РОУТЕР

TOPAZ GSM

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

ПЛСТ.465624.513 РЭ

Москва 2025

ОГЛАВЛЕНИЕ

Настоящее руководство по эксплуатации (РЭ) предназначено для ознакомления со сведениями о конструкции, принципе действия, технических характеристиках роутера **TOPAZ GSM** (далее по тексту – устройство), его составных частях, указания, необходимые для правильной и безопасной эксплуатации, технического обслуживания, ремонта, хранения и транспортирования, а также схемы подключения устройства к цепям питания, телемеханики и передачи данных.

Перед началом работы с устройством необходимо ознакомиться с настоящим РЭ.

РЭ предназначено для эксплуатационного персонала и инженеров-проектировщиков АСУ ТП, систем телемеханики и диспетчеризации.

В СВЯЗИ С ПОСТОЯННОЙ РАБОТОЙ ПО СОВЕРШЕНСТВОВАНИЮ ИЗДЕЛИЯ, В КОНСТРУКЦИЮ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МОГУТ БЫТЬ ВНЕСЕНЫ ИЗМЕНЕНИЯ, НЕ УХУДШАЮЩИЕ ЕГО ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И НЕ ОТРАЖЕННЫЕ В НАСТОЯЩЕМ ДОКУМЕНТЕ.

1 ОПИСАНИЕ И РАБОТА

1.1 Назначение изделия

Устройство является средством связи, предназначенным для и решения задач организации связи, автоматизации, телемеханики и диспетчеризации. Передача данных осуществляется по сети GSM-GPRS, Ethernet и интерфейсам последовательной передачи данных.

Используется при организации каналов связи в системах мониторинга и управления инженерным оборудованием различных объектов:

- жилищно-коммунального и городского хозяйства: котельных, насосных станций, тепловых пунктов, а также инженерных систем «умный дом»;
- энергетики, в том числе цифровых подстанций;
- промышленности и сельского хозяйства.

1.2 Модификации и условные обозначения

Функциональные возможности устройства, количество и тип интерфейсов передачи данных определяются типом базовой платы и количеством/типом плат расширений.

Количество и тип интерфейсов передачи данных устройства, а также наличие дополнительных функциональных возможностей зависят от конкретной модификации и отражены в расшифровке названия (заказной кодировке), согласно таблице 1.

Таблица 1 – Расшифровка кода заказа устройства

TOPAZ GSM-[A]-LTE-[B]-[C1- … -Cx]-[D1- … -Dx]-[E]-[F]-G (H-I-J)		
Позиция	**Код**	**Описание**
Особенности модификации		
A	nCHNL	Активные радиомодули
	«n» – количество активных радиомодулей.	
B	SC	Исполнение SIM-чип
Коммуникационные порты Ethernet		
C1- … -Cx	nGSFP	Ethernet 1000 Мбит/с SFP[1)]
	nGTXSFP	Ethernet 1000 Мбит/с combo-port RJ-45/SFP[1)]
	nGTx	Ethernet 1000 Мбит/с TX RJ-45
	nTx	Ethernet 100 Мбит/с TX RJ-45
	nFxS	Ethernet 100 Мбит/с FX LC single-mode

TOPAZ GSM-[A]-LTE-[B]-[C1- … -Cx]-[D1- … -Dx]-[E]-[F]-G (H-I-J)		
Позиция	**Код**	**Описание**
	nFxM	Ethernet 100 Мбит/с FX LC multi-mode
	«n» – количество портов Ethernet соответствующего типа, максимальное суммарное количество портов Ethernet – 32.	
Коммуникационные порты последовательной передачи данных		
D1- … -Dx	nR	RS-485 клеммный вход
	nRS232	RS-232, клеммный вход или разъем DB9 (определяется заводом-изготовителем)
	nRS422	RS-422 клеммный вход
	«n» – количество портов последовательной передачи данных соответствующего типа, максимальное суммарное количество портов последовательной передачи данных – 16.	
Дополнительные функции		
E	DIOn	Универсальные каналы дискретного ввода-вывода, где «n» - количество каналов. Шаг наращивания – 4.
F	SSDm	SSD накопители, где «m» – суммарный объем ПЗУ накопителей SSD в Гб (Тб)
	SSDmT	
Исполнение по питанию		
G	2LV	Два входа питания 24В DC
	HV	Один вход питания 220В DC/AC
	2HV	Два входа питания 220В DC/AC
Средства защиты сети		
H	-	Отсутствуют дополнительные средства защиты сети
	CSG	CybSec Gateway (Шлюз безопасности)
Сертифицированная ОС		
I	-	Отсутствует сертифицированная ОС на базе Linux
	ОС	Сертифицированная ОС на базе Linux
Дополнительное ПО		
J	-	Отсутствует дополнительное ПО
	01	ТСС-Dcrypt, в комплекте с лицензиями и сертификатами
	02	ИнфоТЕКС-Vipnet, в комплекте с лицензиями и сертификатами
	03	КодБезопасности-Континент АП, в комплекте с лицензиями и сертификатами

1) SFP-модули заказываются дополнительно:
   - **TOPAZ SFP-100-01-MM** – 100 мегабитный многомодовый SFP-модуль
   - **TOPAZ SFP-100-01-SM** – 100 мегабитный одномодовый SFP-модуль
   - **TOPAZ SFP-1G-10-SM** – гигабитный одномодовый SFP-модуль, дальность передачи 10 км
   - **TOPAZ SFP-1G-15-SM** – гигабитный одномодовый SFP-модуль, дальность передачи 15 км
   - **TOPAZ SFP-1G-40-SM** – гигабитный одномодовый SFP-модуль, дальность передачи 40 км
   - **TOPAZ SFP-1G-01-MM** – гигабитный многомодовый SFP-модуль, дальность передачи 1 км
   - **TOPAZ SFP-1G-02-MM** – гигабитный многомодовый SFP-модуль, дальность передачи 2 км

Примеры записи обозначения устройства при заказе:

с двумя Ethernet 100 Мбит/с TX RJ-45, двумя портами RS-485, двумя входами питания 24 В: ***«Роутер TOPAZ GSM-LTE-2Tx-2R-2LV».***

с двумя Ethernet 100 Мбит/с TX RJ-45, двумя активными радиомодулями, четырьмя портами RS-485, двумя входами питания 24 В:

«Роутер TOPAZ GSM-2CHNL-LTE-2Tx-4R-2LV».

с двумя Ethernet 100 Мбит/с TX RJ-45, двумя портами RS-485, 4 каналами дискретного ввода/вывода, двумя входами питания 24 В:

«Роутер TOPAZ GSM*-LTE-*2Tx-2R-DIO4-2LV».

с двумя Ethernet 100 Мбит/с TX RJ-45, двумя портами RS-485, двумя портами RS-232, 4 каналами дискретного ввода/вывода, двумя входами питания 24 В:

«Роутер TOPAZ GSM*-LTE-*2Tx-2R-2RS232-DIO4-2LV».

с двумя Ethernet 100 Мбит/с TX RJ-45, двумя Ethernet 100 Мбит/с FX LC multi-mode, четырьмя портами RS-232, 4 каналами дискретного ввода/вывода, двумя входами питания 220 В:

«Роутер TOPAZ GSM*-LTE-*2Tx-2FxM-4RS232-DIO4-HV».

