На вкладке «Дополнительные аргументы iptables» расположены настройки, позволяющие передать произвольные аргументы iptables [5] в правила классификации входящего и исходящего трафика зоны.

Передача аргументов iptables в правилах классификации входящего и исходящего трафика позволяет сопоставлять пакеты, основанные на других критериях, нежели чем интерфейсы или подсети. Эти опции следует использовать с особой осторожностью, так как неверные значения могут привести к нарушению работы правил межсетевого экрана, полностью открывая доступ ко всем службам системы.

Внешний вид вкладки «Дополнительные аргументы iptables» показан на рисунке 7-36

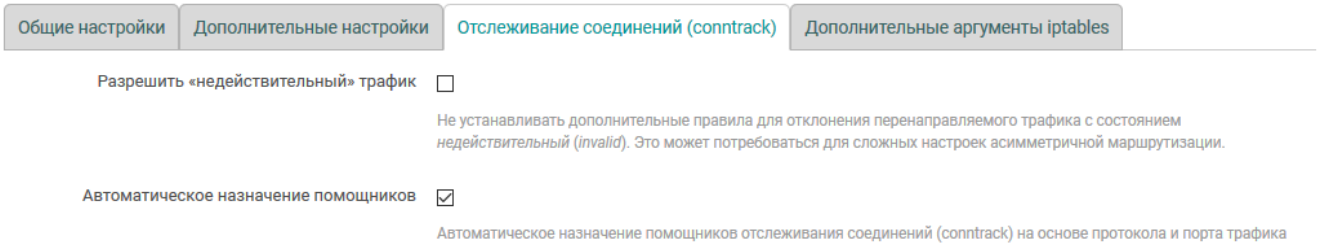


Рис. 7-36: Окно настроек зоны межсетевого экрана. Вкладка «Дополнительные аргументы iptables»

На вкладке «Дополнительные аргументы iptables» доступны следующие настройки:

- «Дополнительные аргументы для источника» — дополнительные аргументы iptables для классификации трафика зоны источника. Например, для классификации только входящего трафика HTTPS (TCP порт 443):

```
-p tcp --sport 443
```

- «Дополнительные аргументы для назначения» — дополнительные аргументы iptables для классификации трафика зоны назначения. Например, для классификации только исходящего трафика HTTPS (TCP порт 443):

```
-p tcp --dport 443
```

7.5.2.2 Добавление зон

Для добавления новой зоны предназначена кнопка «Добавить», расположенная снизу таблицы зон (см. рисунок 7-32). При этом откроется всплывающее окно редактирования параметров зоны, как и при изменении (редактировании) 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 7-32).

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.

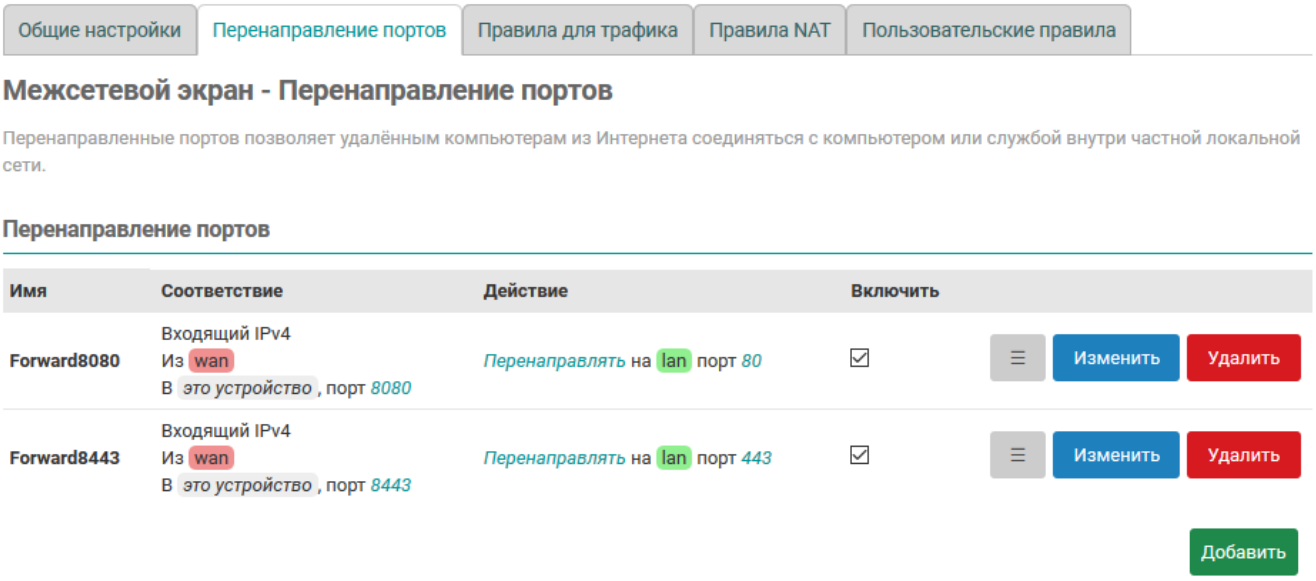


Рис. 7-37: Вкладка «Перенаправление портов» страницы «Межсетевой экран»

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.
- «Соответствие» — в данном столбце приведены условия для входящего трафика, при совпадении которых данное правило будет применяться.
- «Действие» — в данном столбце приведено действие, которое будет применено к входящему трафику (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 предназначена кнопка «≡» (см. рисунок 7-37), позволяющя переместить соответствующее правило в таблице.

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 всплывающее окно настроек правила перенаправления портов, как показано на рисунке 7-38.

Данное окно разделено на две вкладки:

- «Общие настройки» (см. раздел 7.5.3.2.1);
- «Дополнительные настройки» (см. раздел 7.5.3.2.2).

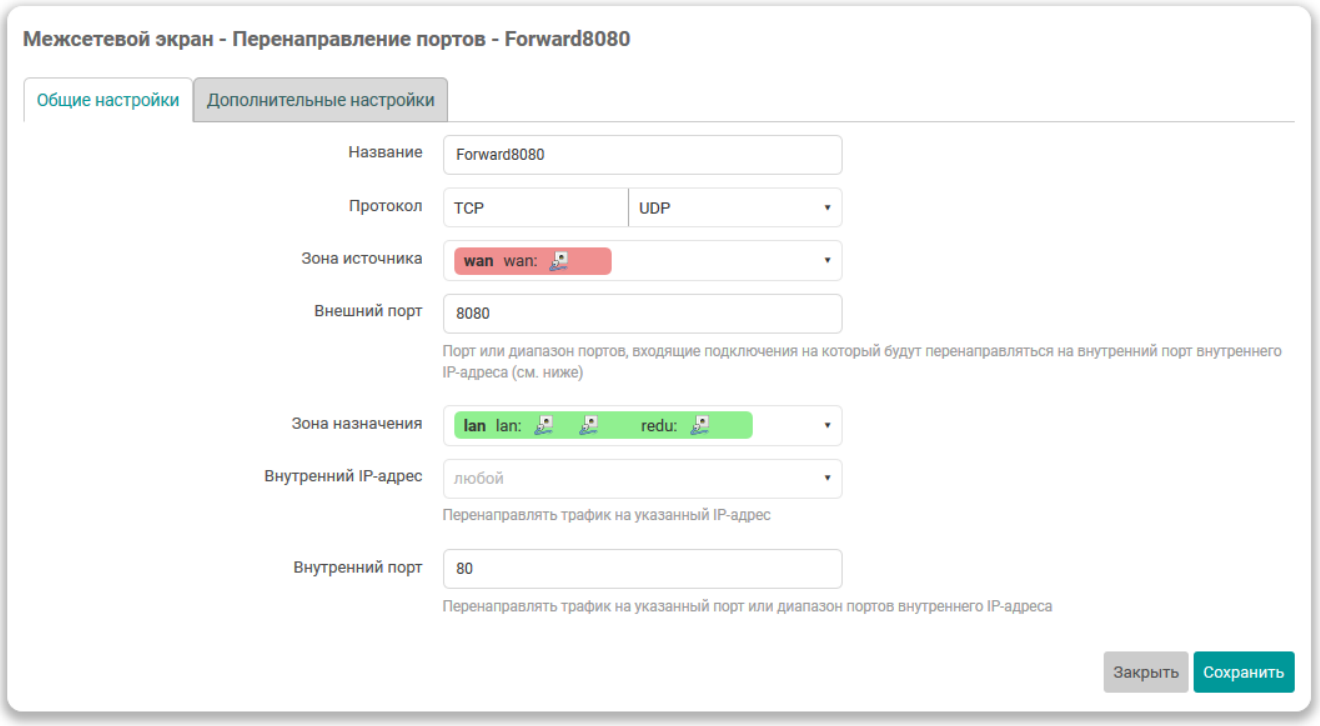


Рис. 7-38: Окно настроек правила перенаправления портов межсетевого экрана

7.5.3.2.1 Вкладка «Общие настройки»

Внешний вид вкладки «Общие настройки» показан на рисунке 7-38.

На данной вкладке доступны для редактирования следующие настройки:

- «Имя» — уникальное символьное имя правила.
- «Протокол» — выбор протоколов для правила. Возможен выбор одного или нескольких протоколов из следующего списка:
  - «любой» — любой протокол. При выборе данного варианта, другие протоколы выбрать нельзя;
  - «UDP»;
  - «TCP»;
  - «ICMP»;
  - пользовательский (произвольное имя протокола).

  В зависимости от выбранного протокола набор прочих настроек может несущественно меняться.
- «Зона источника» — выбор зоны источника трафика для правила.
- «Внешний порт» — позволяет ограничить применение правила для входящих подключений на указанный порт или диапазон портов. Данная настройка доступна только для UDP и TCP протоколов.
- «Зона назначения» — 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.

7.5.3.2.2 Вкладка «Дополнительные настройки»

Внешний вид вкладки «Дополнительные настройки» показан на рисунке 7-39.

На данной вкладке доступны для редактирования следующие настройки:

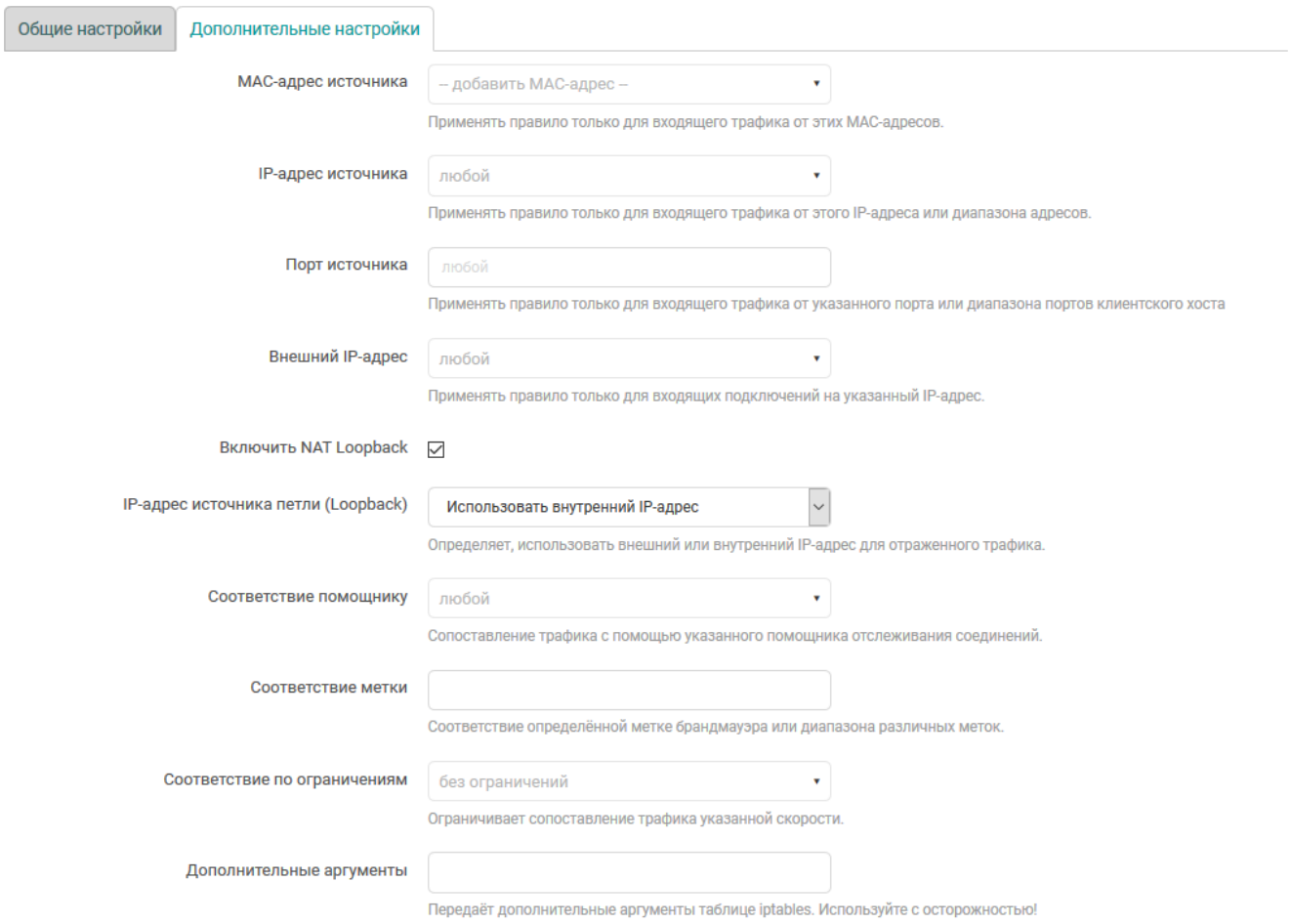


Рис. 7-39: Окно настроек правила перенаправления портов межсетевого экрана. Вкладка «Дополнительные настройки»

- «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.
- «Включить NAT Loopback» — включить для данного правила технологию NAT Loopback [23].

  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.

  При включении данной настройки появляется дополнительная опция «IP-адрес источника петли (loopback)», при помощи которой можно выбрать какой IP-адрес будет использоватся для отраженного трафика — внутренний или внешний.
- «Соответствие помощнику» — настройка позволяет указать конкретного помощника отслеживания соединений (conntrack).
- «Соответствие метки» — настройка позволяет указать метку или диапазон меток межсетевого экрана для соответствия трафика правила.

- «Соответствие по ограничениям» — настройка ограничивает сопоставление трафика указанной скорости.
- «Дополнительные аргументы» — позволяет указать дополнительные аргументы для команды iptables.

7.5.3.3 Добавление правил перенаправления портов

Для добавления нового правила перенаправления портов предназначена кнопка «Добавить», расположенная снизу таблицы перенаправления портов (см. рисунок 7-37). При этом откроется всплывающее окно редактирования параметров правила, как и при изменении (редактировании) существующего правила (см. 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).

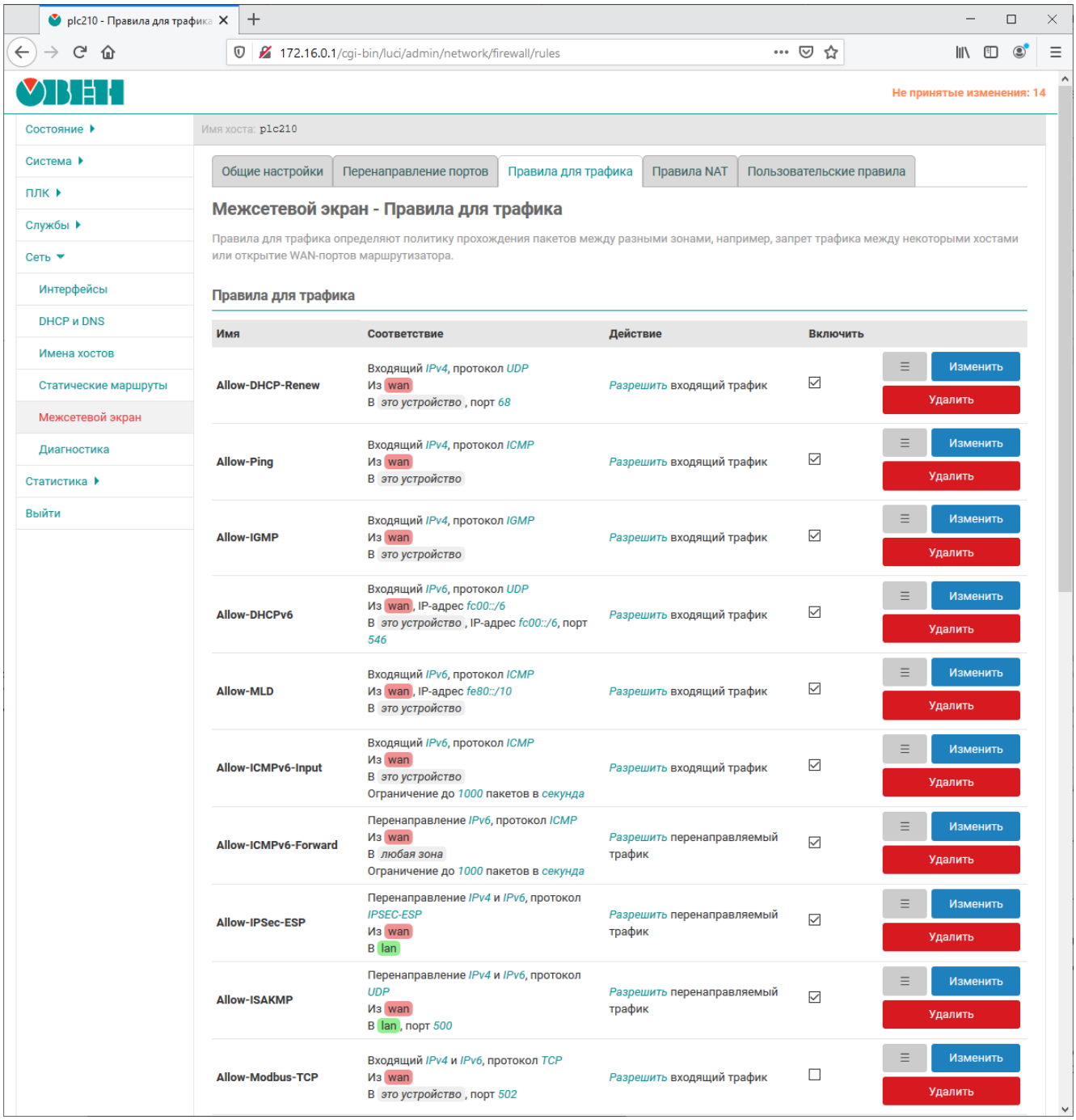


Рис. 7-40: Правила для трафика межсетевого экрана

На странице приведена таблица «Правила для трафика» с перечислением уже созданных правил для трафика. Таблица имеет следующие столбцы:

- «Имя» — уникальное символьное имя правила.
- «Соответствие» — в данном столбце приведены условия для входящего трафика, при совпадении которых данное правило будет применяться.
- «Действие» — действие, применяемое для трафика данного правила.
- «Включить» — позволяет включить или отключить данное правило. 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 предназначена кнопка «≡» (см. рисунок 7-40), позволяющя переместить соответствующее правило в таблице.

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 всплывающее окно настроек правила для трафика, как показано на рисунке 7-41.

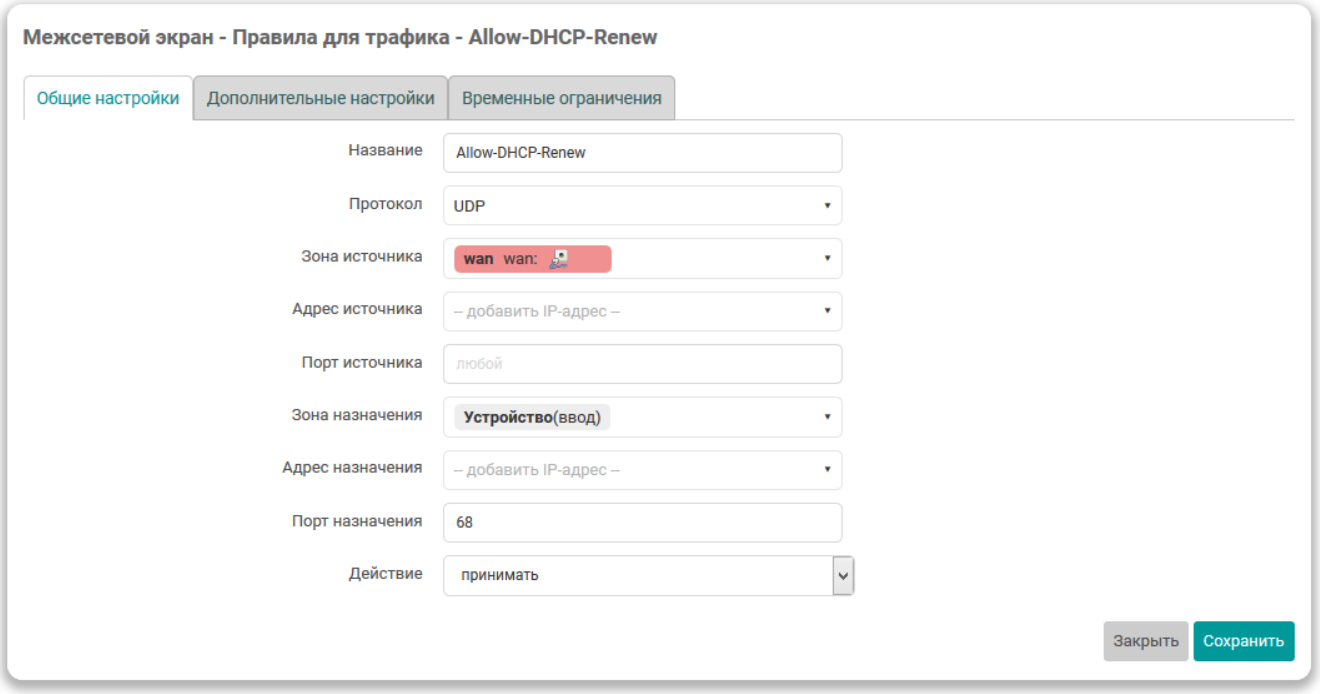


Рис. 7-41: Окно настроек правила для трафика межсетевого экрана

Окно настроек разбито на несколько вкладок:

- «Общие настройки» (см. раздел 7.5.4.2.1);
- «Дополнительные настройки» (см. раздел 7.5.4.2.2);
- «Временные ограничения» (см. раздел 7.5.4.2.3).

7.5.4.2.1 Вкладка «Общие настройки»

Внешний вид вкладки «Общие настройки» показан на рисунке 7-41.

На данной вкладке доступны для редактирования следующие настройки:

- «Имя» — уникальное символьное имя правила.
- «Протокол» — выбор протоколов для правила. Возможен выбор одного или нескольких протоколов из следующего списка:
  - «любой» — любой протокол. При выборе данного варианта, другие протоколы выбрать нельзя;
  - «UDP»;
  - «TCP»;
  - «ICMP»;
  - «IGMP»;
  - «IPSEC-ESP»;
  - пользовательский (произвольное имя протокола).

В зависимости от выбранного протокола набор прочих настроек может несущественно меняться.

- «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.
- «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:
  - «не обрабатывать»;
  - «принимать»;
  - «отвергать»;
  - «не отслеживать»;
  - «назначить помощника отслеживания соединений» — в этом случае появляется дополнительная опция «Помощник отслеживания», в которой необходимо выбрать из списка помощника отслеживания соединений для назначения соответствующему трафику;
  - «применить метку брандмауэра» — в этом случае появляется дополнительная опция «Установить метку», в которой необходимо указать метку, которую требуется установить;
  - «XOR метка брандмауэра» — в этом случае появляется дополнительная опция «XOR метку», в которой необходимо указать значение, с котором будет произведена побитовая операция XOR над существующим значением метки;
  - «DSCP классификация» — в этом случае появляется дополнительная опция «DSCP метка», в которой необходимо выбрать из списка значение требуемой DSCP метки.

7.5.4.2.2 Вкладка «Дополнительные настройки»

Внешний вид вкладки «Дополнительные настройки» показан на рисунке 7-42.

На данной вкладке доступны для редактирования следующие настройки:

- «Соответствие устройству» — настройка позволяет привязать правило к конкретному входящему или исходящему сетевому утсройству. При выборе значения «Входящее устройство» или «Исходящее устройство» появляется дополнительная настройка «Имя устройства», в которой необходимо выбрать конкретное устройство.

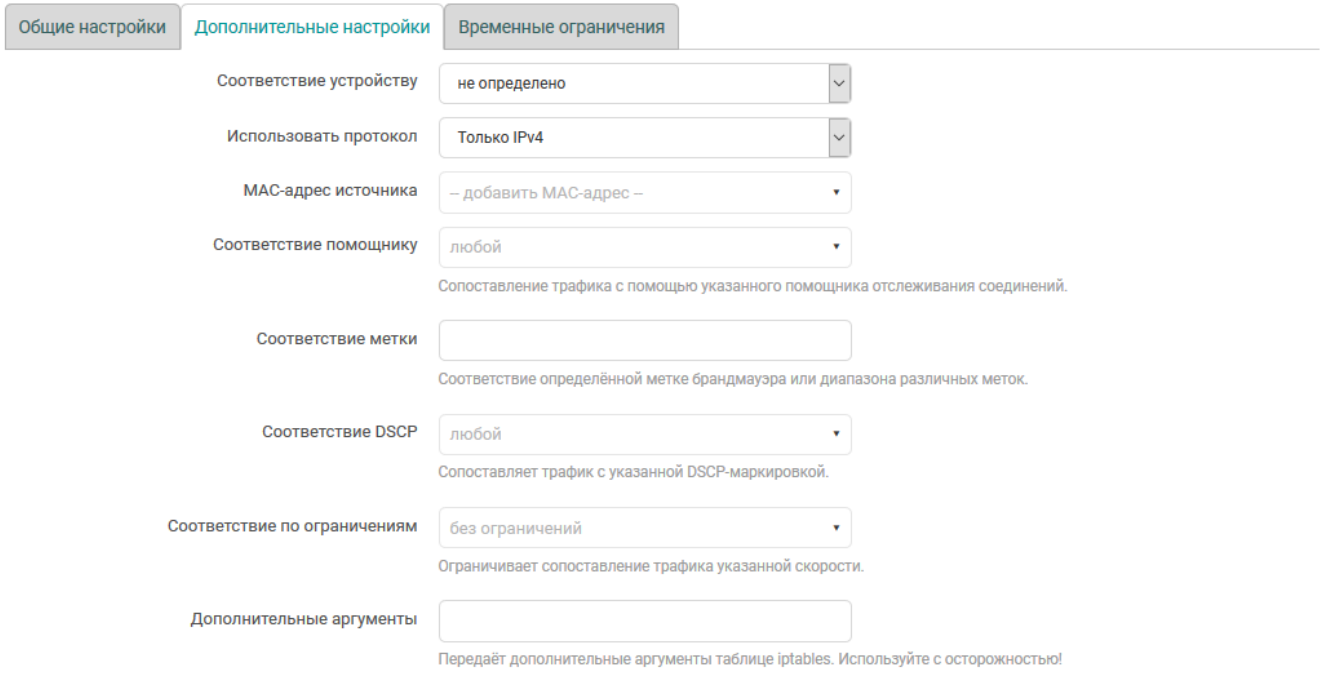


Рис. 7-42: Окно настроек правила для трафика межсетевого экрана. Вкладка «Дополнительные настройки»

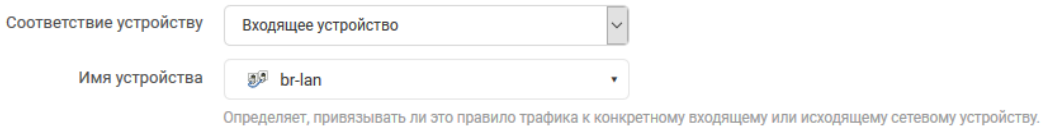


Рис. 7-43: Настройка привязки правила к конкретному сетевому устройству

При выборе значения «не определено» правило не будет привязано к какому либо конкретному сетевому устройству.

- «Использовать протокол» — выбор версий IP-протокола для данного правила. Возможен выбор из вариантов:
  - «только IPv4»;
  - «только IPv6»;
  - «IPv4 и IPv6».
- «Соответствовать ICMP типу» — выбор типов ICMP пакетов, для которых данное правило будет применяться. Настройка доступна только в случае выбора ICMP протокола.
- «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.
- «Соответствие помощнику» — настройка позволяет указать конкретного помощника отслеживания соединений (conntrack).
- «Соответствие метки» — настройка позволяет указать метку или диапазон меток межсетевого экрана для соответствия трафика правила.
- «Соответствие DSCP» — настройка позволяет указать DSCP метку с которой будет производиться сопоставление трафика для правила.
- «Соответствие по ограничениям» — настройка ограничивает сопоставление трафика указанной скорости.
- «Дополнительные аргументы» — позволяет указать дополнительные аргументы для команды iptables.

7.5.4.2.3 Вкладка «Временные органичения»

Внешний вид вкладки «Временные органичения» показан на рисунке 7-44.

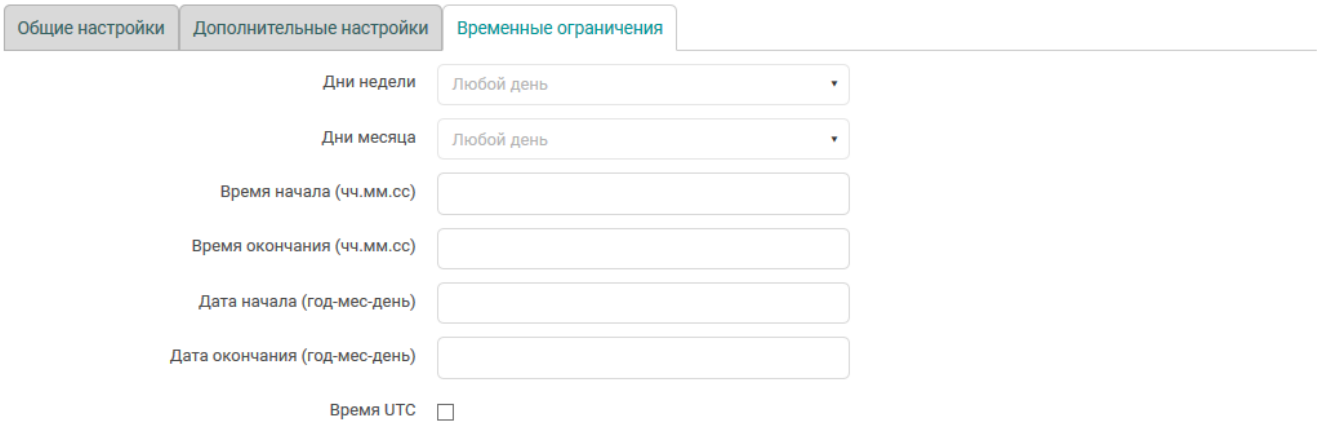


Рис. 7-44: Окно настроек правила для трафика межсетевого экрана. Вкладка «Временные органичения»

На данной вкладке доступны для редактирования следующие настройки:

- «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 предназначена кнопка «Добавить», расположенная снизу таблицы правил для трафика (см. рисунок 7-40). При этом откроется всплывающее окно редактирования параметров правила, как и при изменении (редактировании) существующего правила (см. раздел 7.5.4.2).

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 Правила NAT

Правила NAT позволяют точно контролировать IP-адрес источника в исходящем или перенаправляемом трафике.

Управление правилами NAT межсетевого экрана осуществляется на вкладке «Правила NAT» страницы «Межсетевой экран» (см. рисунок 7-45).

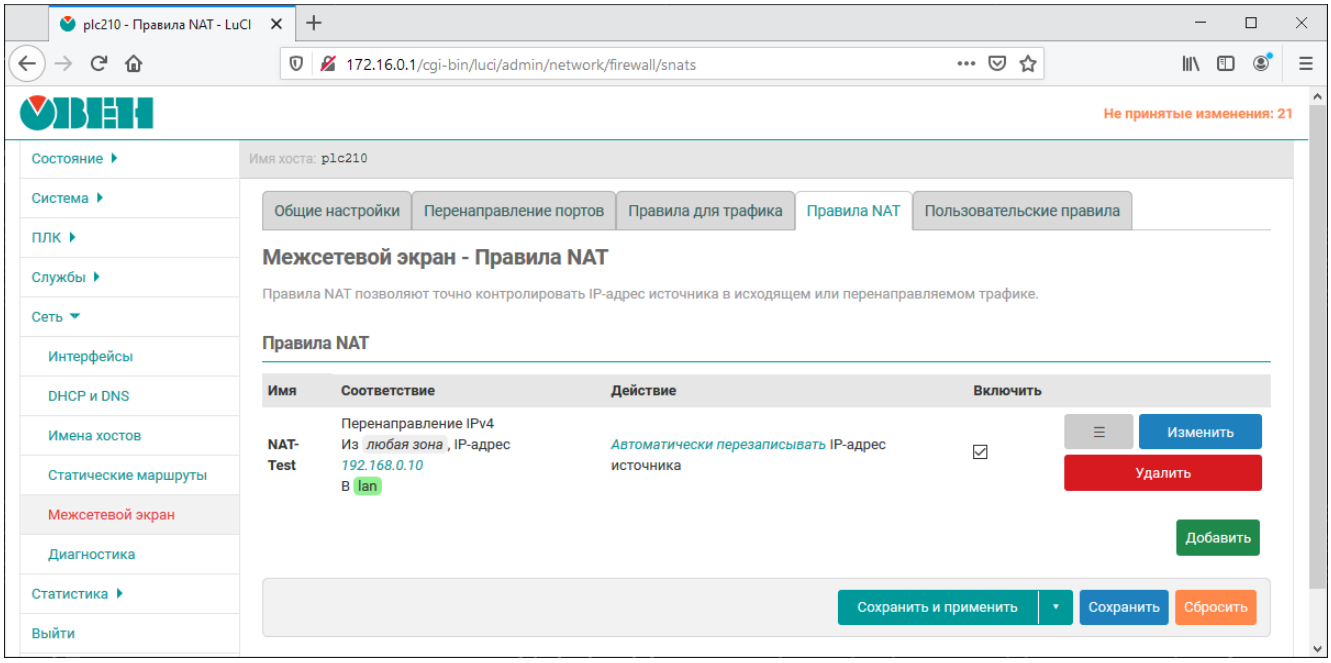


Рис. 7-45: Правила NAT межсетевого экрана

На странице приведена таблица «Правила NAT» с перечислением уже созданных правил NAT. Таблица имеет следующие столбцы:

- «Имя» — уникальное символьное имя правила.
- «Соответствие» — в данном столбце приведены условия для 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 трафику.

7.5.5.1 Порядок применения правил NAT

Правила NAT применяются в том порядке (сверху вниз), в котором они указаны в таблице. Для изменения порядка правил предназначена кнопка «≡» (см. рисунок 7-45), позволяющя переместить соответствующее правило в таблице.

7.5.5.2 Редактирование правил NAT

Для редактирования правила NAT необходимо нажать кнопку «Изменить» (см. рисунок 7-45), расположенную в строке соответствующего правила. При этом откроется всплывающее окно настроек правила NAT, как показано на рисунке 7-46.

Окно настроек разбито на несколько вкладок:

- «Общие настройки» (см. раздел 7.5.5.2.1);
- «Дополнительные настройки» (см. раздел 7.5.5.2.2);
- «Временные ограничения» (см. раздел 7.5.5.2.3).

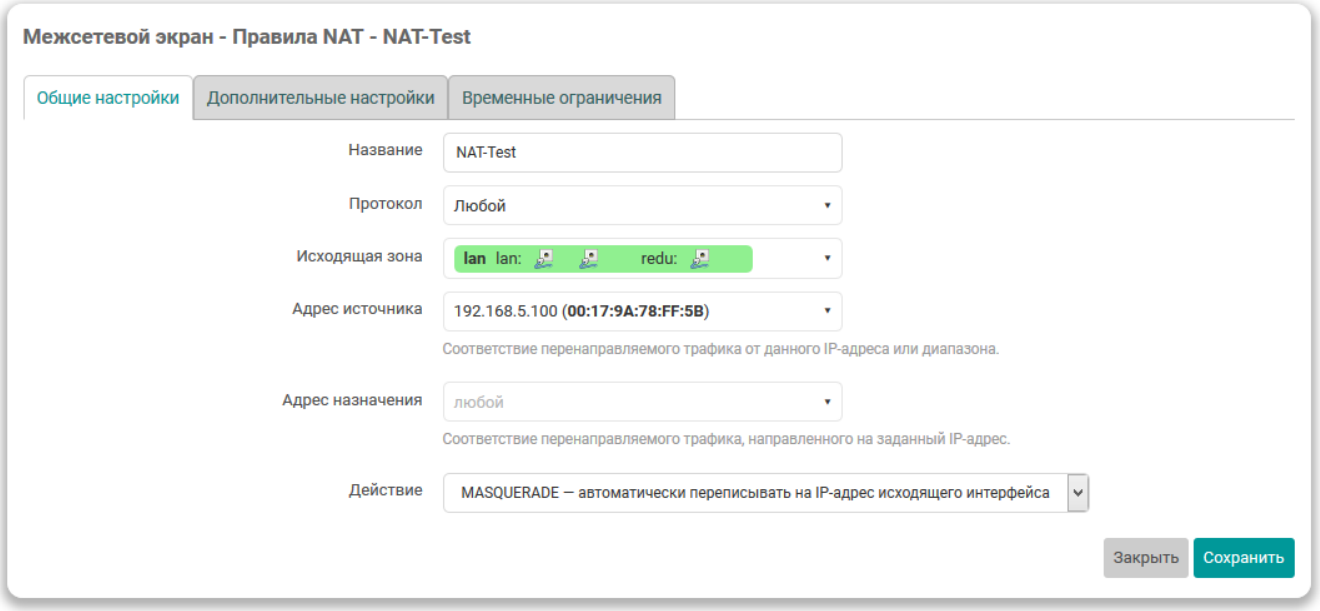


Рис. 7-46: Окно настроек правила NAT межсетевого экрана

7.5.5.2.1 Вкладка «Общие настройки»

Внешний вид вкладки «Общие настройки» настроек правил NAT показан на рисунке 7-46.

На данной вкладке доступны для редактирования следующие настройки:

- «Имя» — уникальное символьное имя правила.
- «Протокол» — выбор протоколов для правила. Возможен выбор одного или нескольких протоколов из следующего списка:
  - «любой» — любой протокол. При выборе данного варианта, другие протоколы выбрать нельзя;
  - «UDP»;
  - «TCP»;
  - «ICMP»;
  - пользовательский (произвольное имя протокола).

  В зависимости от выбранного протокола набор прочих настроек может несущественно меняться.
- «Исходящая зона» — выбор исходящей зоны для трафика правила.
- «Адрес источника» — указание соответствия адреса источника перенаправляемого трафика.
- «Адрес назначения» — указание соответствия адреса назначения перенаправляемого трафика.
- «Действие» — выбор действия, применяемого для трафика данного правила. Возможен выбор из вариантов:
  - «SNAT» — перезапись IP-адреса источника на указанный. При выборе данного действия появляется дополнительная настройка «IP-адрес для перезаписи», где необходимо указать перезаписываемое значение IP-адреса источника;
  - «MASQUERADE» — автоматическая перезапись IP-адреса источника на IP-адрес исходящего интерфейса;
  - «ACCEPT» — отключить перезапись IP-адреса источника.

7.5.5.2.2 Вкладка «Дополнительные настройки»

Внешний вид вкладки «Дополнительные настройки» показан на рисунке 7-47.

На данной вкладке доступны для редактирования следующие настройки:

- «Исходящее устройство» — настройка позволяет привязать правило к конкретному исходящему сетевому утсройству. При выборе значения «не определено» правило не будет привязано к какому либо конкретному сетевому устройству.

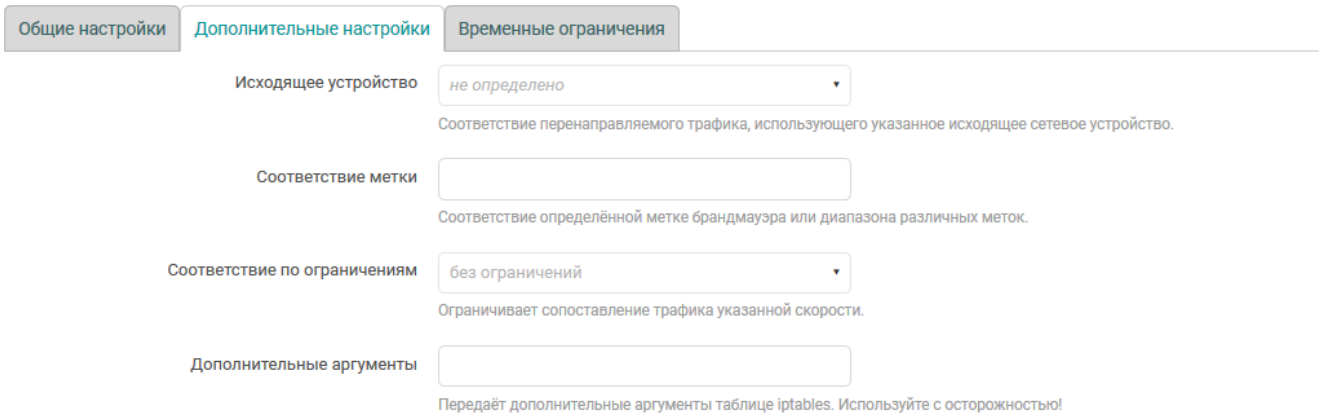


Рис. 7-47: Окно настроек правила NAT межсетевого экрана. Вкладка «Дополнительные настройки»

- «Соответствие метки» — настройка позволяет указать метку или диапазон меток межсетевого экрана для соответствия трафика правила.
- «Соответствие по ограничениям» — настройка ограничивает сопоставление трафика указанной скорости.
- «Дополнительные аргументы» — позволяет указать дополнительные аргументы для команды iptables.