1.3 Технические характеристики

1.3.1 Конструкция

Конструктивно устройство выполнено в пластиковом корпусе, не поддерживающем горение с креплением для установки на DIN-рейку. Вентиляционные отверстия корпуса расположены сверху и снизу корпуса. Степень защиты от проникновения внутрь твердых частиц, пыли и воды – не ниже IP20 по ГОСТ 14254-2015. По устойчивости к механическим воздействиям, устройство относится к классу М40 по ГОСТ 30631-99. Габаритные размеры устройства (ШВГ) не более 180х108,5х124 мм. Масса устройства не более 1 кг.

Внешний вид, описание входов, выходов и индикаторов устройства приведены в приложении А настоящего руководства.

1.3.2 Рабочие условия эксплуатации

По рабочим условиям эксплуатации (климатическим воздействиям) устройство соответствует изделиям группы С2 по ГОСТ Р 52931-2008. По устойчивости к воздействию атмосферного давления устройство соответствует группе Р2 по ГОСТ Р 52931-2008.

Таблица 2 – Рабочие условия эксплуатации

Параметр	Значение
Температура окружающего воздуха, ^{0}C	от -40 до +70
Относительная влажность воздуха при температуре 30 ^{0}C и ниже, %	до 100
Атмосферное давление воздуха, кПа	от 60 до 106,7

1.3.3 Безопасность и электромагнитная совместимость

По устойчивости к электромагнитным помехам устройство соответствует ГОСТ Р 51318.11-2006 для класса А группы 1, и ГОСТ Р 51317.6.5-2006 для оборудования, применяемого на электростанциях и подстанциях.

Радиопомехи не превышают значений, установленных для класса А по ГОСТ 30805.22-2013, для класса А по ГОСТ 30804.3.2-2013.

Устройство, в части защиты от поражения электрическим током, соответствует требованиям ГОСТ 12.2.091-2012. Класс защиты от поражения электрическим током I по ГОСТ 12.2.007.0-75.

Электрическое сопротивление изоляции устройства не менее 2,5 МОм. Электрическая прочность изоляции устройства выдерживает без разрушения испытательное напряжение 2500 В, 50 Гц в течение 1 мин.

Устройство соответствует требованиям технических регламентов Таможенного союза ТР ТС 004/2011 «О безопасности низковольтного оборудования», ТР ТС 020/2011 «Электромагнитная совместимость технических средств».

1.3.4 Надежность

Устройство является восстанавливаемым, ремонтируемым изделием, предназначенным для круглосуточной эксплуатации в стационарных условиях в производственных помещениях. Режим работы устройства непрерывный. Продолжительность непрерывной работы не ограничена. Норма средней наработки на отказ в нормальных условиях применения составляет 140 000 ч. Полный средний срок службы составляет 30 лет. Среднее время восстановления работоспособности на объекте эксплуатации (без учета времени прибытия персонала и при наличии ЗИП) не более 30 минут.

1.3.5 Питание

Количество и тип каналов питания устройства зависят от исполнения по питанию. Характеристики каналов питания приведены в таблице ниже.

Таблица 3 – Характеристики питания

Наименование параметра	Значение
Количество каналов питания	до 2
Номинальное напряжение питания, В: - канал 24 В - канал 220 В	 от 10 до 30 (DC) от 90 до 265 (AC); от 100 до 365 (DC)
Частотный диапазон напряжения питания 220 В, Гц	от 45 до 55
Ток потребления канала питания 220 В, не более, А	0,4
Потребляемая мощность плат устройства, не более, Вт	6

Кратковременные перерывы питания (до 200 мс) не влияют на работу устройства. При нарушении питания на время более 200 мс, устройство корректно завершает свою работу, а при восстановлении напряжения питания устройство переходит в рабочий режим автоматически. Под корректным завершением работы в данном случае понимается отсутствие передачи ложной информации и потери конфигурационной информации. Устройство обеспечивает нормальную работу при произвольном изменении напряжения питания в пределах рабочего диапазона. Время установления рабочего режима при восстановлении питания не более 10 с.

Конфигурация устройства сохраняется в энергонезависимой памяти, которая обеспечивает сохранение параметров, при отсутствии напряжения питания, в течение 30 лет.

1.3.6 Характеристики контроллера

Технические характеристики основного контроллера приведены в таблице ниже.

Таблица 4 – Характеристики контроллера

Наименование параметра	Значение
Характеристики контроллера	
Операционная система	Linux
Слот для Flash-карты	microSD
Процессор	ARM Cortex-A8

Наименование параметра	Значение
Частота, МГц	до 1000
Память ОЗУ, Гб	0,5 (DDR3L)
Память ПЗУ, Гб	4 (eMMC)

1.3.7 Каналы дискретного ввода-вывода

Количество каналов дискретного ввода-вывода указано в заказной кодировке устройства. Технические характеристики каналов дискретного ввода-вывода приведены в таблице ниже.

Таблица 5 – Технические характеристики каналов дискретного ввода-вывода

Наименование параметра	Значение
Устройства, выпущенные до I квартала 2025 года:	
Режим работы	дискретный ввод; дискретный вывод
Номинальное напряжение встроенного источника питания, В	12 ± 15%
Максимальный напряжение внешнего источника питания, В	24
Максимальный допустимый суммарный ток в цепи DIO, мА: - при питании от внутреннего источника питания - при питании от внешнего источника питания	 200 400
Ток потребления на каждом канале, мА	3
Сопротивление токоограничивающего резистора, кОм	4
Устройства, выпущенные после I квартала 2025 года:	
Режим работы	дискретный ввод; дискретный вывод
Номинальное напряжение встроенного источника питания, В	24 ± 10%
Максимальный напряжение внешнего источника питания, В	30
Максимальный допустимый выходной ток встроенного источника питания, мА	100
Максимально допустимый ток каждого канала в режиме дискретного выхода, мА	50
Ток потребления на каждом канале, мА	3
Сопротивление токоограничивающего резистора, кОм	4

1.3.8 Интерфейсы передачи данных

Количество и тип каналов передачи данных обозначается в заказной кодировке устройства.

Таблица 6 – Технические характеристики интерфейса Ethernet

Заказное обозначение	Тип разъема	Скорость передачи данных
nGSFP	SFP-корзина	10/100/1000
nGTx	порт RJ-45	
nGTXSFP	комбо-порт RJ-45/SFP	
nTx	порт RJ-45	10/100
nFxS	порт LC (одномодовое оптоволокно)	
nFxM	порт LC (многомодовое оптоволокно)	

Таблица 7 – Технические характеристики оптических каналов связи Ethernet

Наименование параметра		Одномодовое оптоволокно	Многомодовое оптоволокно
Сечение		9/125 мкм	50/125 мкм; 62,5/125 мкм
Дальность передачи, км	порт LC	15	2
	SFP-модуль	до 40	до 4
Длина волны, нм		1310	1310
Мощность передатчика, дБм		от -20 до 0	от -23,5 до -14
Чувствительность приемника, дБм		до -32	до -31

Примечание Комбо-порт GTXSFP работает в режиме автоматического переключения. При одновременном подключении ко входу RJ-45 и SFP, активен только вход SFP.