7.5.5.2.3 Вкладка «Временные органичения»

Внешний вид вкладки «Временные органичения» показан на рисунке 7-48.

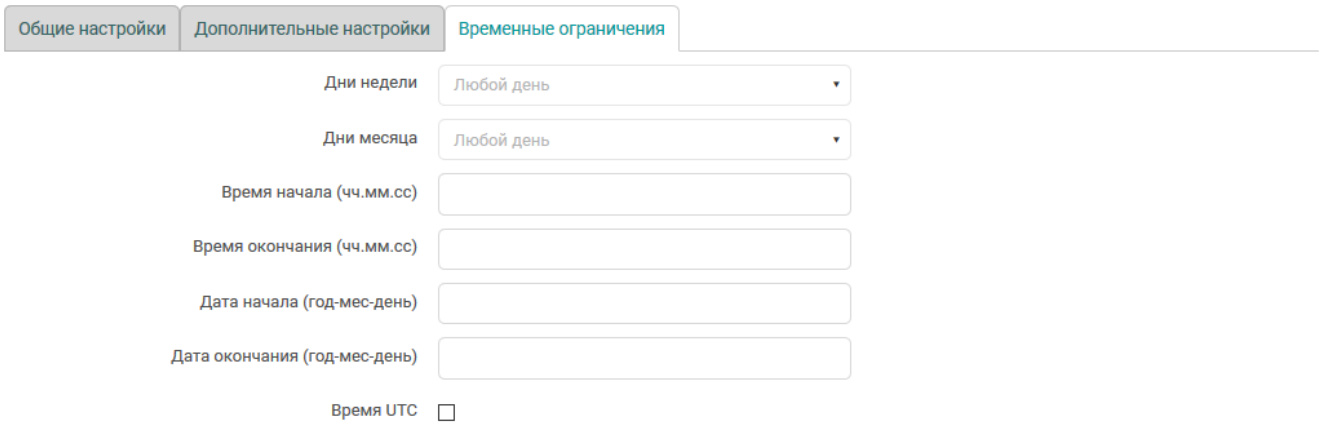


Рис. 7-48: Окно настроек правила NAT межсетевого экрана. Вкладка «Временные органичения»

На данной вкладке доступны для редактирования следующие настройки:

- «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.

7.5.5.3 Добавление правил NAT

Для добавления нового правила NAT предназначена кнопка «Добавить», расположенная снизу таблицы правил для трафика (см. рисунок 7-45). При этом откроется всплывающее окно редактирования параметров правила, как и при изменении (редактировании) существующего правила (см. раздел 7.5.5.2).

7.5.5.4 Удаление правил NAT

Для удаления правила NAT предназначена кнопка «Удалить» (см. рисунок 7-45), расположенная в строке соответствующего правила.

7.5.6 Пользовательские правила

На вкладке «Пользовательские правила» настроек межсетевого экрана (см. рисунок 7-49) 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.

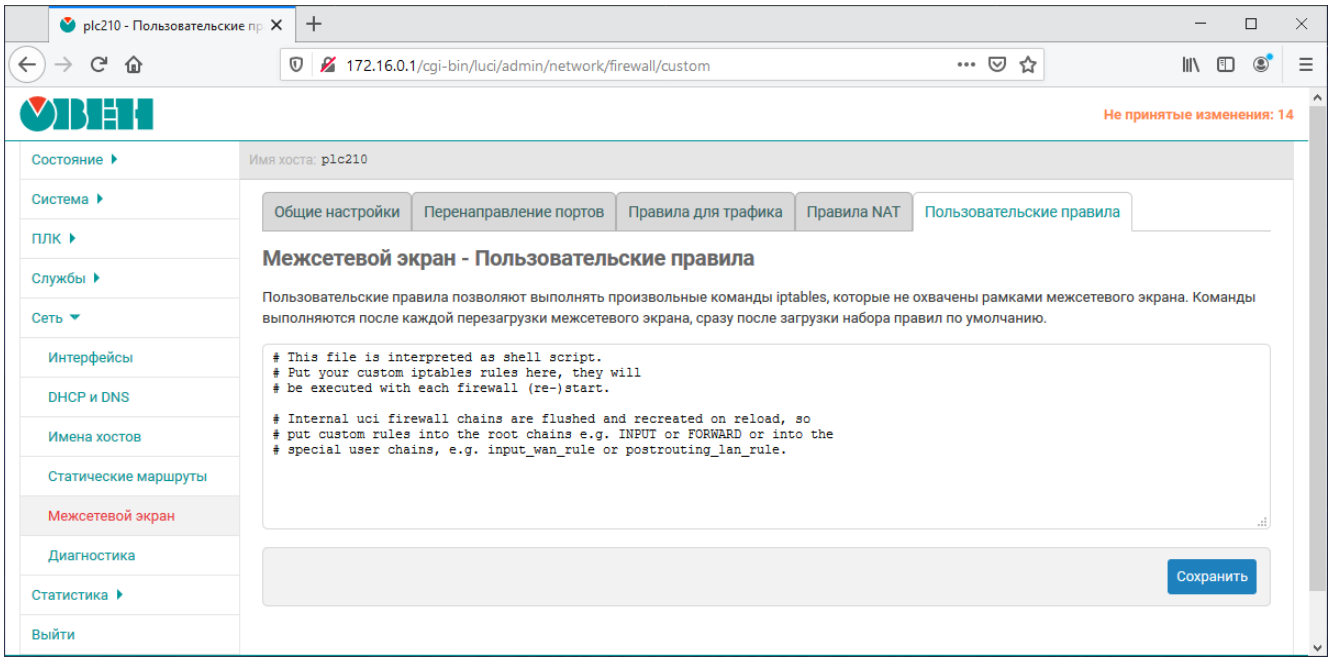


Рис. 7-49: Пользовательские правила межсетевого экрана

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 IP-адрес» (см. раздел 7.6.4) — определение внешнего IP-адреса.

Внешний вид страницы «Диагностика» показан на рисунке 7-50.

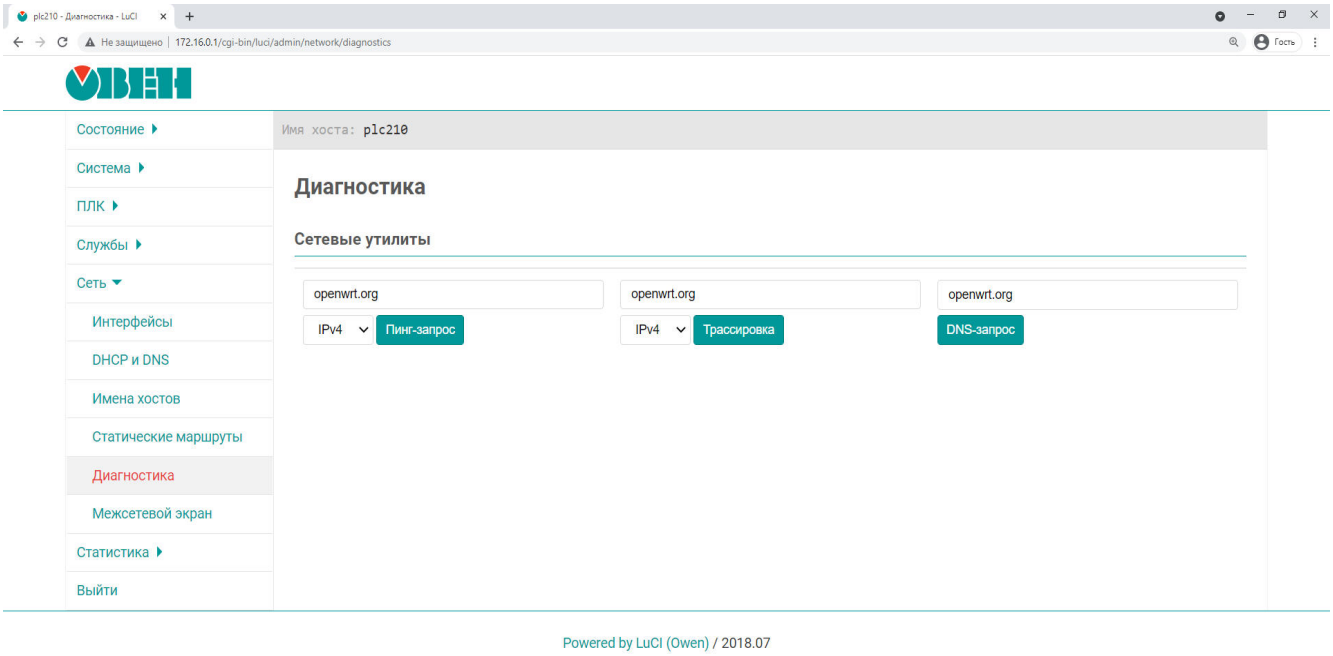


Рис. 7-50: Страница «Диагностика»

При выполнении какой-либо из диагностик, результат будет выведен в текстовом виде, как показано на рисунке 7-51.

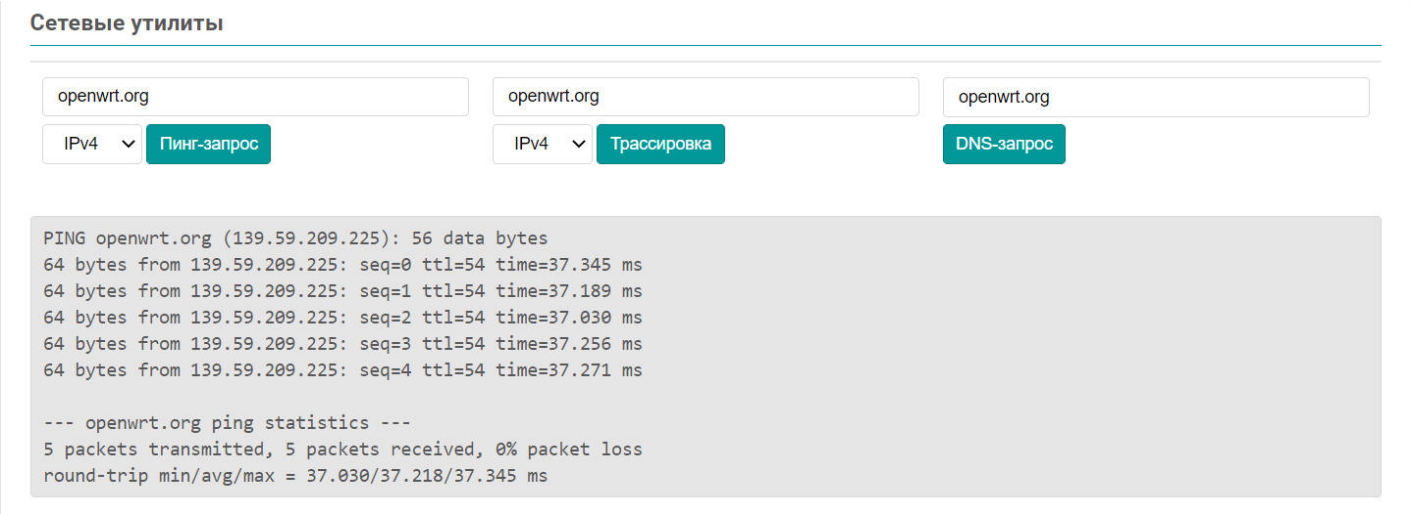


Рис. 7-51: Страница «Диагностика». Пример вывода результата диагностики пинг-запроса

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 openwrt.org (139.59.209.225): 56 data bytes
64 bytes from 139.59.209.225: seq=0 ttl=54 time=37.345 ms
64 bytes from 139.59.209.225: seq=1 ttl=54 time=37.189 ms
64 bytes from 139.59.209.225: seq=2 ttl=54 time=37.030 ms
64 bytes from 139.59.209.225: seq=3 ttl=54 time=37.256 ms
64 bytes from 139.59.209.225: seq=4 ttl=54 time=37.271 ms

--- openwrt.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 37.030/37.218/37.345 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 openwrt.org (139.59.209.225), 30 hops max, 38 byte packets
1  10.2.1.1  3.788 ms
2  10.1.0.126  0.532 ms
3  *
4  172.31.2.133  3.368 ms
5  93.159.234.145  0.813 ms
6  172.31.101.33  0.051 ms
7  185.36.61.55  3.750 ms
8  31.28.19.100  44.064 ms
9  *
```

```
10  *
11  *
12  *
13  *
14  139.59.209.225  60.014 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:      openwrt.org
Address 1: 139.59.209.225
Address 2: 2a03:b0c0:3:d0::1af1:1
```

7.6.4 Определение внешнего IP-адреса

Данная команда выполняет определение внешнего IP-адреса с использованием сервиса ifconfig.me[1]. В случае успешного определения, будет выведен текущий внешний IP-адрес.

[1] https://ifconfig.me/

8 Статистика

В разделе главного меню «Статистика» содержатся страницы управления и просмотра графиков статистики, полученных при помощи службы collectd [24].

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.

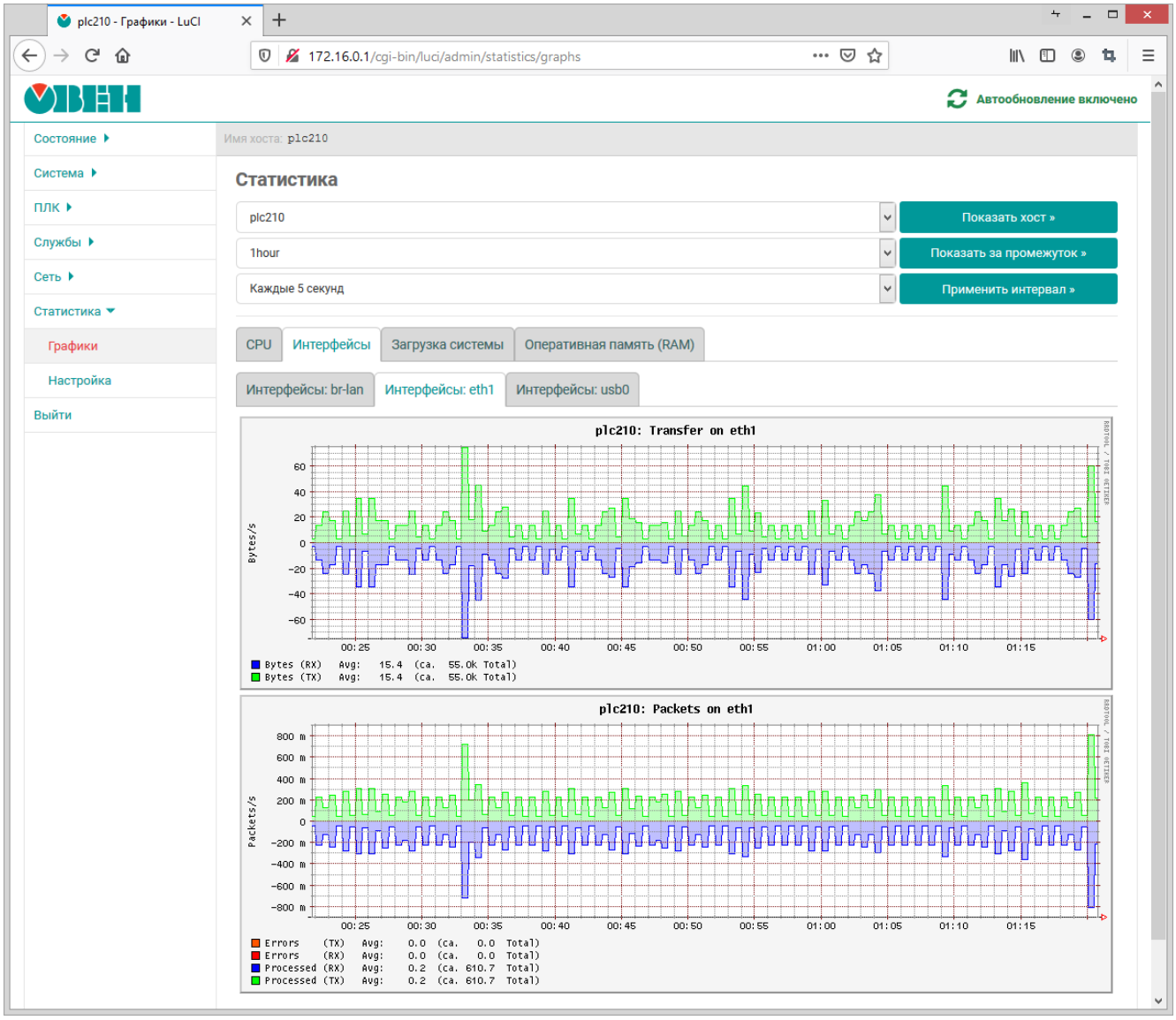


Рис. 8-1: Страница просмотра графиков статистики

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).

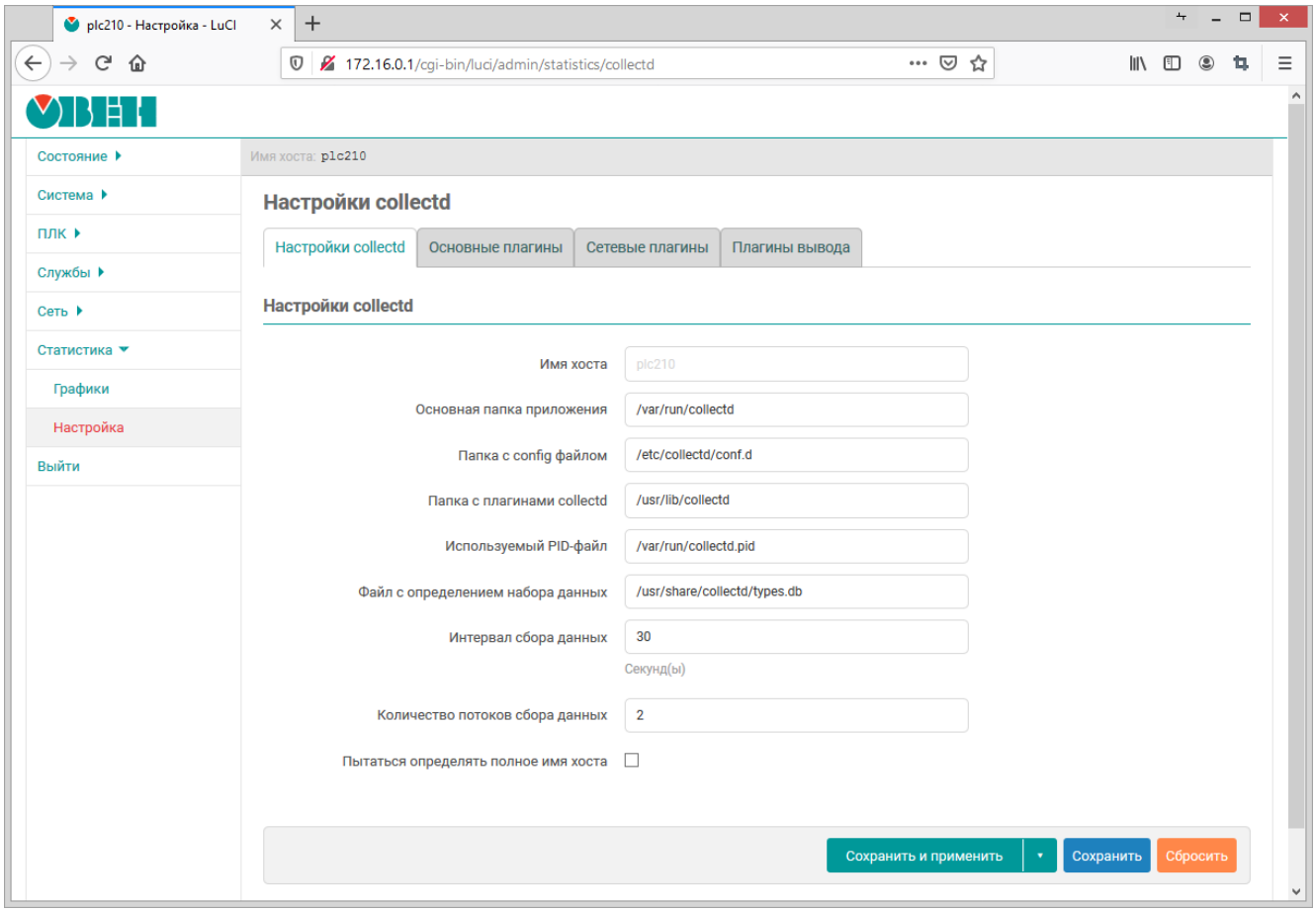


Рис. 8-2: Настройки сбора и отображения статистики

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 [25];
- «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».

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.

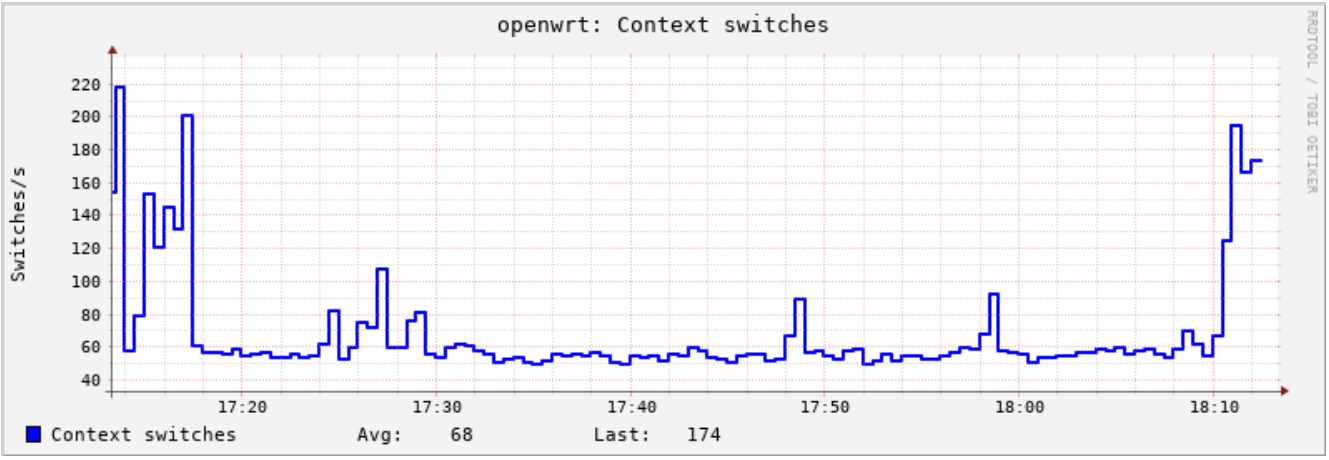


Рис. 8-3: Статистика. График переключений контекста процессора

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.

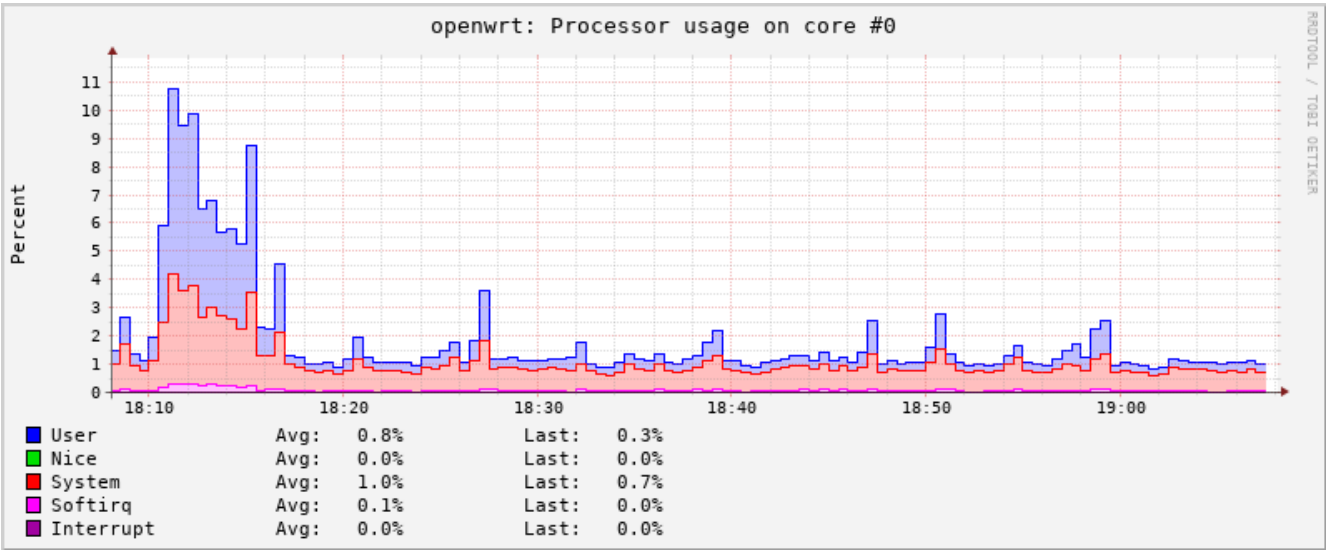


Рис. 8-4: Статистика. График использования процессора

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.

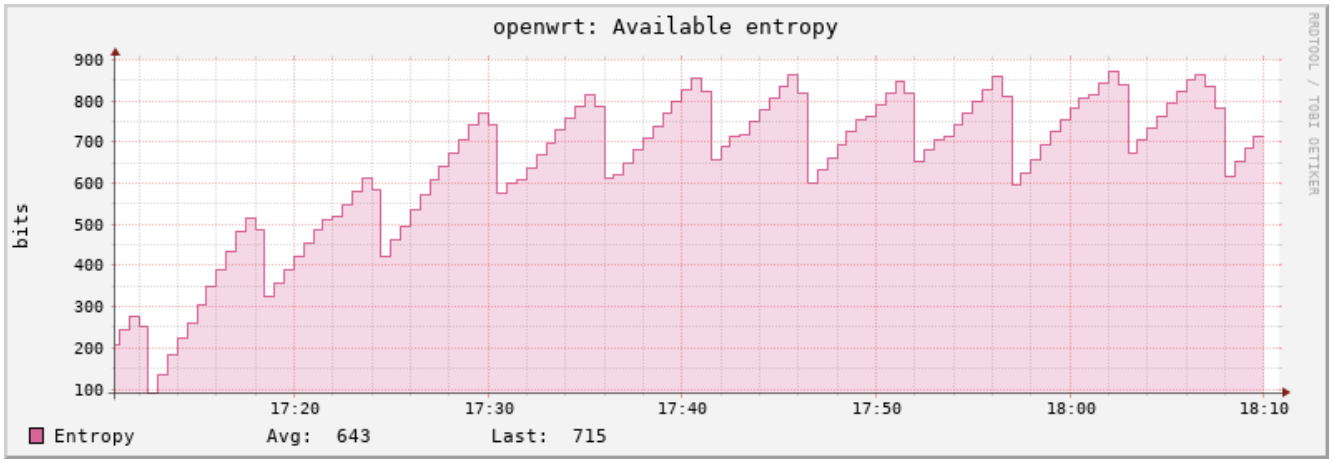


Рис. 8-5: Статистика. График доступной энтропии

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.

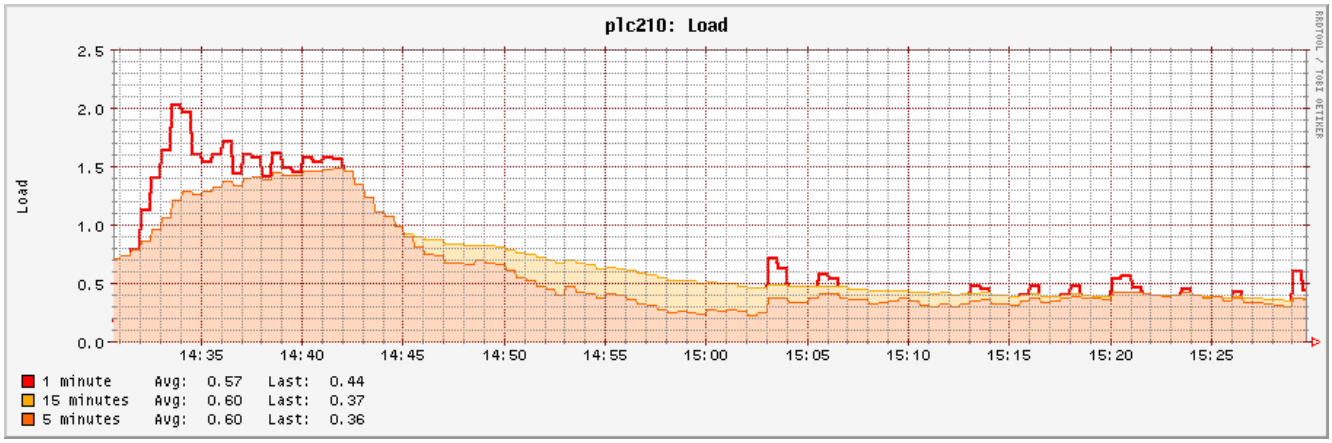


Рис. 8-6: Статистика. График средней загрузки системы

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.

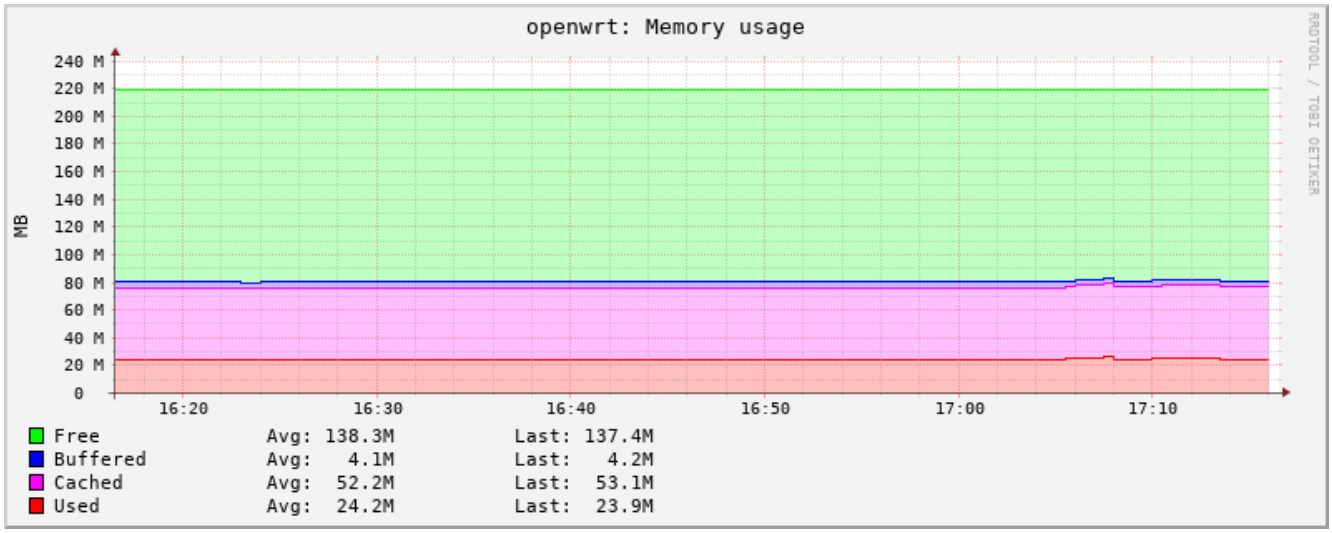


Рис. 8-7: Статистика. График использования оперативной памяти

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.

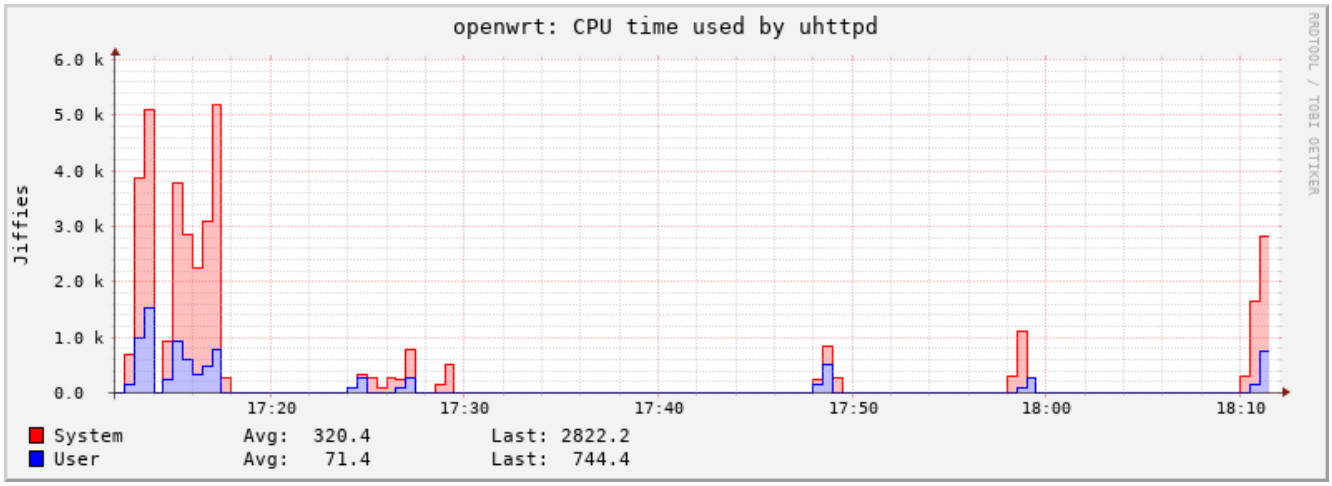


Рис. 8-8: Статистика. График времени CPU для процесса

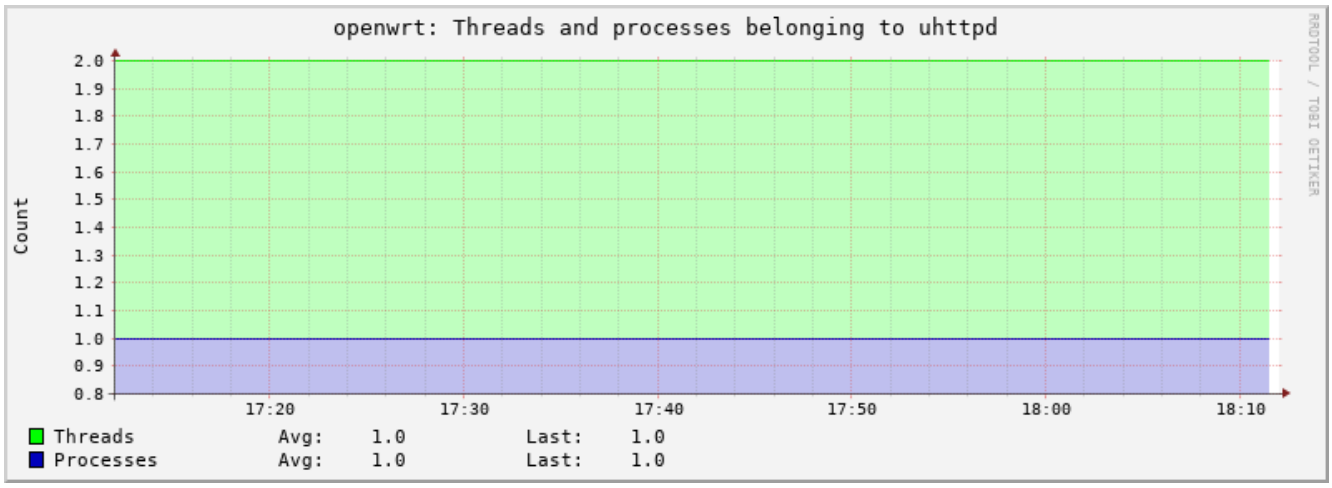


Рис. 8-9: Статистика. График потоков процесса

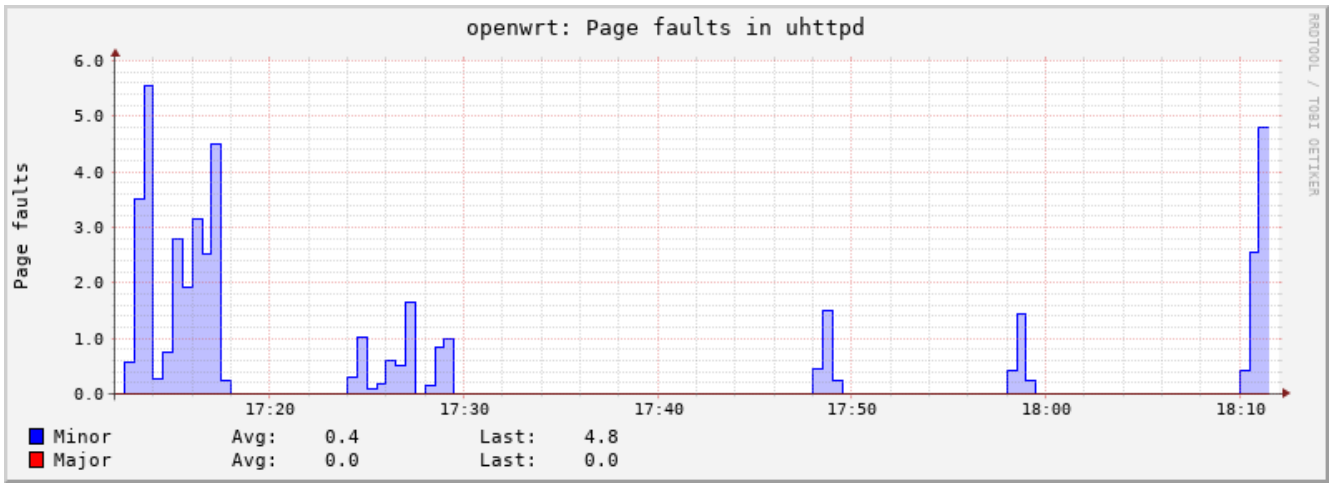


Рис. 8-10: Статистика. График ошибок страниц процесса

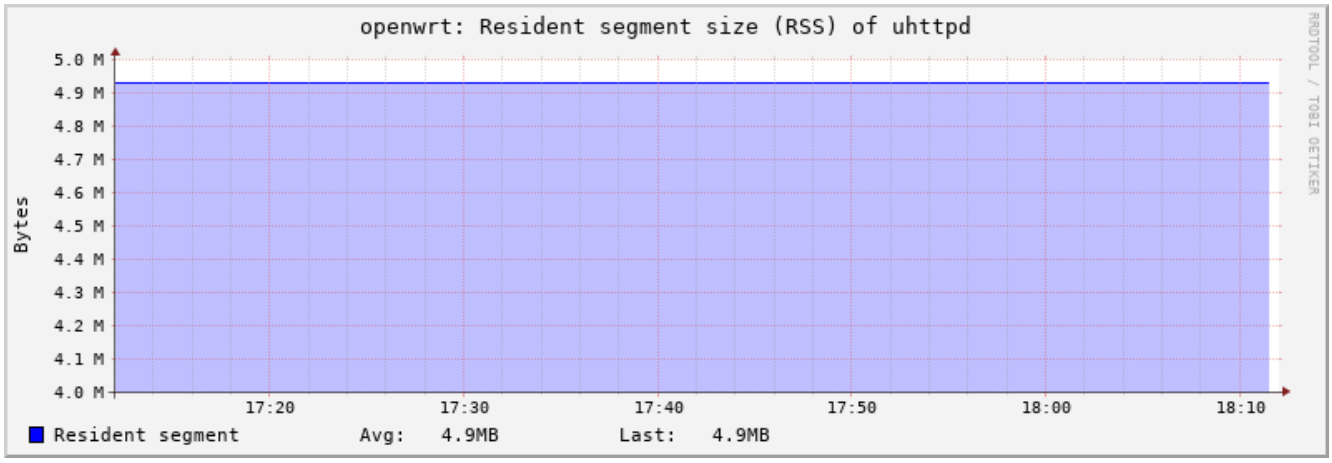


Рис. 8-11: Статистика. График RSS процесса

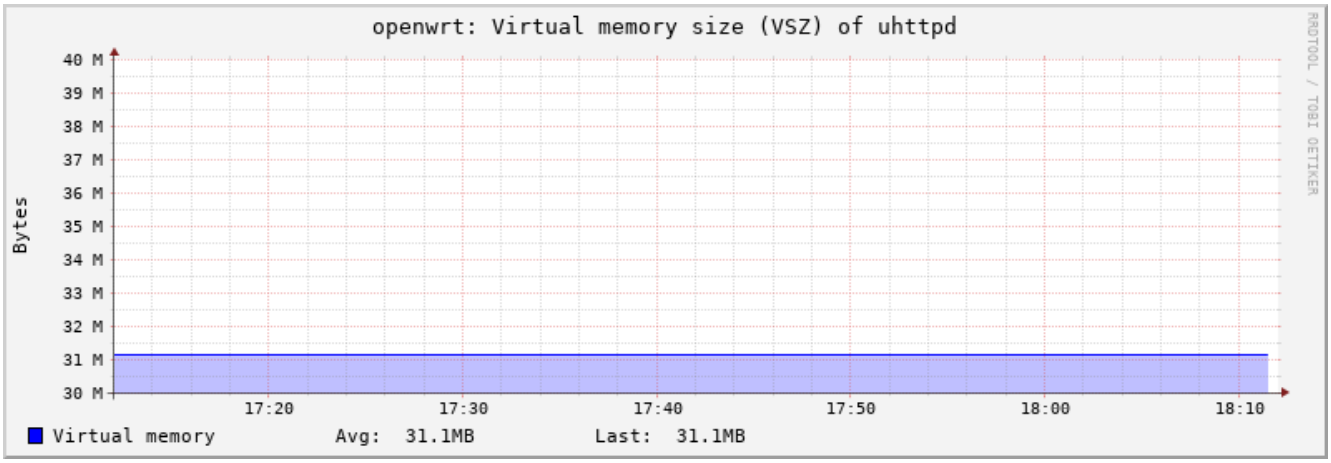


Рис. 8-12: Статистика. График VSZ процесса

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.

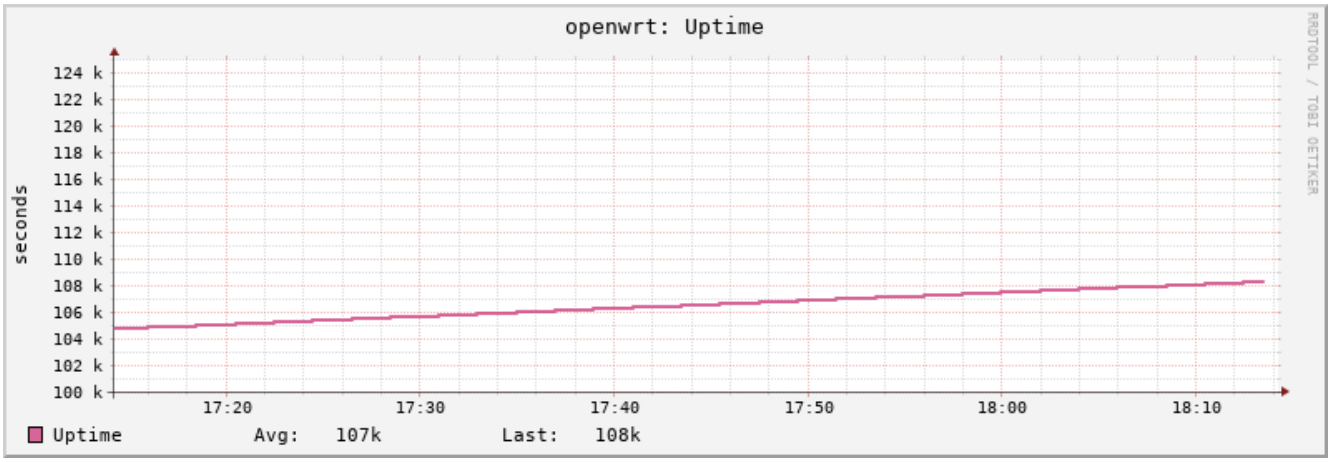


Рис. 8-13: Статистика. График времени работы

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.

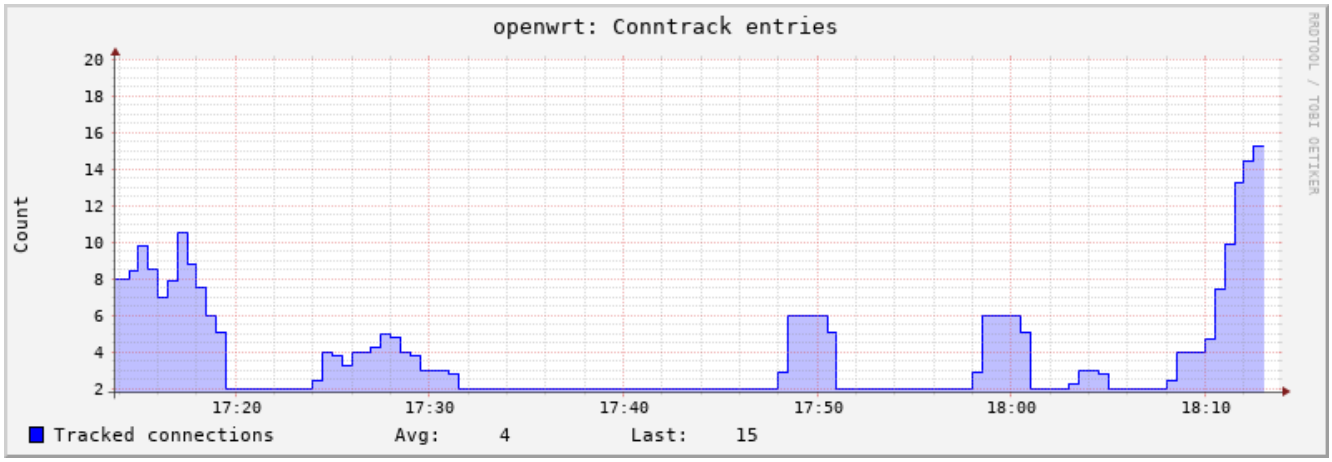


Рис. 8-14: Статистика. График отслеживаемых подключений (conntrack)

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.

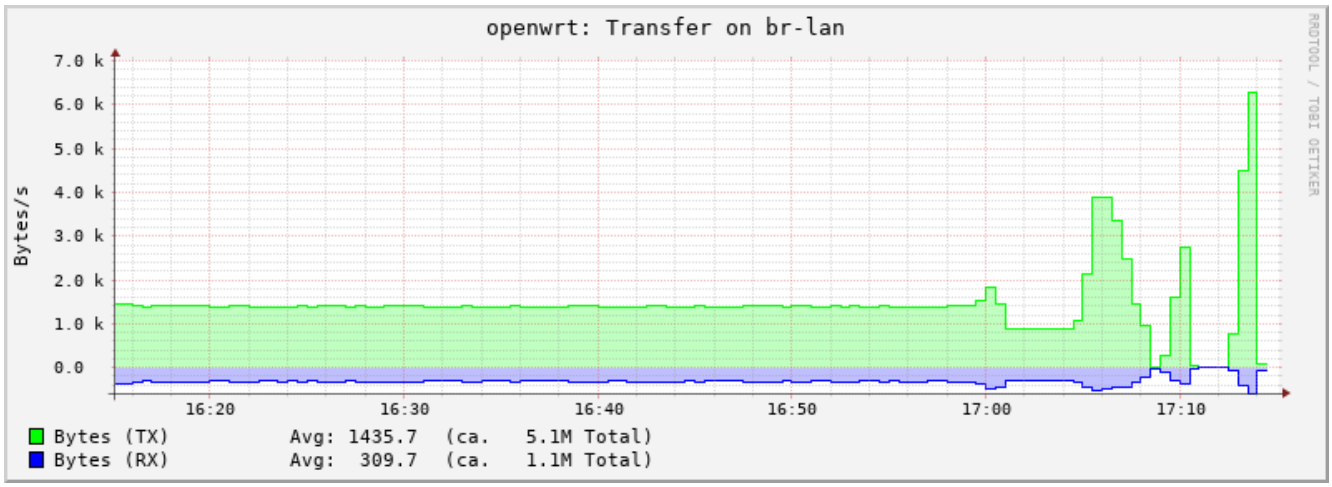


Рис. 8-15: Статистика. График приёма и отправки данных через сетевой интерфейс (байт/с)

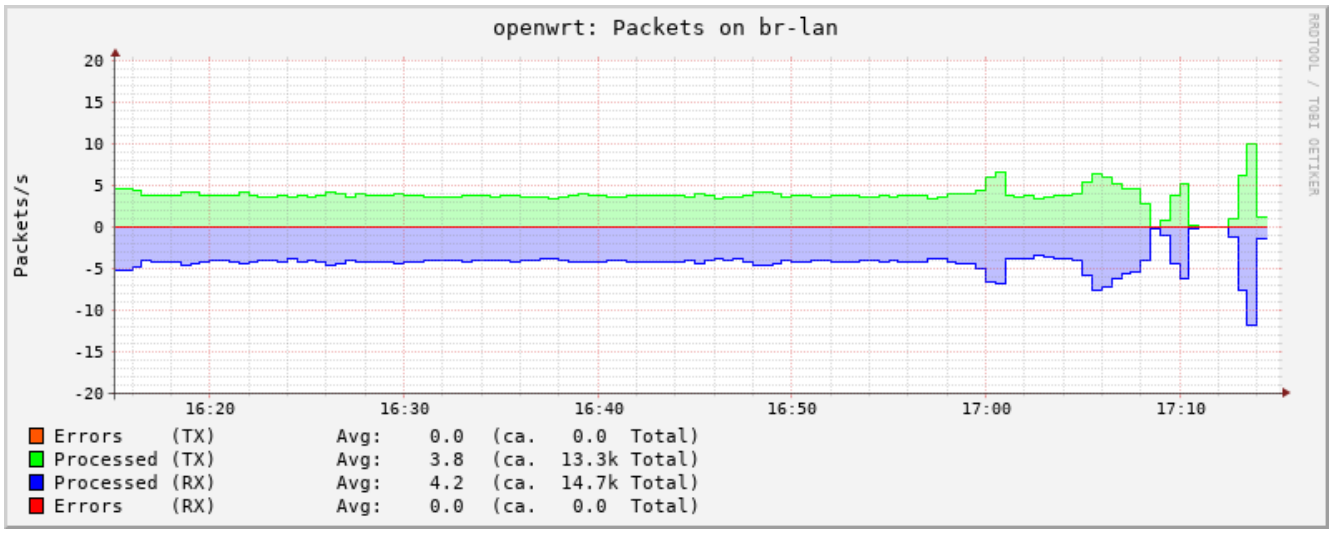


Рис. 8-16: Статистика. График приёма и отправки данных через сетевой интерфейс (пакетов/с)

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.

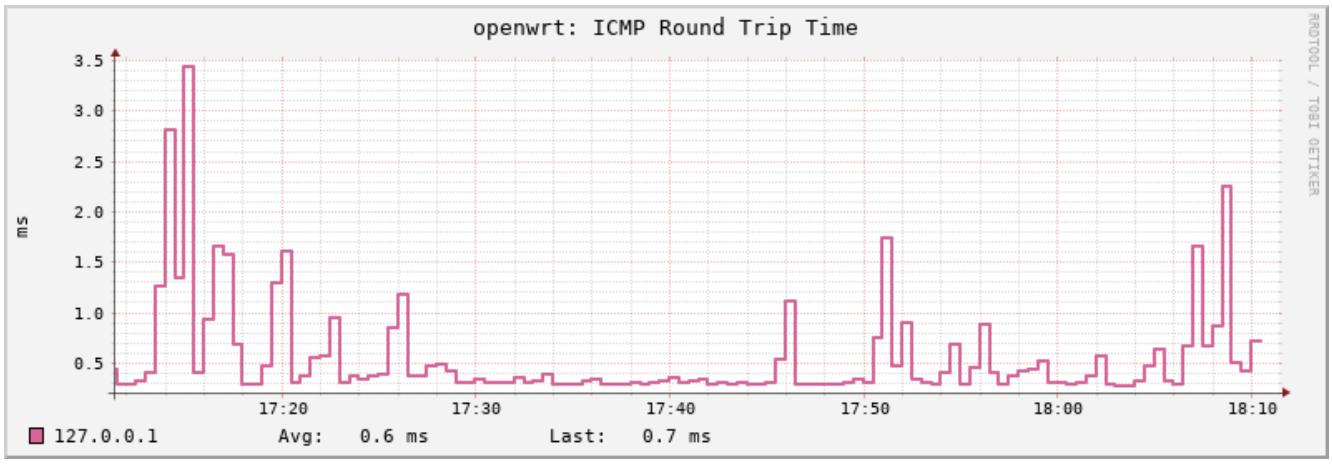


Рис. 8-17: Статистика. График времени отклика ICMP-запроса

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.

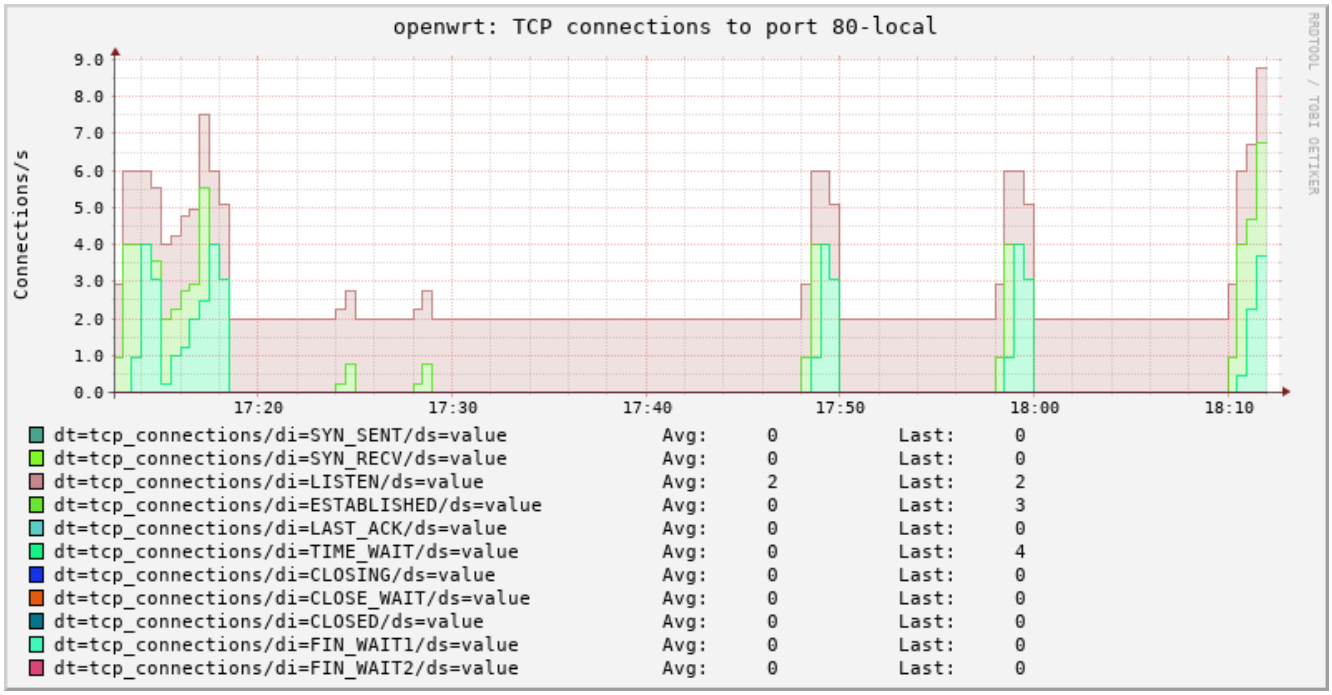


Рис. 8-18: Статистика. График открытых соединений для TCP порта

Приложение А Проверка доступа к консоли устройства ПЛК210 по протоколу SSH

Проверка доступа будет осуществляться с инструментального компьютера с установленной операционной системой Ubuntu 18.04.4 LTS при помощи утилит ssh, scp и sftp пакета OpenSSH версии 7.6.

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 18.04.4 LTS
Release:        18.04
Codename:       bionic
```