Примечание Скорость передачи данных порта SFP соответствует скорости передачи данных SFP-модуля

Таблица 8 – Поддерживаемые технологии Ethernet

Технологии	Описание
Поддерживаемые стандарты	IEEE 802.3 10BaseT; IEEE 802.3u 100BASE-TX, 100BASE-FX; IEEE 802.3z 1000BASE-X; IEEE 802.3ab 1000BASE-T; IEEE 802.3x управление потоком; IEEE 802.3az Ethernet с энергосберегающим режимом IEEE 802.1D-2004 STP, QoS; IEEE 802.1d STP; IEEE 802.1w RSTP; IEEE 802.1Q тегирование трафика.
Промышленные протоколы	Ethernet/IP; ГОСТ Р МЭК 60870-5-104; Modbus/TCP; IEC 61850
Управление	SSH; Console – CLI; Web.
Протоколы фильтрации трафика	VLAN на основе портов
Протоколы резервирования сети	STP/RSTP; PRP; HSR
Информационная безопасность	Authentication Certificate - SSL Certificate/SSH Key Regenerate; 802.1X – Port Based; Port Security – Static MAC Port Lock.
Протоколы синхронизации времени	ГОСТ Р МЭК 60870-5-104; NTP Server/Client; IEEE 1588v2 (PTP v2)

Таблица 9 – Технические характеристики последовательных интерфейсов

Наименование параметра	Значение
Протоколы передачи данных	ГОСТ Р МЭК 60870-5-101 (master/slave), Modbus RTU/ASCII (slave)
Режим передачи	асинхронный последовательный двухсторонний полудуплексный
Скорость передачи	2400 – 115 200 бит/с

Наименование параметра	Значение
	(по заказу до 4 Мбит/с)
Интерфейс RS-485	
Тип разъема	клеммный вход
Контакты	-D, +D, G
Максимальная длина линии связи, м	1 200
Количество устройств в сегменте сети	до 32 (до 254 с повторителями)
Интерфейс RS-232	
Тип разъема	Разъем DB9/Клеммный вход/Шина T-BUS
Контакты	Tx, Rx, GND
Количество устройств в сегменте сети, (работа в режиме точка-точка)	1
Интерфейс RS-422	
Тип разъема	клеммный вход
Контакты	-TX, +TX, -RX, +RX
Максимальная длина линии связи, м	1 200
Количество устройств в сегменте сети	1 в режиме master, до 10 в режиме slave

1.3.9 GSM модем

Тип модема и формат SIM-карт указаны в заказной кодировке устройства. Технические характеристики модема приведены в таблице ниже.

Таблица 10 – Технические характеристики модема

Наименование параметра		Значение
Количество SIM-карт		2
Формат SIM-карты		mini-SIM или SIM-chip
Разъём для антенны		SMA
Диапазоны частот, МГц	GSM, EDGE	850/900/1800/1900
	UMTS	800/850/900/1900/2100
	LTE FDD	800/850/900/1800/2100/2600
Выходная мощность	GSM 850/900	Class 4 (33дБм±2дБ)
	GSM 1800/1900	Class 1 (30дБм ±2дБ)
	EDGE 850/900	Class E2 (27дБм ±3дБ)
	EDGE 1800/1900	Class E2 (26дБм +3/-4дБ)
	UMTS	Class 3 (24дБм+1/-3дБ)
	LTE FDD	Class 3 (23дБм±2дБ)
GSM-LTE модем		
Поддерживаемые стандарты передачи данных		GPRS, EDGE, UMTS, HSPDA, HSUPA, HSPA+, DC-HSPA+, LTE
Количество антенн		до 2 (поддержка MIMO)

1.4 Комплектность

Комплект поставки указывается в индивидуальном паспорте устройства.

В стандартный комплект поставки входят:

1) устройство TOPAZ GSM;
2) паспорт;
3) штекер MC 1,5/5-ST-3,81;
4) шинные соединители ME 22.5 TBUS 1.5/5-ST-3,81;*

5) разъем MSTBT 2,5/4-ST.*

Примечание: * – количество шинных соединителей и клеммных блоков согласно индивидуальному паспорту устройства;

Эксплуатационная документация доступна на сайте: http://www.tpz.ru

1.5 Устройство и работа

1.5.1 Функциональные возможности

Настройка, управление и контроль работы устройства осуществляется с использованием персонального компьютера, подключаемого через сеть Ethernet, либо через консоль (виртуальный COM-порт).

Устройство работает под управлением операционной системы Linux и реализует следующие базовые функции:

- передачи данных по GPRS сети;
- прием информации по цифровым каналам связи;
- выполнение прикладных программ;
- автоматическое накопление, хранение и передача информации по цифровым каналам связи;
- самодиагностика и тестирование работоспособности первичных преобразователей (датчиков);
- синхронизации собственных часов от внешней сети по протоколам PTP, NTP и SNTP;

В зависимости от исполнения, устройство также может выполнять функции:

- контроля состояния дискретных входов (телесигнализация);
- управления дискретными выходами (телеуправление).

1.5.2 Встроенная система безопасности

Встроенная система информационной безопасности устройства реализует следующие функции:

- идентификация, аутентификация пользователей;
- разделение прав пользователей;
- передача данных с использованием СКЗИ;
- регистрация событий безопасности;
- межсетевое экранирование;
- регистрация событий безопасности и их отправка в централизованные системы мониторинга;
- контроль целостности системы;

Система включает следующие подсистемы:

- подсистема регистрации событий безопасности;
- подсистема проверки целостности;
- подсистема криптозащиты каналов связи;
- подсистема аудита.

Подробное описание работы и конфигурирования системы информационной безопасности устройства приведены в ПЛСТ.421457.100 РП «Контроллер TOPAZ IEC DAS. Руководство пользователя».

1.5.3 Работа кнопок и индикаторов

На передней панели устройства расположены светодиодные индикаторы, отображающие работу устройства. Названия и количество индикаторов зависит от модификации и заказного обозначения устройства.

Также на передней панели устройства расположены кнопки, нажатие на которые осуществляется заостренным предметом.

- Кнопка **RS** предназначена для перезагрузки устройства без отключения питания. Кнопка **RS** может отсутствовать.
- Кнопка **RB** предназначена для активации загрузчика с SD-карты, при одновременном нажатии с кнопкой **RS**. В случае отсутствия кнопки **RS** активация загрузчика с SD-карты осуществляется посредством нажатия кнопки **RB**.

Информация о работе кнопок и индикаторов в различных исполнениях устройства содержится в приложении А.

1.6 Конфигурирование устройства

1.6.1 Подключение к командной строке

Конфигурирование устройства с помощью командной строки возможно через серийную консоль (порт USB на лицевой стороне устройства) либо через порт Ethernet по протоколу ssh.

Таблица 11 – Варианты доступа к настройкам устройства

Протокол	Описание	Требуемое ПО
SSH	Защищенный протокол передачи данных. Аналог протокола Telnet с шифрованием трафика при авторизации и работе с консолью.	UNIX – утилита `ssh` (стандартный SSH-клиент UNIX); Windows – PuTTY, WinSCP, openssh.
Серийная консоль	Подключение через консольный USB-порт устройства (virtual COM-port).	UNIX – утилита `minicom`; Windows XP – HyperTerminal (встроенное ПО); Windows 7, 8, 10 – PuTTY или аналог.

Конфигурирование устройства через SSH-соединение или серийную консоль можно осуществлять с помощью одной из терминальных программ. В приложении Б настоящего РЭ приведен пример подключения к устройству с помощью одной из таких программ.

ВНИМАНИЕ! ПРИ КОНФИГУРИРОВАНИИ УСТРОЙСТВА РЕКОМЕНДУЕТСЯ УДЕЛИТЬ ОСОБОЕ ВНИМАНИЕ НАСТРОЙКАМ ДОСТУПА ПО ПРОТОКОЛУ SSH. ОТ СЛОЖНОСТИ ПАРОЛЕЙ, РАЗРЕШЕНИЯ УДАЛЕННОГО ДОСТУПА, ИСПОЛЬЗУЕМЫХ ПОРТОВ СЕТЕВЫХ СЛУЖБ, НАСТРОЕК МЕЖСЕТЕВОГО ЭКРАНА И ДРУГИХ НАСТРОЕК СЕТЕВЫХ СЛУЖБ ЗАВИСИТ БЕЗОПАСНОСТЬ УСТРОЙСТВА И ПОДКЛЮЧЕННЫХ К НЕМУ УСТРОЙСТВ.