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

```
openssh-client:
  Installed: 1:7.6p1-4ubuntu0.3
  Candidate: 1:7.6p1-4ubuntu0.3
  Version table:
 *** 1:7.6p1-4ubuntu0.3 500
        500 http://ru.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages
        500 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages
        100 /var/lib/dpkg/status
     1:7.6p1-4 500
        500 http://ru.archive.ubuntu.com/ubuntu bionic/main amd64 Packages
```

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

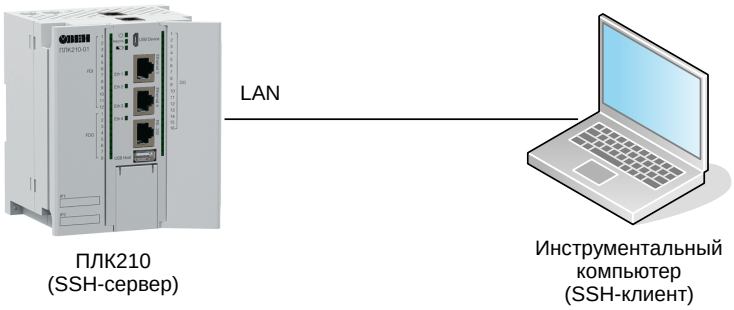


Рис. А-1: Схема подключения проверки доступа к консоли устройства ПЛК210 по протоколу SSH

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 А-2.

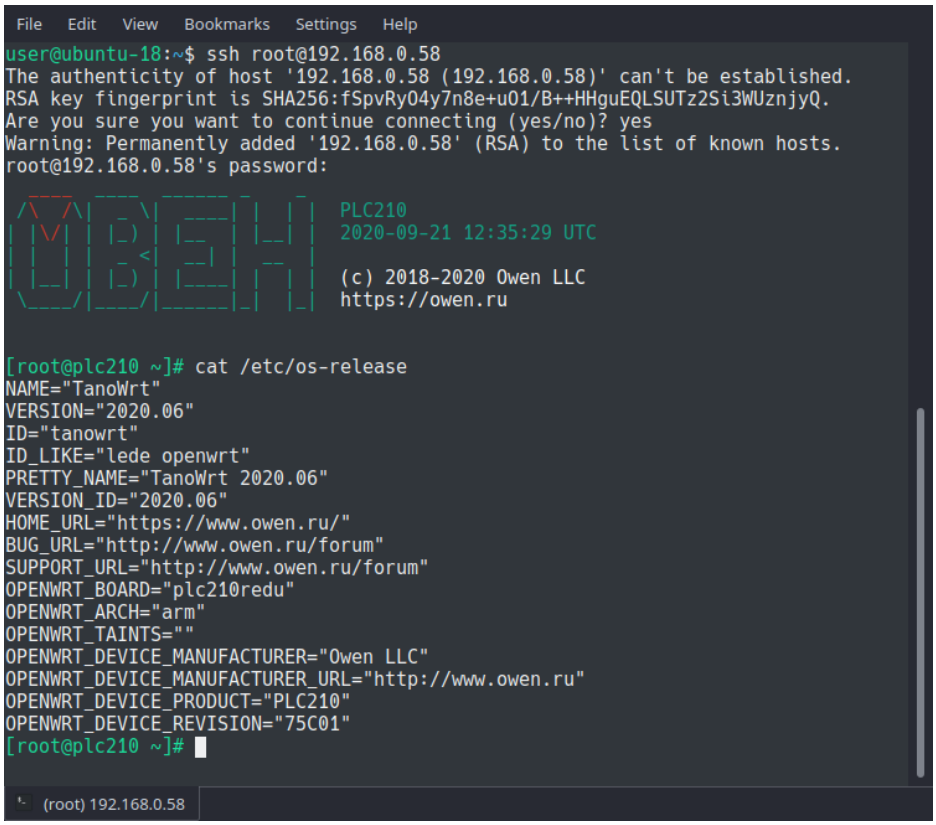


Рис. А-2: Доступ к консоли устройства ПЛК210 при помощи утилиты ssh

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 А-2.

А.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 A-3.

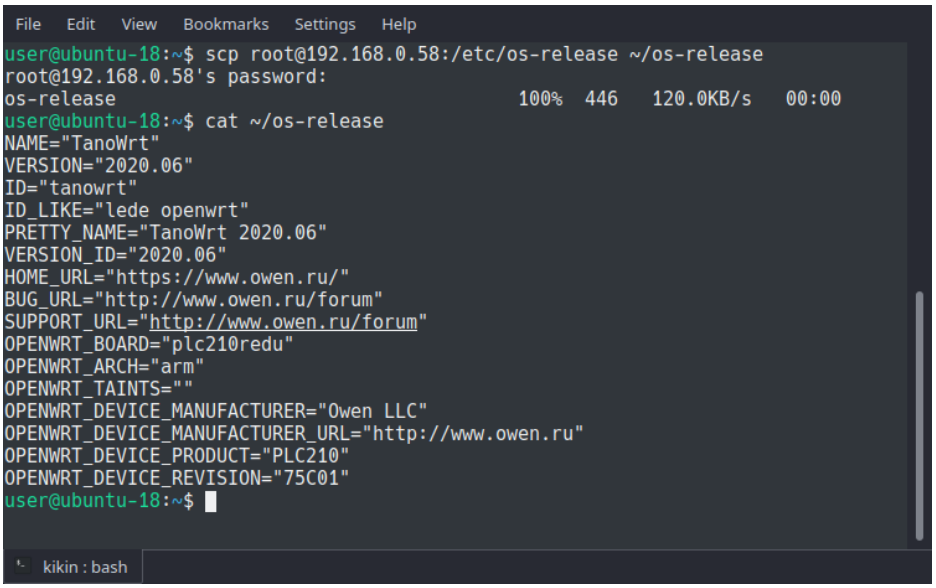


Рис. A-3: Доступ к файловой системе устройства ПЛК210 при помощи утилиты scp

A.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 A-4.