Логин и пароль при заводских настройках следующие:

Логин (Login): **root**

Пароль (Password): **root**

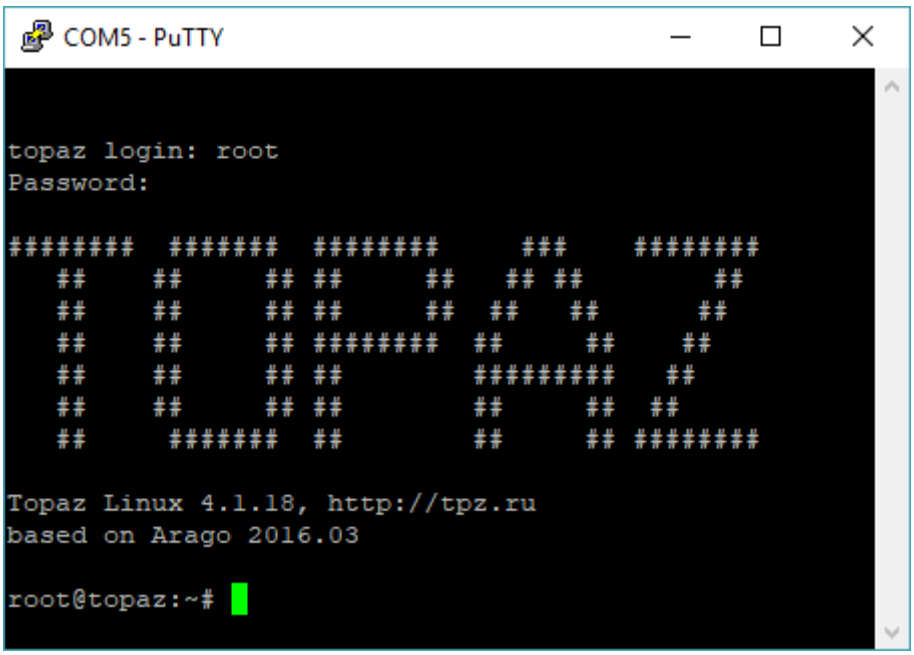


Рисунок 1 – Экран приветствия командной строки

1.6.1.1 Подключение через серийную консоль

При подключении устройства через консольный порт (USB) в системе появится виртуальный последовательный COM-порт, который можно использовать для соединения персонального компьютера с устройством. Для того, чтобы узнать номер порта, перейдите в «Диспетчер устройств» Windows и откройте вкладку «Порты». После чего, убедившись, что на устройство подано питание, соедините устройство с компьютером. Во вкладке «Порты» появится новый последовательный порт.

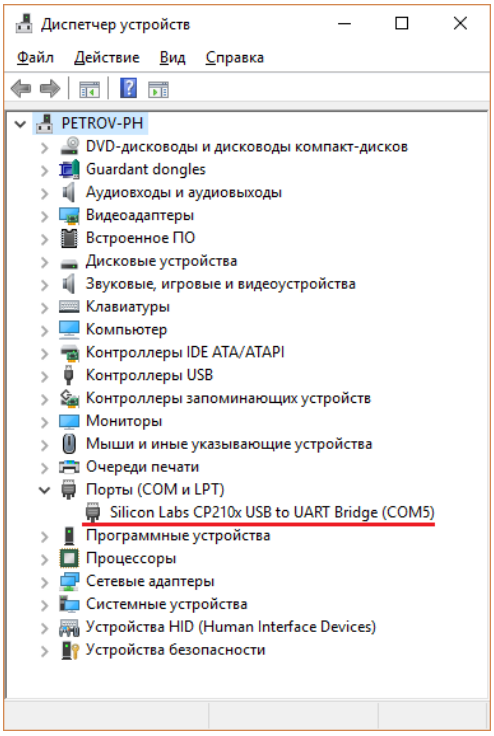


Рисунок 2 – Отображение устройства в диспетчере устройств Windows

Примечание Номер виртуального COM-порта присваивается операционной системой автоматически, поэтому на вашем компьютере он может отличаться от указанного в примере.

Последовательный порт консоли предоставляет пользователю удобный способ подключения к устройству, особенно при первом подключении и настройке устройства. Связь осуществляется по прямому последовательному соединению и пользователю не нужно знать IP адреса Ethernet-портов для того, чтобы подключиться к устройству.

Параметры передачи данных по виртуальному COM-порту приведены в таблице ниже.

Таблица 12 – Параметры соединения с устройством по виртуальному COM-порту

Параметр	Значение
Скорость передачи / Baudrate	115 200 bps
Биты данных / Parity None Data bits	8
Стоповые биты / Stop bits	1
Контроль четности / Parity	None
Управление потоком / Flow Control	None

1.6.1.2 Подключение через порт Ethernet по протоколу SSH

При подключении роутера к персональному компьютеру через Ethernet используются следующие настройки LAN:

порт LAN#1 192.168.1.1

макса подсети: 255.255.255.0

1.6.2 **Команды и утилиты для работы с устройством**

Команды консоли, описанные в данном разделе, предназначены для настройки работы.

1.6.2.1 Команда dmesg

Команда **dmesg** предназначена для вывода сообщений ядра системы при загрузке операционной системы.

1.6.2.1.1 Синтаксис

```
dmesg [-c] [-n <уровень>] [-s <размер>]
```

Таблица B.1 – Опции команды dmesg

Опция	Описание
-c	Очистить содержимого кольцевого буфера после вывода на экран.
-n <уровень>	Задать *уровень* выводимых сообщений. **-n 1** – выводить только тревожные сообщения
-s <размер>	Использовать буфер заданного *размера* для буфера сообщений. (По умолчанию 16392 байт)

1.6.2.1.2 Пример использования

Вывести на экран последние события ядра и очистить буфер логирования

```
dmesg -c
```

1.6.2.2 Команда factory_reset

Команда **`factory_reset`** предназначена для сброса роутера на заводские настройки.

После ввода команды необходимо ввести подтверждение операции. Для подтверждения сброса необходимо нажать клавишу «y», для отмены – «n».

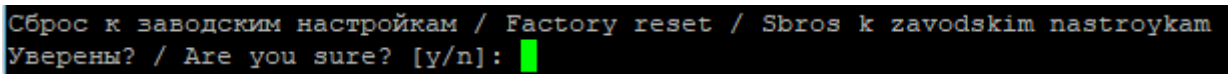


Рисунок В.1 – Текст подтверждения сброса роутера

1.6.2.3 Утилита ifconfig

Команда `ifconfig` предназначена для мониторинга и настройки сетевых интерфейсов. При отладке команда ifconfig позволяет получить информацию о состоянии интерфейса связи. Команда ifconfig является стандартной утилитой Linux.

Примечание При перезагрузке системы все изменения, внесенные в атрибуты интерфейса с помощью команды `ifconfig`, будут потеряны.

1.6.2.3.1 Синтаксис

`ifconfig [-a] [<интерфейс>] [параметры]`

Таблица В.2 – Опции команды ifconfig

Опция	Описание
-a	Данная опция влияет на все проинициализированные сетевые интерфейсы в системе. При использовании без параметров показывает информацию обо всех сетевых интерфейсах, установленных в системе. При использовании с любой из допустимых опций ifconfig, вносимые изменения будут выполняться для всех инициализированных интерфейсов.