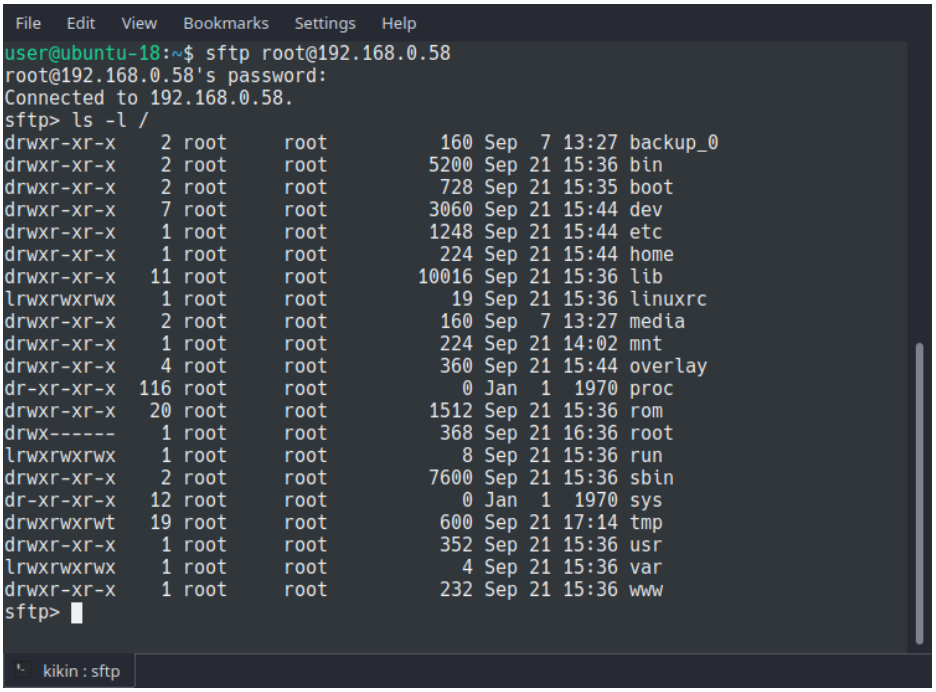


Рис. А-4: Доступ к файловой системе устройства ПЛК210 при помощи утилиты sftp

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.

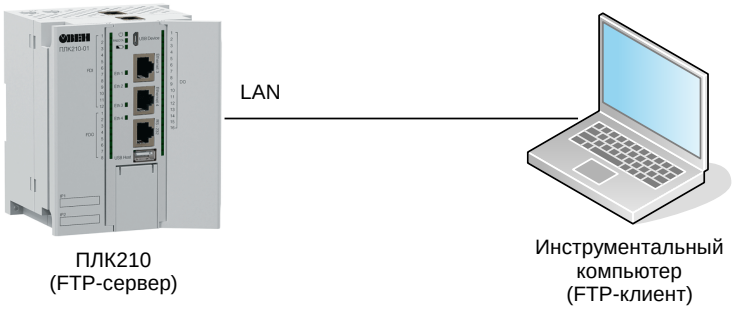


Рис. Б-1: Схема подключения проверки доступа к содержимому FTP-сервера устройства ПЛК210

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 2.9), 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 В-1).

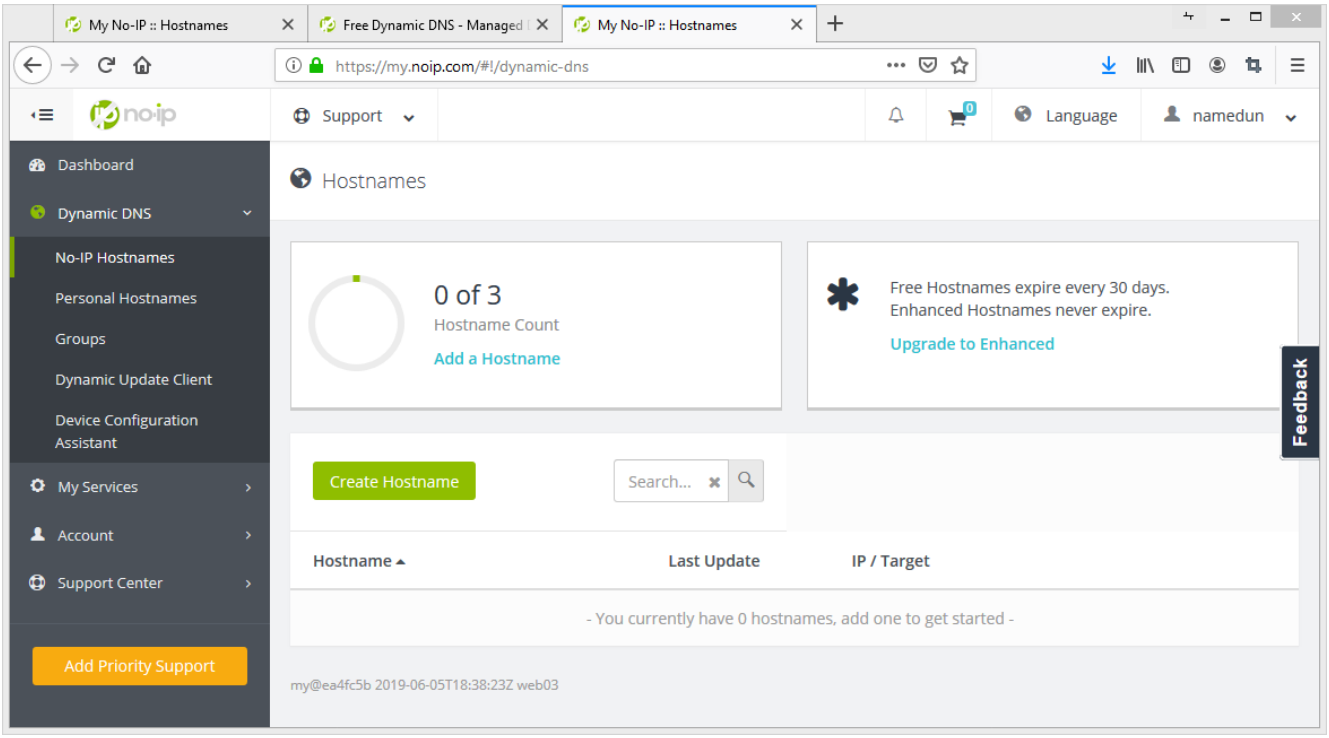


Рис. В-1: Раздел «Dynamic DNS» панели управления DDNS провайдера no-ip.com

B.1.3 Нажмите кнопку «Create Hostname». В открывшемся окне (см. рисунок В-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 В-3.

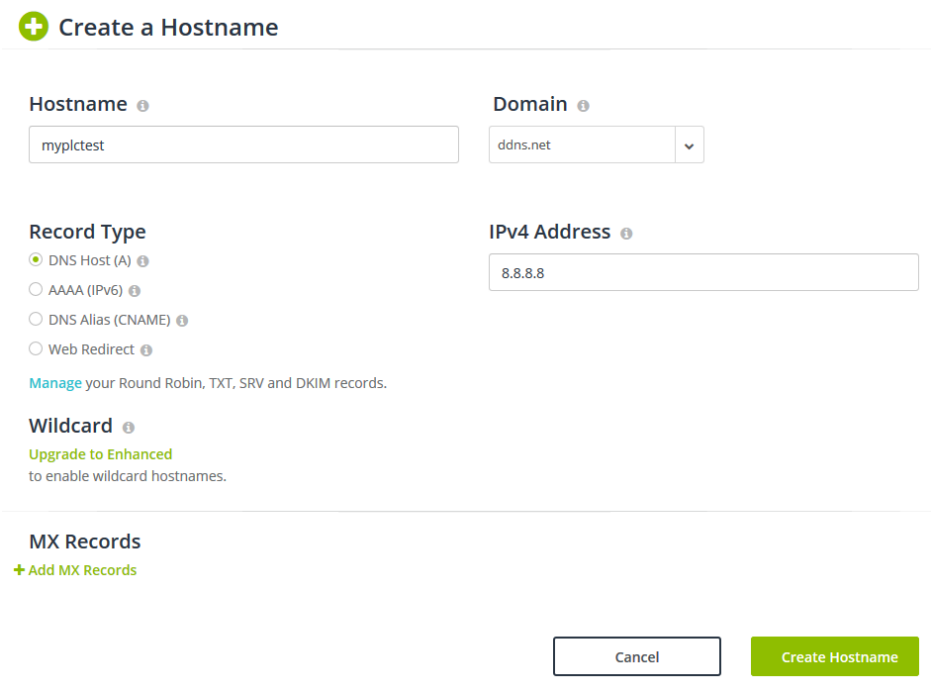


Рис. B-2: Создание Hostname в панели управления DDNS провайдера no-ip.com

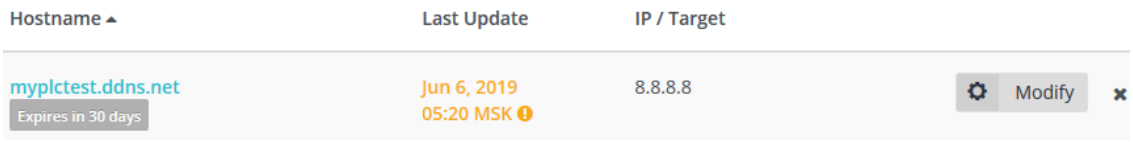


Рис. B-3: Таблица «Hostnames» в панели управления DDNS провайдера no-ip.com

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» нажмите кнопку «Добавить новую службу...» в подразделе «Службы». В открывшемся всплывающем окне в поле «Имя» введите произвольное имя новой DDNS службы (в данном примере «myplctest») и нажмите кнопку «Создать службу» (см. рисунок B-4).

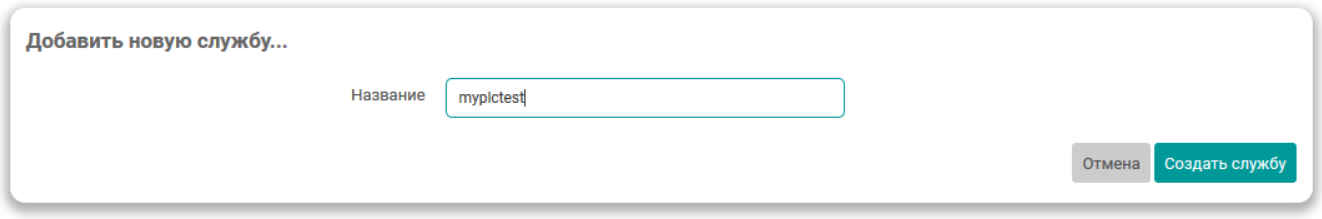


Рис. B-4: Добавление новой DDNS записи

B.2.4 В открывшемся окне редактирования настроек новой DDNS службы, на вкладке «Основные настройки» установите следующие настройки (см. рисунок B-5):

- «Включено» — да;
- «Провайдер службы DDNS» — no-ip.com;
- «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/ca-certificates.crt.

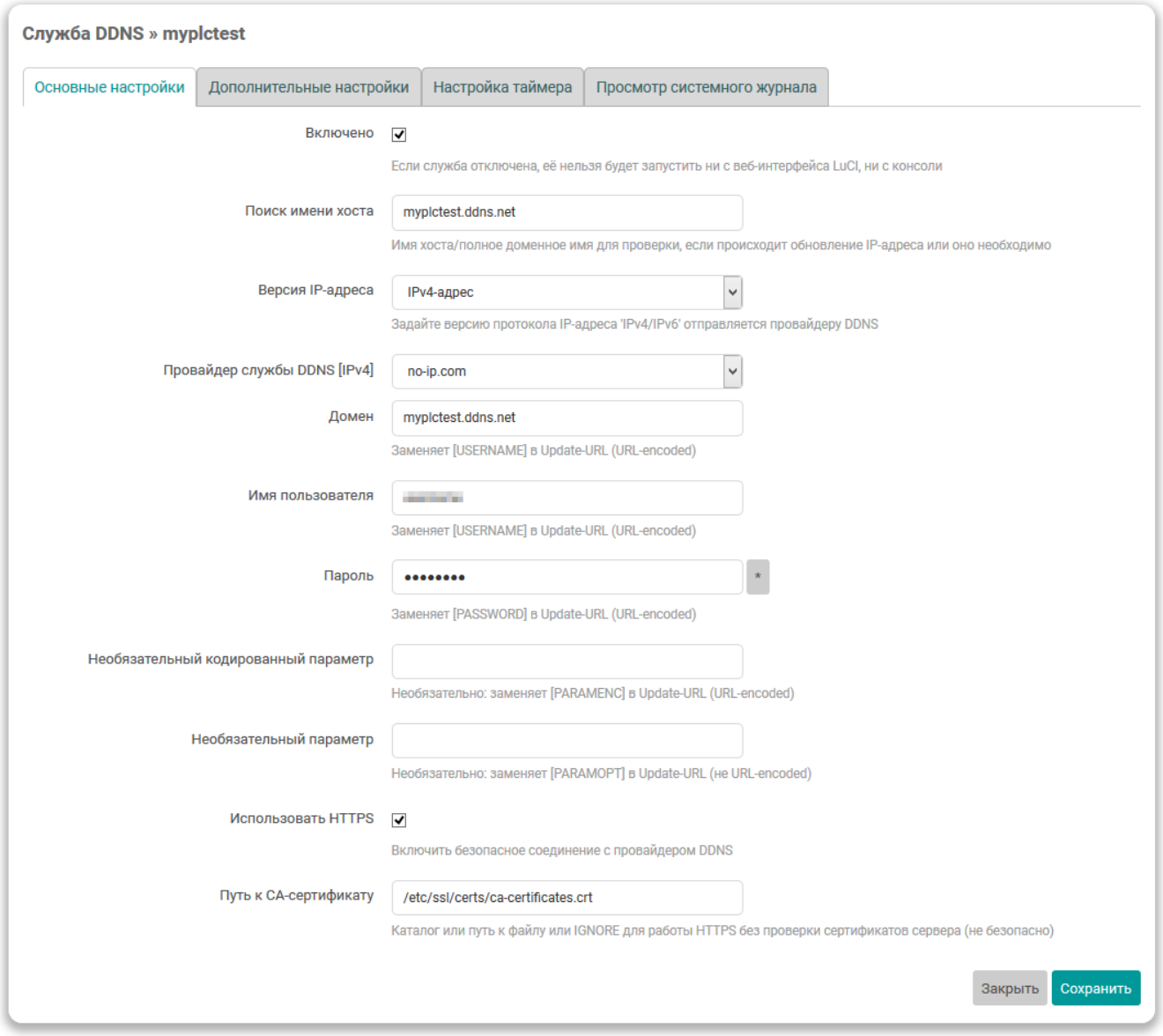


Рис. B-5: Основные настройки новой DDNS записи

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.

B.2.6 Нажмите кнопку «Сохранить». На основной странице «DDNS» в таблице DDNS записей (подраздел «Службы») должна отображаться строка с новой DDNS службой, как показано на рисунке B-6.

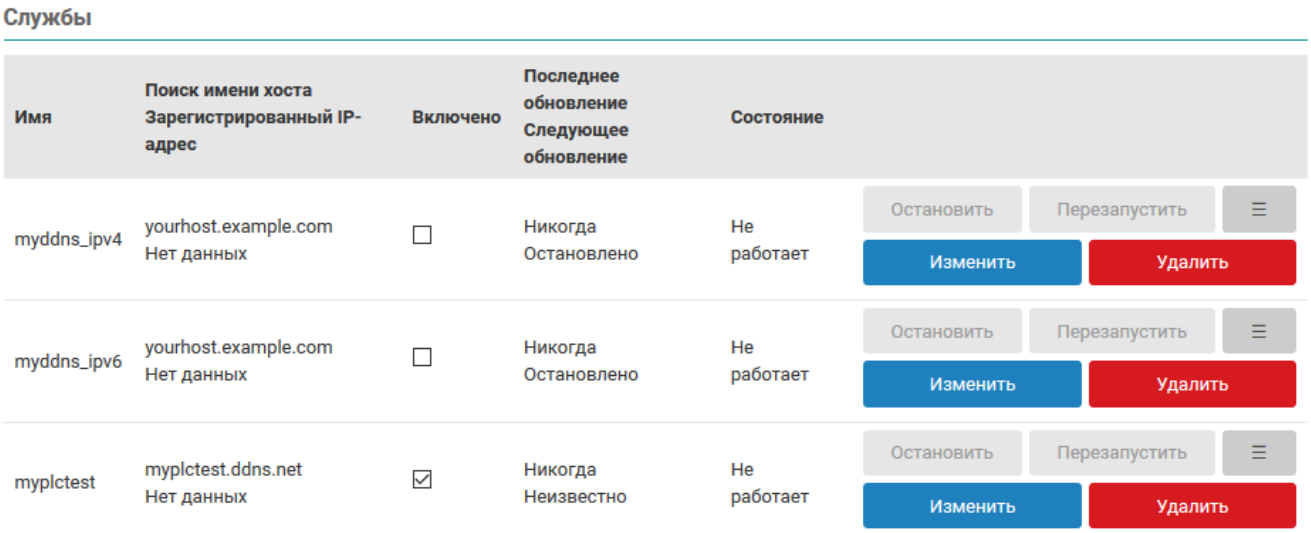


Рис. В-6: Созданная DDNS служба

В.2.7 Нажмите кнопку «Сохранить и применить» (в нижней части страницы) и подождите некоторое время (от 1 до 5 минут). Строка DDNS службы в таблице должна измениться, как показано на рисунке В-7.

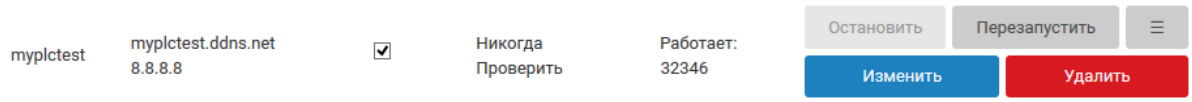
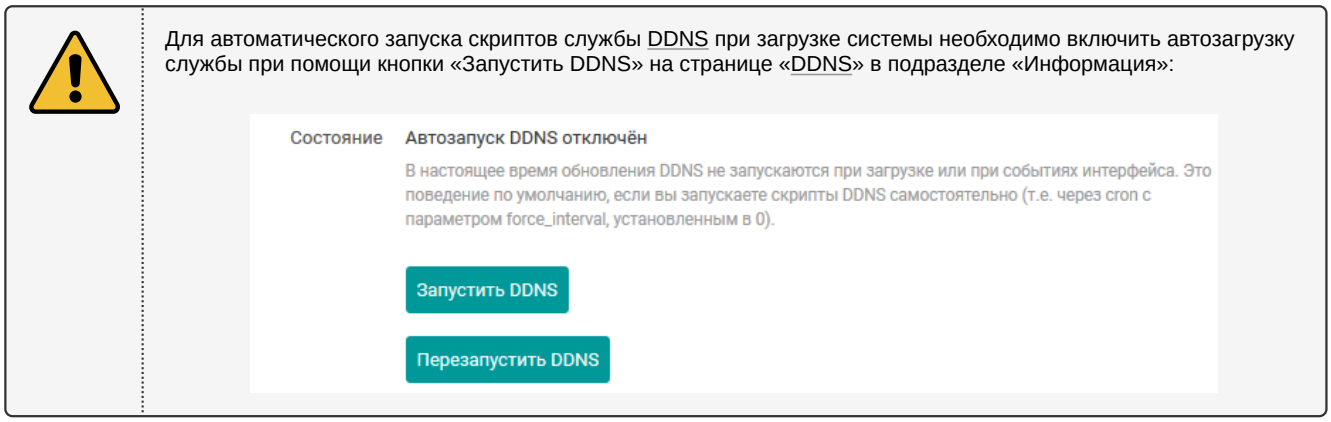


Рис. В-7: Созданная DDNS служба с запущенным скриптом



Как видно на рисунке В-7, 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-8) только при выполнении следующей плановой проверки (по умолчанию, проверка выполняется раз в 10 минут).