Таблица В.3 – Параметры команды ifconfig

Параметры	Описание
up	Включить интерфейс. Данное действие происходит автоматически при установке первого адреса интерфейса.
down	Отключить интерфейс. Если интерфейс помечен как отключенный, устройство перестает пересылать через него сообщения. Данное действие не отключает автоматические маршруты, использующие данный интерфейс.
netmask <маска>	(только **inet**) Задать часть адреса, зарезервированную для деления сетей на подсети.
<адрес>	Задает адрес соответствующего устройства на другом конце при связи типа точка-точка.
broadcast <адрес>	(только **inet**) Задает *адрес*, используемый для посылки широковещательных сообщений в сети.
pointtopoint <адрес>	Включает режим точка-точка интерфейса, что обеспечивает прямую связь между данным устройством и устройством на заданном *адресе* без посторонних слушателей.

dstaddr <адрес>	Задает удаленный IP-адрес для соединения типа точка-точка (например PPP).
metric <NN>	Задает метрику интерфейса.
mtu <NN>	Задает максимальный объём данных, который может быть передан протоколом за одну итерацию (Maximum Transfer Unit, сокр. MTU) для данного интерфейса.
trailers	(только **inet**) Флаг, задающий использование нестандартной инкапсуляции inet пакетов на уровне связи.
arp	Включает использование протокола разрешения адреса (Address Resolution Protocol) при сопоставлении адресов на уровне сети и адресов на уровне связи (используется по умолчанию).
allmulti	Включает/отключает режим all-multicast. Если включено, то все многоадресные пакеты в сети будут приниматься интерфейсом.
multicast	Задает флаг multicast интерфейса. Как правило использование данной опции не требуется, так как данный флаг задается автоматически.
promisc	Включает/отключает «неразборчивый» режим (Promiscuous mode) на данном интерфейсе. Если включено, то интерфейс будет получать все пакеты данных из сети.
txqueuelen <NN>	Задает длину очереди передачи устройства.

Имена интерфейсов:

Интерфейс «внутренней петли» (loopback) роутера имеет имя **lo** и адрес по умолчанию 127.0.0.1.

Имена физических портов роутера имеют имя **ethX**, где X – номер порта роутера, начиная с 0 (LAN1 – eth0, LAN2 – eth1 и т.д.).

Примеры использования:

Отобразить все интерфейсы Ethernet роутера:

```
ifconfig –a
```

Включить интерфейс LAN1 (eth0)

```
ifconfig eth0 up
```

Назначить IP-адрес 192.168.2.1 для интерфейса LAN2 (eth1)

```
ifconfig eth1 192.168.2.1 netmask 255.255.255.0 up
```

1.6.2.4 Утилита ip

Утилита **ip** предназначена для настройки сетевого интерфейса или для отображения текущей конфигурации.

1.6.2.4.1 Синтаксис

```
ip [ <опции> ] <объект> { <команды> | help }
```

Таблица В.4 – Опции утилиты ip

Опция	Описание
-V	Отображение версию утилиты.

-s	Вывести на экран больше информации. Количество повторяющихся опций –s влияет на количество выведенной информации.
-r	Использовать DNS имена вместо адресов хостов.
-f <семейство_прот.>	Задать используемое *семейство протоколов*. На выбор: inet, inet6, bridge, ipx, dnet или link

Таблица В.5 – Объекты утилиты ip

Объект	Описание
link	Задать / отобразить сетевой интерфейс
address	Операция с адресом
route	Значение таблицы маршрутизации
rule	Операции с правилами таблицы маршрутизации
neigh	Управление таблицей соседей/ARP
tunnel	Настройка туннеля IP
maddress	Добавить / изменить / удалить адрес multicast
mroute	Управление кэшем маршрутизации multicast
monitor	Мониторинг состояния сети
xfrm	Управление политиками IPsec (IP Security)

1.6.2.4.2 Пример использования

Отобразить статус работы всех интерфейсов.

ip link show

Отобразить таблицу правил маршрутизации.

ip route list

Создать правило маршрутизации сетей 192.168.3.0/24 через интерфейс eth0.

ip route add 192.168.3.0/24 dev eth0

Создать правило маршрутизации IP-адреса 192.168.3.1 через шлюз 192.168.1.2.

ip route add 192.168.3.1 via 192.168.1.2

Добавить шлюз по умолчанию 192.168.1.2.

ip route add default via 192.168.1.2

1.6.2.5 Утилита iptables

Утилита **iptables** предназначена для управления таблицами маршрутизации и NAT.

1.6.2.5.1 Синтаксис

```
iptables [-t <таблица>] [<опции>]
```

Таблица В.6 – Таблицы утилиты iptables

Таблица	Описание
filter	Таблица по умолчанию. Данная таблица содержит предопределённые цепочки INPUT (для входящих), FORWARD (для перенаправляемых пакетов) и OUTPUT (для исходящих пакетов).

nat	Данная таблица используется для пакетов, устанавливающих новое соединение. В ней содержится три предопределённых цепочки: PREROUTING (для изменения входящих пакетов), OUTPUT (для изменения локально сгенерированных пакетов перед их отправлением) и POSTROUTING (для изменения всех исходящих пакетов).
mangle	Данная таблица используется для специальных изменений пакетов. В ней содержатся цепочки PREROUTING (для изменения входящих пакетов до их перенаправления-маршрутизации), OUTPUT (для изменения локально сгенерированных пакетов перед их маршрутизацией), INPUT (для изменения входящих пакетов), FORWARD (для изменения перенаправляемых пакетов) и POSTROUTING (для изменения исходящих пакетов).
raw	Используется преимущественно для создания исключений в слежении за соединениями совместно с целью NOTRACK. Таблица содержит следующие предопределённые цепочки: PREROUTING (для пакетов приходящих из сетевых интерфейсов) OUTPUT (для пакетов генерируемых локальными процессами)

1.6.2.5.2 Пример использования

Отобразить статус.

```
iptables -L -n -v
```

Отобразить список правил с номерами строк.

```
iptables -n -L -v --line-numbers
```

Отобразить цепочку правил OUTPUT.

```
iptables -L OUTPUT -n -v --line-numbers
```

Удалить все правила.

```
iptables -F
```

Заблокировать все входящие запросы порта 80.

```
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -i emp -p tcp --dport 80 -j DROP
```

1.6.2.6 Команда logread

Команда **logread** предназначена для вывода сообщений кольцевого буфера syslog.

Синтаксис:

```
logread [-f]
```

Таблица В.7 – Опции команды logread

Опция	Описание
-f	Выводить сообщения на экран по мере их появления

1.6.2.6.1 Пример использования

Вывести на экран все сообщения буфа syslog и включить вывод новых сообщений по мере их появления

```
logread -f
```

1.6.2.7 Утилита mstpctl

Утилита **mstpctl** предназначена для конфигурирования MST (Multiple Spanning Tree).