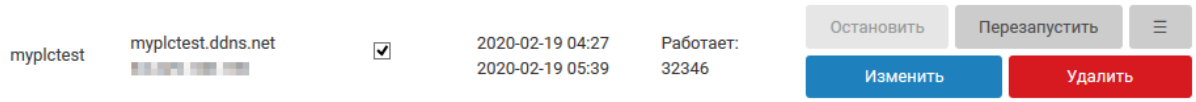


Рис. В-8: Созданная DDNS запись с обновлённым IP-адресом

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 6.1.3.1.4) 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-9.

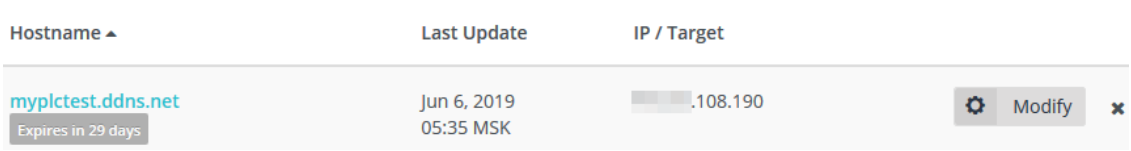


Рис. B-9: Таблица «Hostnames» с обновлённым IP-адресом домена в панели управления DDNS провайдера no-ip.com

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.

Приложение Г Пример настройки OpenVPN клиента

В данном приложении, в качестве примера, приведено описание процедуры настройки экземпляра OpenVPN клиента с использованием сервиса бесплатного VPN доступа freeopenvpn.org[1].

Г.1 Учётные данные и конфигурационный файл OVPN

Г.1.1 Перейдите на сайт сервиса freeopenvpn.org по ссылке https://www.freeopenvpn.org с использованием любого доступного браузера. На открывшейся странице необходимо выбрать любой доступный VPN-сервер в разделе «Список бесплатных VPN-серверов» (см. рисунок Г-1). В данном приложении, в качестве примера, был выбран сервер «Нидерланды».

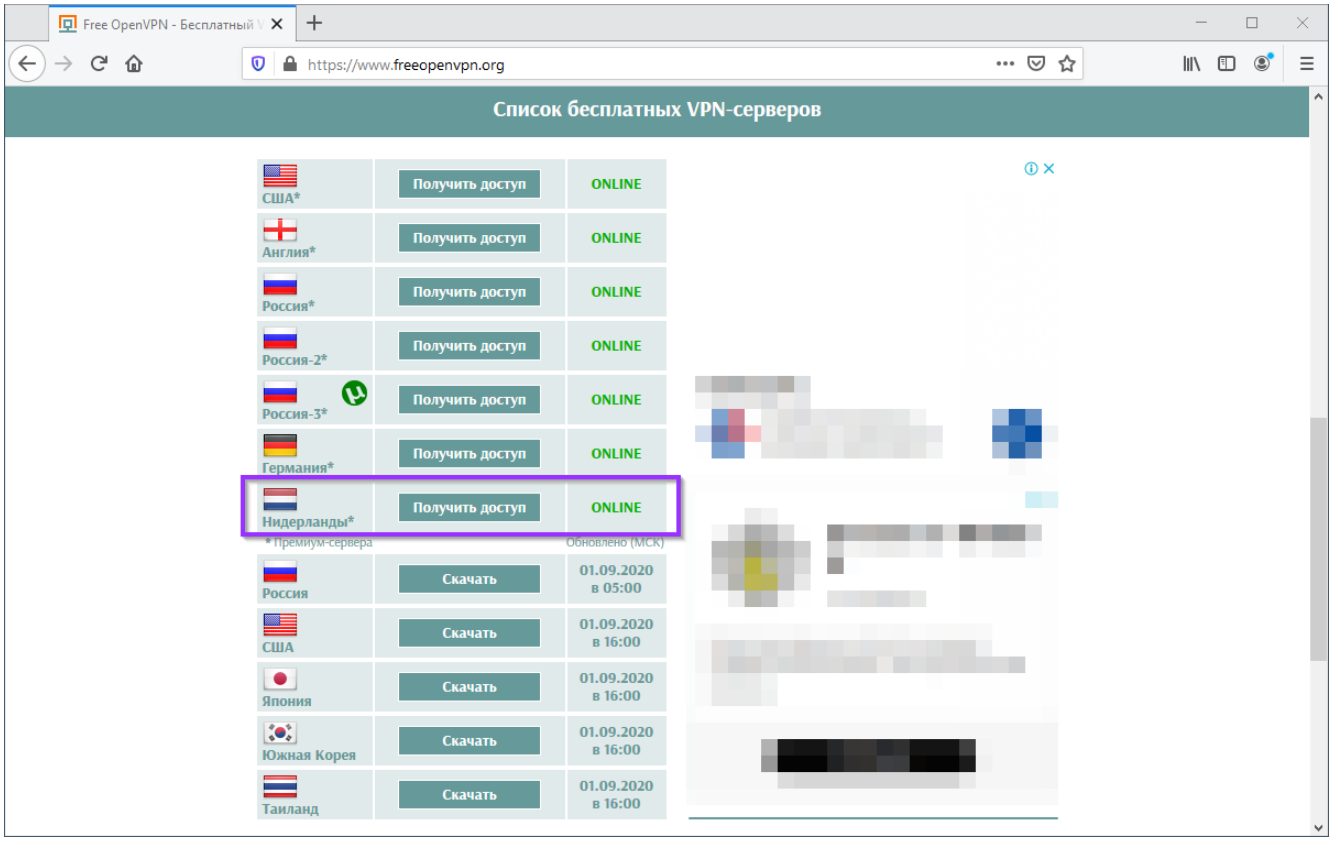


Рис. Г-1: Сайт сервиса бесплатного VPN доступа freeopenvpn.org

Г.1.2 На открывшейся странице в разделе «Доступ к бесплатному VPN-серверу в Нидерландах» будут расположены две ссылки для скачивания конфигурационного файла в формате OVPN и учётные данные в виде имени пользователя и пароля/PIN (см. рисунок Г-2).

Для скачивания доступно два конфигурационных файла:

- для использования протокола UDP — ссылка «UDP»;
- для использования протокола TCP — ссылка «TCP».

В данном документе рассматривается пример с использованием протокола TCP. Поэтому был скачан и сохранён файл по ссылке «TCP».

Учётные данные (имя пользователя и пароль) на данном шаге необходимо запомнить. Эти данные потребуются на шаге настройки подключения на устройстве (см. раздел Г.3).

[1] https://www.freeopenvpn.org/

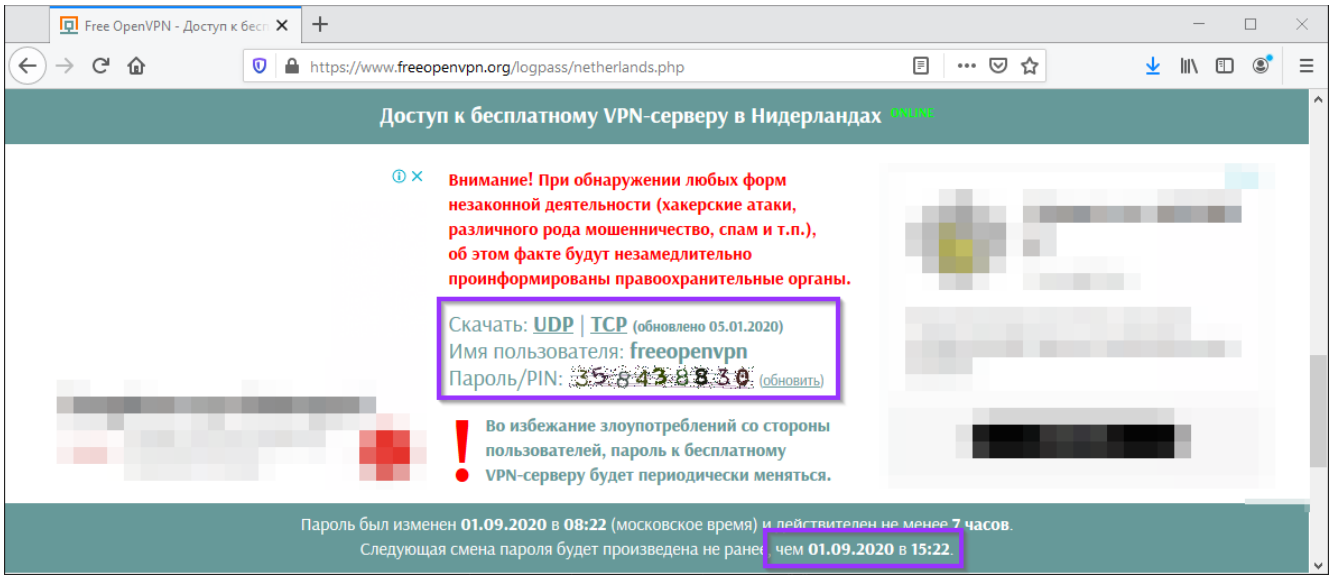


Рис. Г-2: Сайт сервиса бесплатного VPN доступа freeopenvpn.org

Г.2 Подготовка сетевого подключения

Г.2.1 Перейдите в Web-интерфейсе управления устройством на страницу «Интерфейсы» раздела главного меню «Сеть». На открывшейся странице нажмите кнопку «Добавить новый интерфейс...» (см. рисунок Г-3).

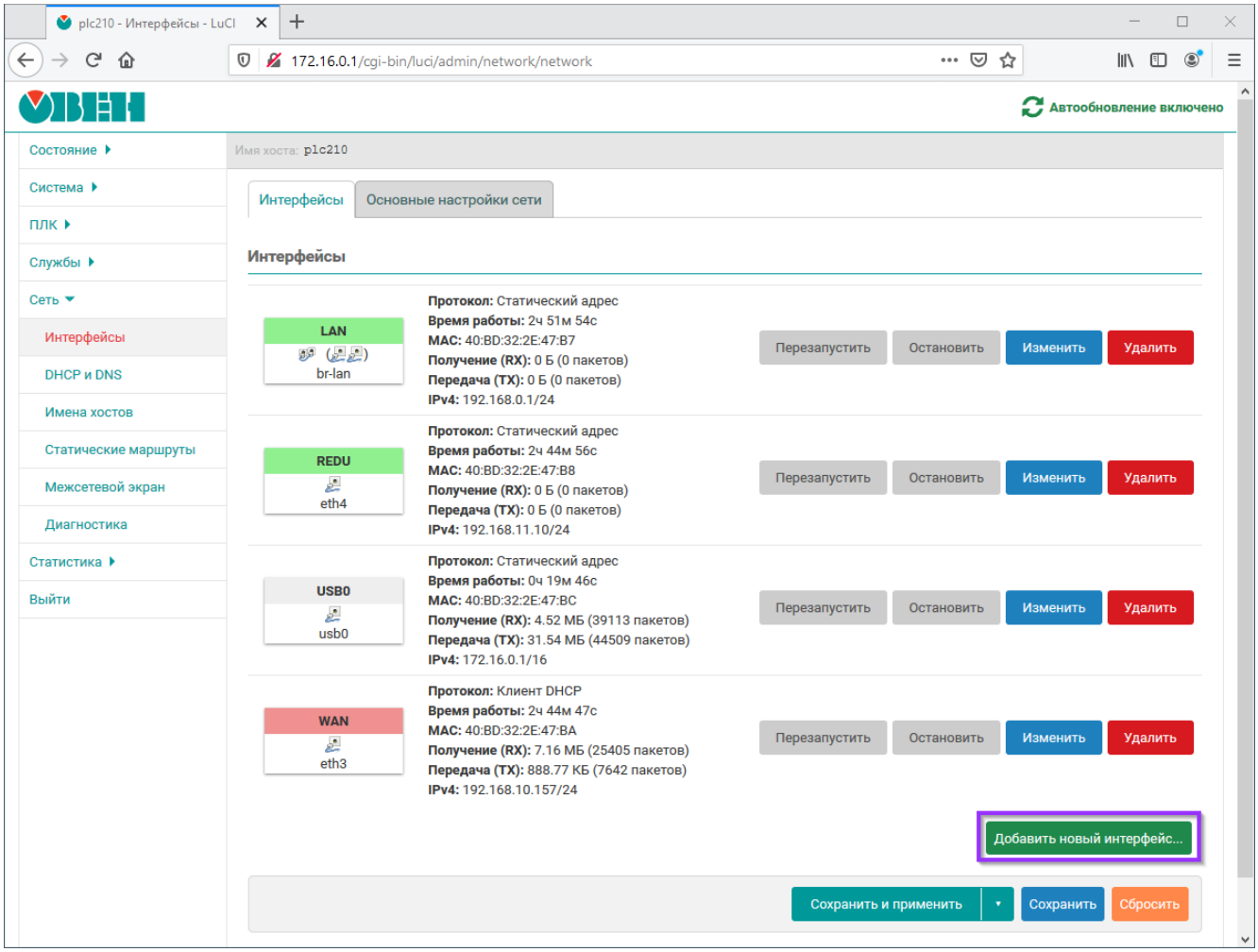


Рис. Г-3: Создание сетевого интерфейса OpenVPN подключения

Г.2.2 В открывшемся окне настроек необходимо установить следующие значения (см. рисунок Г-4):

- «Имя» — произвольное имя интерфейса (в данном приложении, в качестве примера, устанавливается имя «OpenVPN»);
- «Протокол» — неуправляемый;
- «Объединить в мост» — выключено (на контроллерах ПЛК200 и СПК1xx данная настройка отсутствует);
- «Интерфейс» — имя виртуального интерфейса OpenVPN подключения. Следует выбрать произвольное, не конфликтующее с другими интерфейсами, имя в формате `tunX`, где `X` — произвольный номер. В данном приложении, в качестве примера, было выбрано имя `tun100`. Так как на момент создания интерфейса его ещё не существует, то имя интерфейса необходимо ввести вручную в поле «– пользовательский –», которое появляется при раскрытии списка доступных интерфейсов.

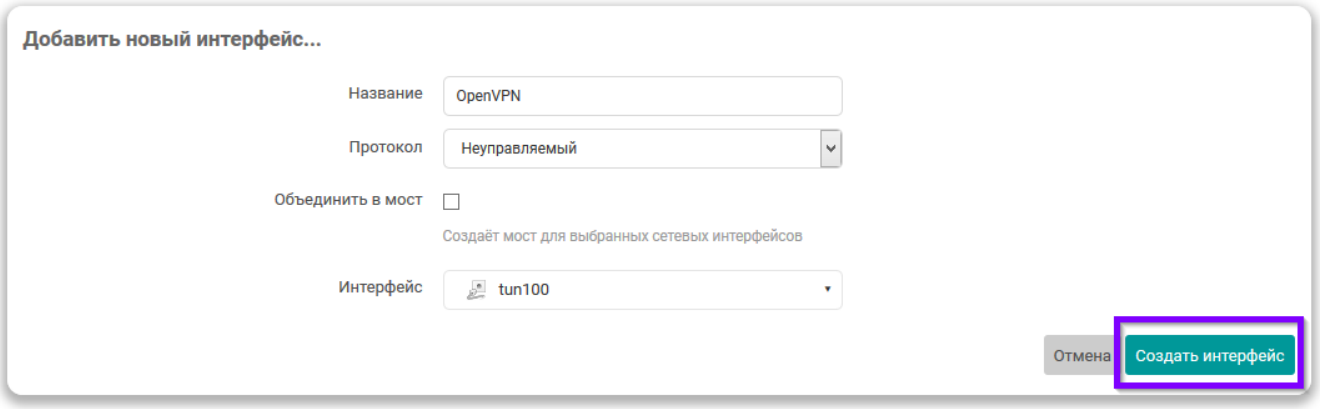


Рис. Г-4: Настройки сетевого интерфейса OpenVPN подключения

Г.2.3 После ввода настроек нового интерфейса необходимо нажать кнопку «Создать интерфейс» (см. рисунок Г-4).

Г.2.4 В открывшемся окне перейти во вкладку «Настройки межсетевого экрана» и выбрать зону «wan» в списке «Создать / назначить зону сетевого экрана» (см. рисунок Г-5). Нажать кнопку «Сохранить».

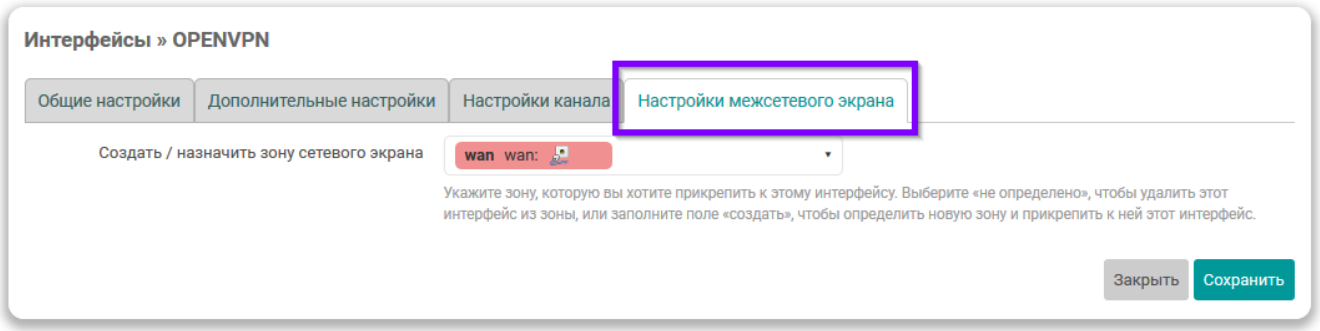


Рис. Г-5: Настройка зоны межсетевого экрана интерфейса OpenVPN подключения

Г.2.5 На основной странице настройки сетевых интерфейсов нажать кнопку «Сохранить и применить».

Г.3 Настройка экземпляра OpenVPN клиента

Г.3.1 Перейдите в Web-интерфейсе управления устройством на страницу «Конфигурация» раздела главного меню «Службы -> OpenVPN клиент». На открывшейся странице отметьте флажок «включить автозапуск OpenVPN» и нажмите кнопку «Добавить новый экземпляр...» (см. рисунок Г-6).

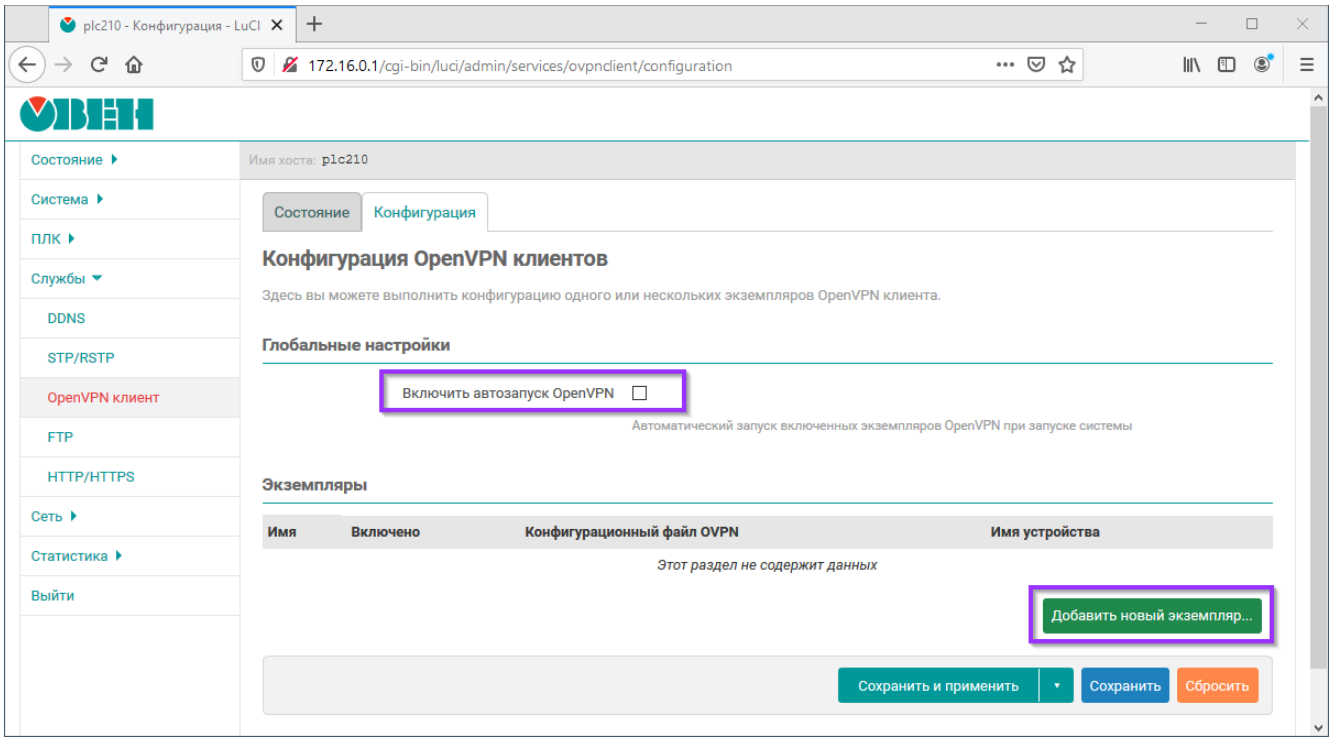


Рис. Г-6: Настройка экземпляра OpenVPN клиента

Г.3.2 В открывшемся всплывающем окне необходимо ввести произвольное имя нового экземпляра OpenVPN клиента (см. рисунок Г-7). В данном приложении, в качестве примера, так как ранее был выбран VPN-сервер в Нидерландах (см. раздел Г.1), было выбрано имя «netherlands».