1.6.2.7.1 Синтаксис

```
mstpctl [<команда>]
```

Таблица B.8 – Команды утилиты mstpctl

Команда	Аргументы	Описание
Команды конфигурирования		
createtree	**<мост> <mstid>**	Создать MSTI (multiple spanning-tree instance) с индексом *msid* для *моста*.
deletetree	**<мост> <mstid>**	Удалить MSTI с индексом *msid* для *моста*.
setmaxage	**<мост> <max_age>**	Задать параметр *Max age* для *моста* (20 по умолчанию)
setfdelay	**<мост> <время>**	Задать параметр *время* параметра forward delay для *моста* (15 по умолчанию)
setmaxhops	**<мост> <max_hops>**	Задать параметр *maximum hops* для *моста* (20 по умолчанию)
setforcevers	**<мост> {mstp|rstp|stp}**	Использовать выбранный протокол для *моста* (mstp по умолчанию)
settxholdcount	**<мост> <tx_hold_count>**	Задать параметр *transmit hold count* для *моста*
settreeprio	**<мост> <mstid> <приоритет>**	Задать приоритет моста для дерева с индексом msid. Приоритет – значение между 0 и 15.
setportpathcost	**<мост> <порт> <cost>**	Задать «стоимость» (*cost*) *порта* (0 по умолчанию)
setportadminedge	**<мост> <порт> {yes|no}**	Задать *порт моста* как Edge Port
setportautoedge	**<мост> <порт> {yes|no}**	Включить/отключить автоматическое переключение режима Edge Port для *порта*
setportp2p	**<мост> <порт> {yes|no|auto}**	Включить/отключить режим определения точка-точка (по умолчанию auto)
setportrestrrole	**<мост> <порт> {yes|no}**	Включить/отключить ограничение возможности становиться «корневым» для *порта* (по умолчанию no – без ограничения)
setportrestrtcn	**<мост> <порт> {yes|no}**	Включить/отключить ограничение на распространение полученных оповещений об изменений топологии для *порта* (по умолчанию no – без ограничения)

Команда	Аргументы	Описание
setbpduguard	**<мост> <порт> {yes|no}**	Включить/отключить функцию **BPDU Guard** (функция, которая позволяет выключать порт при получении BPDU) *порта*. (по умолчанию no – выключена)
settreeportprio	**<мост> <порт> <mstid> <приоритет>**	Задать *приоритет порта* в *мосте* для MSTI с индексом *mstid.* Приоритет – значение между 0 и 15.
sethello	**<мост> <время>**	Задать *время* **Hello BPDU** *порта*. (2 по умолчанию)
setageing	**<мост> <время>**	(только STP) Задать время aging-time в секундах (300 по умолчанию)
setportnetwork	**<мост> <порт> {yes|no}**	Включить/отключить функцию **Bridge Assurance** для данного *порта*
Команды отображения		
showbridge	**[<мост>]**	Отобразить информацию о топологии CIST *моста*
showport	**<мост> [<порт>]**	Отобразить краткую информацию о топологии CIST *порта* данного *моста*
showportdetail	**<мост> [<порт>]**	Отобразить детальную информацию о топологии CIST *порта* данного *моста*
showtree	**<мост> <mstid>**	Отобразить информацию о MST с индексом *mstid* для *моста*
showtreeport	**<мост> <порт> <mstid>**	Отобразить детальную информацию о MST с индексом *mstid* для *порта* данного *моста*

1.6.2.8 Утилита netstat

Утилита **netstat** предназначена для отображения информации о сети.

1.6.2.8.1 Синтаксис

```
netstat [<опции>]
```

Таблица В.9 – Опции команды netstat

Опция	Описание
-l [<интерфейс>]	Отобразить сокеты прослушивателя. Сокет - программный интерфейс для обеспечения обмена данными между процессами.
-a	Отобразить все сокеты
-e	Отобразить больше информации
-n	Показывать сетевые адреса как числа.
-r	Отобразить таблицы маршрутизации
-t	Отобразить сокеты TCP

-u	Отобразить сокеты UDP
-w	Отобразить сокеты RAW
-x	Отобразить сокеты UNIX

1.6.2.8.2 Пример использования

Отобразить сокеты TCP.

```
netstat -t
```

1.6.2.9 Команда passwd

Команда **passwd** предназначена для изменения пароля учетной записи.

Пароль может состоять из букв английского алфавита и цифр.

После ввода команды и нажатия клавиши Enter необходимо дважды ввести новый пароль. По завершению в консоли отобразится сообщение о том, что пароль был изменен, как показано на рисунке ниже.

```
root@TOPAZ:~# passwd
Changing password for root
New password:
Retype password:
passwd: password for root changed by root
```

Рисунок В.2.

Примечание При заводских настройках во время авторизации так же появится предупреждение об уязвимости системы по причине отсутствия пароля авторизации, как показано на рисунке 8.

```
=== WARNING! ======================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
```

Рисунок В.3.

1.6.2.10 Команда ping и ping6

Команда **ping (ping6)** предназначена для отправки ICMP эхо-запроса на указанный хост.

1.6.2.10.1 Синтаксис

```
ping [-c <NN>] [-s <размер>] [-q] <хост> [-I <интерфейс>] <интерфейс>
ping6 [-c <NN>] [-s <размер>] [-q] <хост> [-I <интерфейс>] <интерфейс>
```

Таблица В.10 – Опции команды ping (ping6)

Опция	Описание
-c <NN>	Послать *NN* запросов
-s <размер>	Послать объем данных указанного *размера* (по умолчанию 56 байт)
-q	«Тихий режим», выводит на экран информацию во время начала посылки данных и по завершению.
-I <интерфейс>	Выбрать исходящий *интерфейс*

1.6.2.10.2 Пример использования

Отправить IPv4 эхо-запрос в виде одного ICMP пакета размером 500 В на адрес 10.0.0.1.

```
ping -c 1 -s 500 10.0.0.1
```

1.6.2.11 Команда poweroff

Команда **poweroff** предназначена для выключения устройства без снятия питания. Для включения устройства используйте кнопку RB на лицевой панели либо снимите и снова подайте питание на устройство.

1.6.2.11.1 Синтаксис

```
poweroff [-d <задержка>] [-n] [-f]
```

Таблица В.11 – Опции команды poweroff

Опция	Описание
-d <задержка>	Задержка перед выключением (задается в секундах)
-n	Без вызова команды sync
-f	Принудительное выключение (без ожидания завершения работы устройства)

1.6.2.11.2 Пример использования

Выключение роутера.

```
poweroff
```

1.6.2.12 Команда reboot

Команда **reboot** предназначена для перезагрузки роутера.

1.6.2.12.1 Синтаксис

```
reboot [-d <задержка>] [-n] [-f]
```

Таблица В.12 – Опции команды reboot

Опция	Описание
-d <задержка>	Задержка перед перезагрузкой (задается в секундах)
-n	Без вызова команды sync
-f	Принудительная перезагрузка (без ожидания завершения работы устройства)

1.6.2.12.2 Пример использования

Перезагрузка роутера через 5 секунд.

```
reboot -d 5
```

1.6.2.13 Утилита route

Утилита **route** предназначена для отображения и изменения таблиц маршрутизации. Стандартная команда Linux.

1.6.2.13.1 Синтаксис

```
route [-n] [-e] [-A] [{add|del|delete}]
```

Таблица В.13 – Опции команды route

Опция	Описание
-n	Показывать сетевые адреса как числа.
-e	Показать больше информации
-A	Выбрать семейство адресов

1.6.2.13.2 Пример использования

Отобразить таблицы маршрутизации без перевода IP адресов в доменные имена.

route -n

Добавить новый маршрут 192.168.3.0/24 через порт eth1.

route add -net 192.168.3.0/24 dev eth1

Добавить новый маршрут 192.168.3.1 через шлюз 192.168.1.2.

route add -host 192.168.3.1 gw 192.168.1.2

Добавить шлюз по умолчанию 192.168.1.2.

route add default gw 192.168.1.2

1.6.2.14 Утилита service

Утилита `service` предназначена для запуска, перезагрузки и остановки сервисов. Что бы узнать имя сервиса, введите данную команду без аргументов. На экране будет отображен список всех сервисов.

```
root@TOPAZ:~# service
service "" not found, the following services are available:
bird4           dropbear        odhcpd          sysfixtime
bird6           firewall        pstore          sysntpd
boot            gpio_switch     quagga          system
collectd        led             rpcd            uhttpd
cron            log             snmpd           umount
dnsmasq         luci_statistics snmptrapd       urandom_seed
done            network         sysctl
```

Рисунок В.4 – Список запущенных сервисов

1.6.2.14.1 Синтаксис

```
service [<сервис> <команда>]
```

Таблица В.14 – Опции команды service

Команды	Описание
start	Запуск сервиса
stop	Остановка сервиса
restart	Перезапуск сервиса
reload	Обновление конфигурации сервиса (Для применения изменений конфигурации устройства без перерыва в работе)
enable	Разрешить сервис

Команды	Описание
disable	Запретить сервис

1.6.2.14.2 Пример использования

Обновление конфигурации сервиса firewall.

```
service firewall reload
```

1.7 Настройка функций безопасности

1.7.1 Конфигурирование порта управления

Для обеспечения требований безопасности необходимо ограничить возможность удаленного управления устройством по протоколу SSH. Подключение должно быть разрешено только через специально выделенный порт управления, либо отключено. Настройка порта управления осуществляется при помощи утилиты iptables (описание приведено в р. 1.6.2.5)

Пример:

```
#Разрешить входящие соединения по протоколу SSH только на интерфейсе eth0
iptables –A INPUT –I eth0 –p TCP --dport 22 -J ACCEPT
…
…
…
iptables –P INPUT DROP
```

1.7.2 Подсистема регистрации событий безопасности.

Подсистема реализована системной службой syslogd, которая осуществляет журналирование событий, происходящих в системе и сообщений ядра системы, а также поддерживает отправку событий на удаленный сервер по протоколу syslog.

Для настройки отправки событий необходимо указать источник, объем событий и адрес централизованной системы мониторинга. Настройки данных параметров хранятся в конфигурационном файле syslog.conf

Конфигурационный файл **syslog.conf** является главным конфигурационным файлом для службы **syslogd** является конфигурационный файл **syslog.conf**. Файл **syslog.conf** представляет собой **набор правил**. Каждое **правило** представляет из себя строку, состоящую из *селектора* и *действия*, разделенных пробелом или табуляцией. **Селектор** представляет собой запись в виде <*источник*>.<*приоритет*>. (*источник* иногда именуют - *категорией*) **Селектор** может состоять из нескольких записей <*источник*>.<*приоритет*>, разделенных символом ";" . Можно указывать несколько источников в одном селекторе (через запятую). Поле **действие** - устанавливает журналируемое действие для селектора.

Сообщения, предназначенные для записи в журнал, проверяются на соответствие шаблонам определяемым селектором. Если соответствует, то выполняется указанное в правиле действие.

Сообщения с уровнем, *равным* или *выше* указанного в селекторе, и источником, *равным указанному* в селекторе, считается *подходящим*. **Звездочка перед** точкой соответствует *любому источнику*, **после** точки - *любому уровню*. Слово **none** после точки - никакому уровню для данного источника. Можно указывать несколько источников в одном селекторе (через запятую).

Источник (категория) может быть следующим:

- 0 - **kern** - Сообщения ядра
- 1 - **user** - Сообщения пользовательских программ
- 2 - **mail** - Сообщения от почтовой системы.
- 3 - **daemon** - Сообщения от тех системных служб, не имеющих категорий.
- 4 - **auth** – Сообщения, связанные с авторизацией пользователей (безопасность/права доступа: login, su и т.д.)
- 5 - **syslog** – Сообщения системы протоколирования.
- 6 - **lpr** - Сообщения от системы печати.
- 7 - **news** - Сообщения от сервера новостей (не используется).
- 8 - **uucp** - Сообщения от UNIX-to-UNIX Copy Protocol (не используется).
- 9 - **cron** - Сообщения от системного планировщика.
- 10 - **authpriv** - Сообщения, связанные с авторизацией пользователей, доступные только определенным пользователям.
- 11 - **ftp** - Сообщения FTP сервера.
- 12 - **NTP** - сообщения сервера времени
- 13 - **log audit**
- 14 - **log alert**
- 15 - **clock daemon -** сообщения службы времени
- с 16 по 23 **local0 - local7** Зарезервированные категории для использования администратором системы. Категория local7 обычно используется для сообщений, генерируемых на этапе загрузки системы.
- **mark** (не имеющая цифрового эквивалента) - присваивается отдельным сообщениям, формируемым самим сервисом syslogd

Приоритет (степени важности) сообщений имеет 8 уровней, которые кодируются числами от 0 до 7:

- 0 - **emerg** (старое название **PANIC**) - Чрезвычайная ситуация. Система неработоспособна.
- 1 - **alert -** Тревога! Требуется немедленное вмешательство.
- 2 - **crit -** Критическая ошибка (критическое состояние).
- 3 - **err** (старое название **ERROR**) - Сообщение об ошибке.
- 4 - **warning** (старое название **WARN**) - Предупреждение.
- 5 - **notice -** Информация о каком-то нормальном, но важном событии.

- 6 - **info -** Информационное сообщение.
- 7 - **debug -** Сообщения, формируемые в процессе отладки.

Согласно **действию,** указанному в правиле, сообщение может быть записано в следующие назначения:

Обычный файл

Задается полным путем, начиная со слеша (/).

Удаленная машина

Для отправки сообщений на другой хост, необходимо перед адресатом добавить символ @.

```
# Пример конфигурационного файла syslogd.
# Все сообщения перенаправляются на
# удалённую сетевую машину.
*.*         @192.168.10.10
```

1.7.3 Подсистема проверки целостности

Проверка целостности системных файлов осуществляется автоматически с периодичностью раз в сутки утилитой afick. Ручной контроль целостности осуществляется посредством команды afick с ключом -k.

На этапах ввода системы в опытную, промышленную эксплуатацию необходимо пересоздать базу данных с контрольными суммами файлов и настроить отправку данных на централизованный сервер мониторинга событий безопасности (в случае необходимости).

1.7.3.1 Утилита afick

Afick — утилита, помогающая при обнаружении вторжений, а также позволяющая контролировать общую целостность системы.

Afick контролирует изменения в файловой системе и сразу сообщает вам о них, таким образом, предоставляя вам выбор решить, действительно ли ожидались эти изменения. Эта информация может помочь вам в расследовании инцидента, когда необходимо определить, какие были произведены изменения в системе в результате взлома.

В процессе установки Afick формирует базу данных файлов, каталогов и соответствующих им MD5 контрольных сумм. Файлы и каталоги, включенные в эту базу данных, выбираются соответственно входным данным из файла конфигурации Afick, называемого **afick.conf**, после того, как Afick установит этот файл в /etc каталог. Файл конфигурации afick.conf имеет простую синтаксическую структуру. По вашему усмотрению Вы можете очень быстро добавить или удалить типы файлов, каталоги, и т.д. Ниже приведено содержимое файла afick.conf. Обратите внимание, что элементы в файле конфигурации чувствительны к регистру.

```
# afick config sample file
# directives
#############
database:=/var/lib/afick/afick - Определяет какую базу данных будет использовать Afick
# report_url := stdout - Определяет куда Afick будет выводить результаты своей работы
# verbose := no
# warn_dead_symlinks := no
```

```
# report_full_newdel := no

# warn_missing_file := no

# running_files := no

# timing := no

# text files
```

exclude_suffix := log LOG html htm HTM txt TXT xml - Определяет, что Afick должен игнорировать текстовые файлы с такими расширениями.

```
# help files
```

exclude_suffix := hlp pod chm - Определяет, что Afick должен игнорировать файлы справки с такими расширениями

```
# old files
```

exclude_suffix := tmp old bak - Определяет, что Afick должен игнорировать временные файлы с такими расширениями

```
# fonts
```

exclude_suffix := fon ttf TTF - Определяет, что Afick должен игнорировать файлы шрифтов с такими расширениями

```
# images
```

exclude_suffix := bmp BMP jpg JPG gif png ico - Определяет, что Afick должен игнорировать файлы изображений с такими расширениями

```
# audio
```

exclude_suffix := wav WAV mp3 avi - Определяет, что Afick должен игнорировать медиа файлы с такими расширениями

```
# macros

########

# used by cron
```

@@define MAILTO root - Определяет пользователя, которому будут отсылаться отчеты по работе Afick.