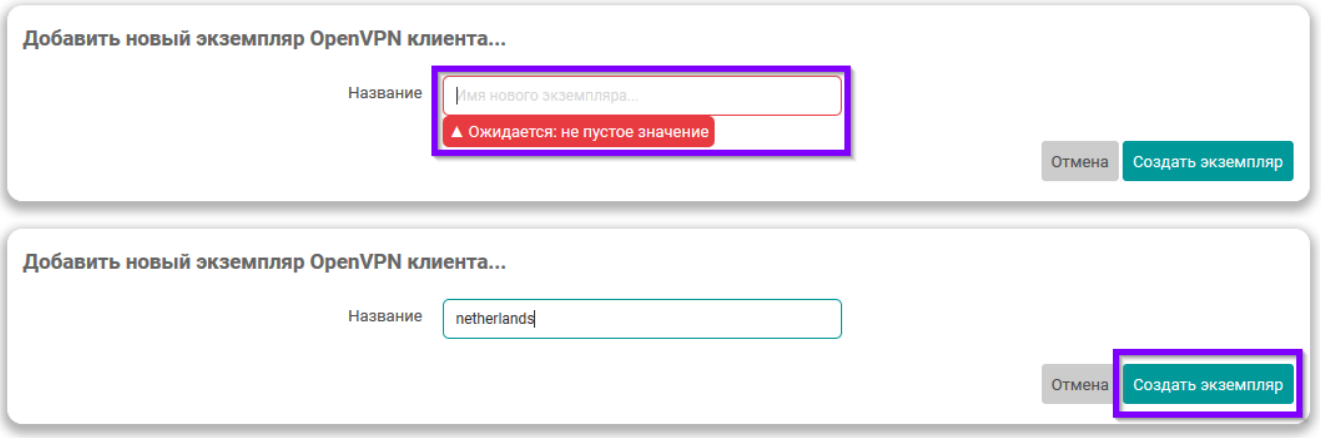


Рис. Г-7: Ввод имени нового экземпляра OpenVPN клиента

Г.3.3 В открывшемся окне настроек экземпляра OpenVPN клиента необходимо установить следующие значения (см. рисунок Г-8):

- «Включено» — включить;
- «Конфигурационные файл OVPN» — выбрать (загрузить) конфигурационный файл в формате OVPN. Процедура скачивания подобного файла на примере сервиса freeopenvpn.org рассмотрена выше в разделе Г.1. Общая процедура загрузки конфигурационных файлов OVPN подробно рассмотрена в разделе 6.3.2.1.1;
- «Имя устройства» — ввести имя устройства, которое было выбрано при подготовке сетевого интерфейса OpenVPN подключения (см. раздел Г.2);
- «Аутентификация по имени пользователя и паролю» — включить;
- «Имя пользователя», «Пароль» — учётные данные, получение которых рассмотрено в разделе Г.1.

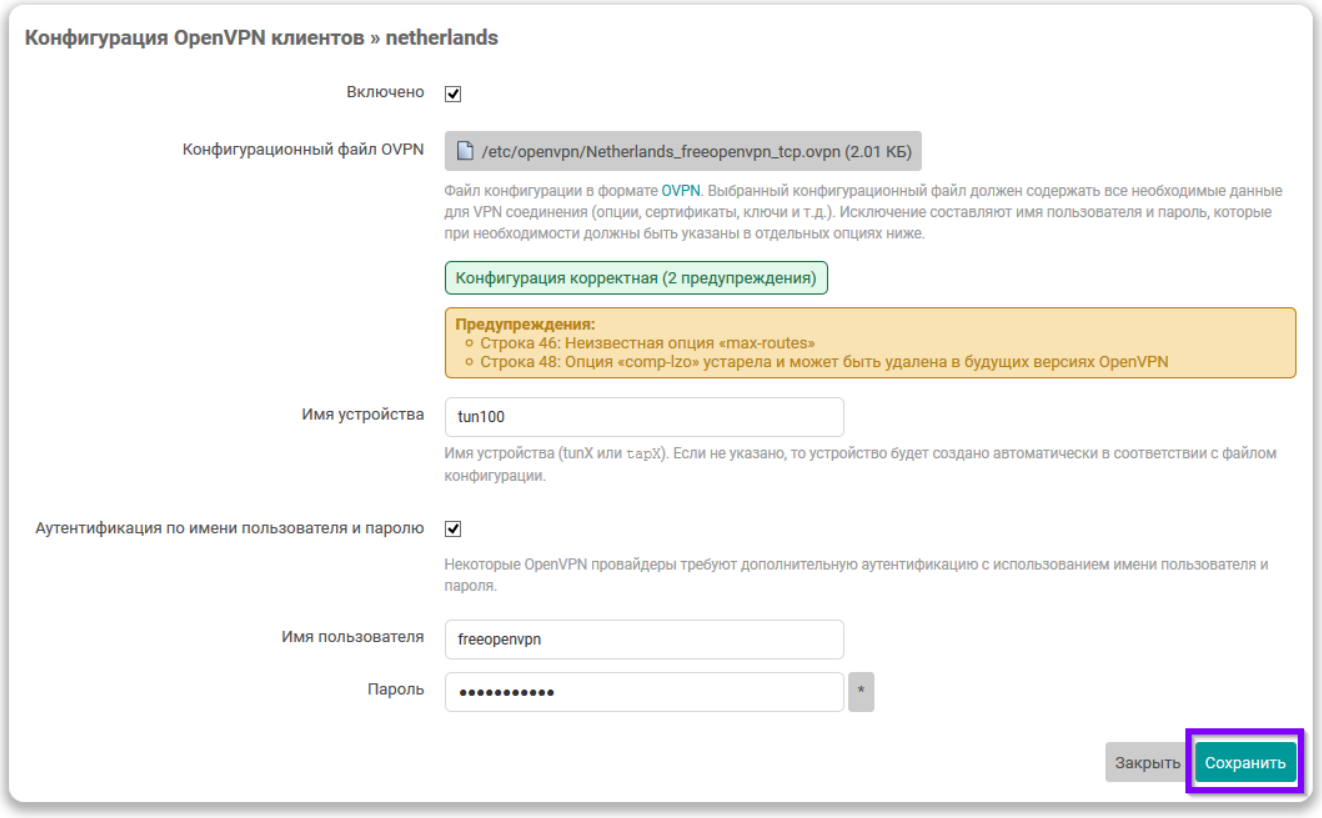


Рис. Г-8: Ввод настроек нового экземпляра OpenVPN клиента

Г.3.4 Нажать кнопку «Сохранить». На основной странице настроек экземпляров OpenVPN клиентов нажать кнопку «Сохранить и применить» (см. рисунок Г-9).

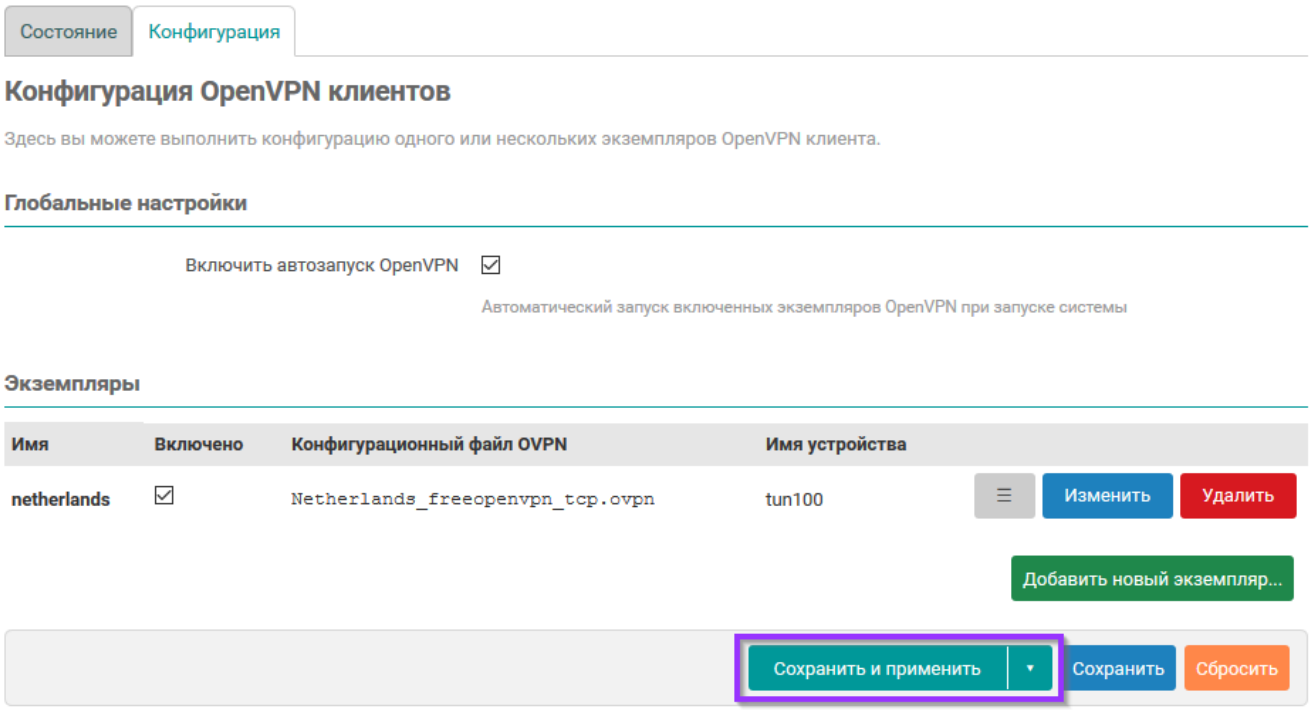


Рис. Г-9: Сохранение и применение настроек нового экземпляра OpenVPN клиента

Г.4 Проверка подключения экземпляра OpenVPN клиента

Г.4.1 Перейдите в Web-интерфейсе управления устройством на страницу «Состояние» раздела главного меню «Службы -> OpenVPN клиент». На открывшейся странице должно отображаться состояние созданного (см. раздел Г.3) экземпляра OpenVPN клиента (см. рисунок Г-10).

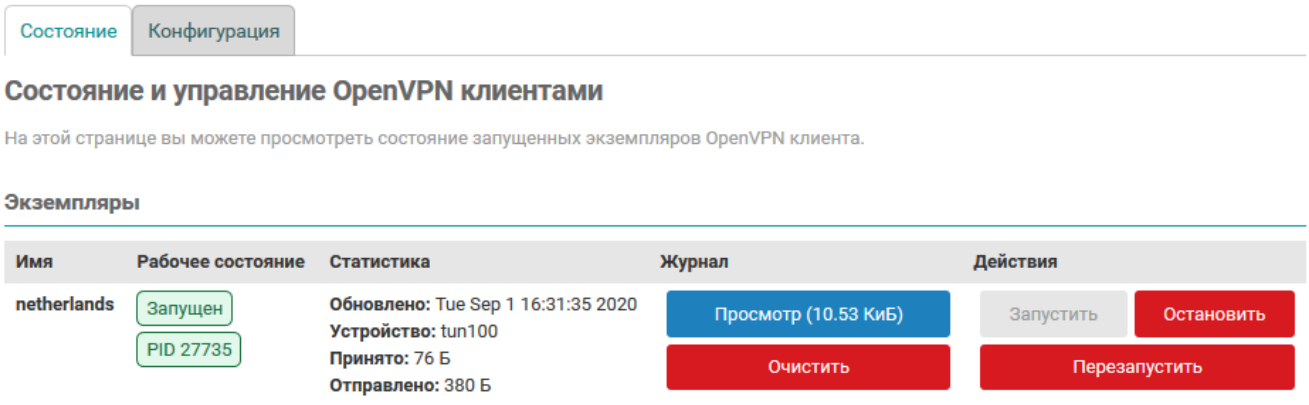


Рис. Г-10: Состояние экземпляра OpenVPN клиента

Г.4.2 При помощи сетевой диагностики «определение внешнего IP-адреса» (см. раздел 7.6.4) можно посмотреть реальный внешний IP-адрес.

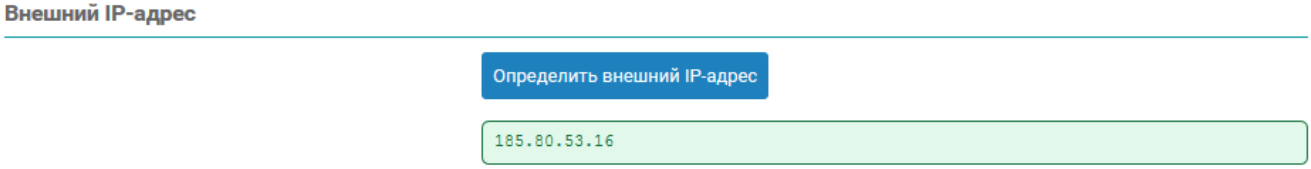


Рис. Г-11: Внешний IP-адрес при включённом OpenVPN подключении

Г.4.3 На странице «Обзор» (см. раздел 3.1) в разделе «Состояние портов сетевых интерфейсов» (см. раздел 3.1.4) будет отображаться сетевой интерфейс созданного экземпляра OpenVPN клиента (см. рисунок Г-12).

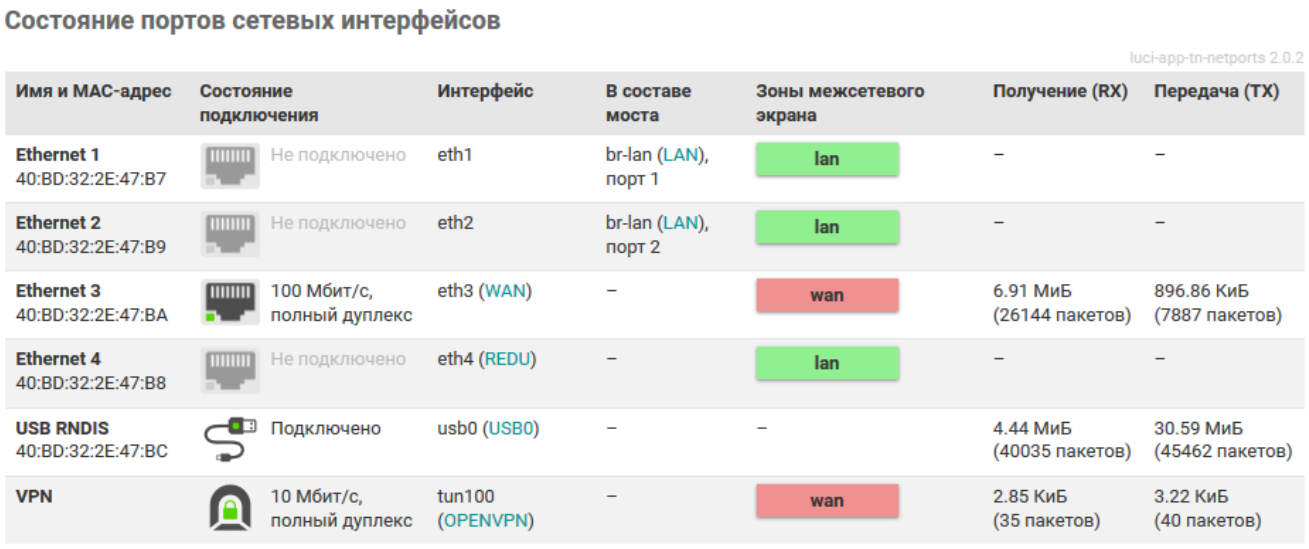


Рис. Г-12: OpenVPN подключение в таблице состояния портов сетевых интерфейсов

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. 31, 125).
2. Использование устройства ПЛК210 в сетях Ethernet с поддержкой протоколов STP/RSTP. Руководство пользователя. TN-UG-KSZ8895-RSTP. ОВЕН (цит. на с. 31, 125).
3. Load Average. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Load_Average (цит. на с. 45, 53, 200).
4. Netfilter. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Netfilter (цит. на с. 51).
5. Iptables. Викиучебник. Открытые книги для открытого мира. URL: https://ru.wikibooks.org/wiki/Iptables (цит. на с. 51, 179, 193).
6. sched — overview of CPU scheduling. Linux man page. URL: http://man7.org/linux/man-pages/man7/sched.7.html (цит. на с. 67, 68).
7. mount — mount a filesystem. Linux man page. URL: http://man7.org/linux/man-pages/man8/mount.8.html (цит. на с. 71, 73).
8. Bell character. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Bell_character (цит. на с. 84).
9. ping — send ICMP ECHO_REQUEST to network hosts. Linux man page. URL: https://www.man7.org/linux/man-pages/man8/ping.8.html (цит. на с. 100).
10. CSV. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/CSV (цит. на с. 110).
11. C++ Reference. Function strftime(). URL: http://www.cplusplus.com/reference/ctime/strftime/ (цит. на с. 116).
12. Reference manual for OpenVPN 2.4. URL: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/ (цит. на с. 139, 140, 143).
13. 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. 145, 168).
14. 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. 156).
15. Spanning Tree Protocol. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/STP (цит. на с. 156).
16. IGMP snooping. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/IGMP_snooping (цит. на с. 156).
17. BOOTP / DHCP options. RFC Sourcebook. URL: http://www.networksorcery.com/enp/protocol/bootp/options.htm (цит. на с. 160).
18. DNS rebinding. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/DNS_rebinding (цит. на с. 168).
19. resolv.conf — resolver configuration file. Linux man page. URL: http://man7.org/linux/man-pages/man5/resolv.conf.5.html (цит. на с. 168).
20. hosts — static table lookup for hostnames. Linux man page. URL: http://man7.org/linux/man-pages/man5/hosts.5.html (цит. на с. 168).
21. ethers — Ethernet address to IP number database. Linux man page. URL: http://man7.org/linux/man-pages/man5/ethers.5.html (цит. на с. 168).
22. SYN-flood. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/SYN-%D1%84%D0%BB%D1%83%D0%B4 (цит. на с. 175).
23. NAT loopback. Wikipedia. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/NAT#NAT_loopback (цит. на с. 182).

24. collectd – The system statistics collection daemon. Official site.
URL: https://collectd.org/ (цит. на с. 197).

25. 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. 198).

26. Краткое описание основных функций Web-интерфейса управления устройства ПЛК210. Руководство пользователя. TN-UG-OWRT-LUCI-R2. ОВЕН (цит. на с. 227).

История редакций

Редакция	Дата	Изменения
3.1.0	xx.yy.2020	Текст документа адаптирован для применения на устройствах ПЛК200, ПЛК210 и СПК1xx. 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 и 7-17. Заменён рисунок 7-5. Внесены изменения в раздел 2 в связи с изменениями интерфейса мастера настройки. Добавлено описание шага настройки функции резервирования ПЛК (раздел 2.7). Добавлено описание новой сетевой диагностики «Внешний IP-адрес» (раздел 7.6.4). Отражены изменения страниц настроек FTP-сервера (раздел 6.5). Отражены изменения на страницах состояния и настроек службы STP/RSTP (раздел 6.2). Добавлен раздел с описанием страницы управления и мониторинга функции резервирования ПЛК (раздел 5.5). Добавлен раздел с описанием режимов работы аппаратного коммутатора контроллеров ПЛК200 (раздел 3.1.4.1). Добавлен раздел с описанием настроек OpenVPN клиента (раздел 6.3). Обновлено описание проверки доступа к консоли устройства ПЛК210 по протоколу SSH (приложение A). Заменены рисунки 3-18, 3-19, 3-20 и 3-21.
3.0.2	28.04.2020	Исправлены небольшие неточности в тексте раздела 4.7.
3.0.1	04.03.2020	Изменён текст и рисунки раздела 4.7.
3.0.0	21.02.2020	Глобальное обновление документа «TN-UG-OWRT-LUCI-R2» [26] в соответствии с обновлением версии веб-интерфейса LuCI. Добавлено описание дополнительных настроек, заменено большинство рисунков.