@@define LINES 1000 - Определяет максимальное количество строк в отчете

```
# list the file or directories to scan

# syntaxe :

# file action

# to have action on file (see below

# ! file

# to remove file from scan

# file with blank character have to be quoted
```

 # action : a list of item to check - Ниже описаны опции, определяющие какие атрибуты файлов нужно контролировать.

```
# md5 : md5 checksum

# d : device

# i : inode
```

```
# p : permissions
# n : number of links
# u : user
# g : group
# s : size
# b : number of blocks
# m : mtime
# c : ctime
# a : atime
#R: p+d+i+n+u+g+s+m+c+md5
#L: p+d+i+n+u+g
# action alias may be configured with
# your_alias = another_alias|item[+item][-item]
# all is a pre-defined alias for all items except "a"
# alias :
#########
DIR = p+i+n+u+g
ETC = p+d+i+u+g+s+md5
Logs = p+n+u+
MyRule = p+d+i+n+u+g+s+b+md5+m .
# files to scan
###############
=/ DIR - Проверка с использованием описанных выше правил для каталогов
#
/bin MyRule
/boot MyRule
!/boot/map - Игнорируется указанный каталог.
!/boot/System.map - Игнорируется указанный файл
/etc ETC
/etc/mtab ETC - i
/etc/adjtime ETC - md5
/etc/aliases.db ETC - md5
/etc/mail/statistics ETC - md5
!/etc/map
!/etc/webmin/sysstats/modules/
!/etc/cups/certs/0
/lib MyRule
```

```
/lib/modules MyRule -m
/root MyRule
!/root/.viminfo
!/root/.bash_history
!/root/.mc
/sbin MyRule
/usr/bin MyRule
/usr/sbin MyRule
/usr/lib MyRule
/usr/local/bin MyRule
/usr/local/sbin MyRule
/usr/local/lib MyRule
/var/ftp MyRule
/var/log Logs
/var/www MyRule
```

1.7.3.2 Пример использования

В данном разделе приведен пример, в котором к проверке целостности Afick добавляется основной каталог системы. К примеру, если необходимо, чтобы файлы в основном каталоге проверялись на изменения при монопольном доступе, изменение прав доступа, изменения размера файлов и времени последнего обращения к файлу.

Для начала нужно создать новый элемент, под разделом **#alias** в файле конфигурации afick.conf, как показано ниже:

```
HOME = u+g+p+m+s
```

Затем в разделе **#files to scan** необходимо добавить следующую строку:

```
/home/yourusername HOME
```

Теперь, при следующем запуске, Afick добавит данный каталог в свою базу данных и будет контролировать находящиеся в нем файлы, согласно заданным критериям. Если нужно, чтобы изменения применились немедленно, то можно запустить Afick вручную, используя следующую команду:

```
Afick -- update
```

Иначе придется ждать запуска крон задачи Afick. Эта задача добавляется автоматически во время инсталляции программы и запускается один раз в день. Результаты работы данного задания будет получен по электронной почте на адрес, указанный в разделе **MAILTO** файла конфигурации **afick.conf**. Используя почтового клиента, можно будет увидеть ежедневный отчет приблизительно в следующем виде:

```
This is an automated report generated by Another File Integrity Checker on
+localhost.localdomain at 07:46:07 AM on 02/25/2004.
Output of the daily afick run:
```

```
new file : /var/log/afick/afick.log.2
new file : /var/log/afick/error.log.2
deleted file : /etc/sysconfig/iptables
changed file : /etc/adjtime
changed file : /etc/aliases.db
changed file : /etc/mail/statistics
changed file : /etc/prelink.cache
changed file : /etc/printcap
detailed changes
changed file : /etc/adjtime
MD5 : 7+bTDZQbxsTXEJXhyI2GCw ao6a/yDwoBR8GSL1AKlWXQ
changed file : /etc/aliases.db
MD5 :GT/eP5D+B8apNoa7L5CLRw soh7MnLDuQw4gI9KHlhpTA
changed file : /etc/mail/statistics
MD5 :oshq17jZ2a0o5pYhVBRgwQ vb69gMWXvpIEEZ4fmOl9/Q
changed file : /etc/prelink.cache
MD5 : SKh/403FRMUqBNdCIInQ9A zeC+5EPFfWBR4OeT7xZdbw
changed file : /etc/printcap
MD5 : b5e3g2//bGaxeCxVyRJqaw QFY1NJGy/kdt32B1YV0TXQ
filesize : 194 581
```

В примере выше Afick сообщает, что некоторые файлы были изменены, созданы или удалены. Также показаны начальные и текущие контрольные суммы файлов, и сообщается, что в одном из файлов был изменен его размер. Afick проконтролирует наличие изменений в файле, сравнивая его атрибуты с атрибутами, которые были сохранены при последнем запуске Afick. Примером этого могут служить файлы в папке **/usr/bin** или в **/sbin**. Как правило эти файлы изменяются не часто, если только их не изменили, обновляя программу (в противном случае они не останутся неизменны).

Следует обратить внимание на то, где сохраняется вашу базу данных Afick (по умолчанию — **/var/lib/afick/**), так как возможно возникновение ситуации, когда система была взломана, ну это не было зафиксировано, так как была нарушена целостность базы данных. Возможным решением данного вопроса может быть сохранение базы на защищенных от записи носителях (например, CD-ROM), после чего изменить файл конфигурации afick.conf, чтобы указать на выбранное вами место сохранения базы.

1.7.3.3 Проведение процедуры контроля целостности ОС

Для **сертифицированной редакции** в состав репозитория ОС включена база данных утилиты контроля целостности afick, которая содержит перечень контролируемых бинарных исполняемых файлов изделия, согласно документации на изделие. Для самостоятельной проверки целостности ОС необходимо сделать следующее:

1. Запустить проверку файлов ОС командой:

```
# afick -k
```

```
...
new file : /var/lib/afick/redos/redos.ctr
new file : /var/lib/afick/redos/redos.db
deleted file : /lib/modules/4.19.79-1.el7.x86_64.debug/kernel/arch/x86/crypto/aegis128-aesni.ko
...
deleted file : /var/lib/afick/afick.db
        parent_date               : Fri Apr 24 09:17:05 2020
changed file : /etc/afick.conf
        md5                       : 03bf42d0327b3f2fe195d0eca359b1ec       addfc78d9551417
18f78df7587ae3ceb
        filemode                  : 100600        100644
        filesize                  : 924772        924774
# Hash database : 6793 files scanned, 6320 changed (new : 2; delete : 6317; changed : 1; dangling : 0; exclude_suffix : 0; exclude_prefix : 0; exclude_re : 0; degraded : 3)
# ###################################################################
# MD5 hash of /var/lib/afick/redos/redos => oRTAm4SAHdk9vwSktXz88A
# user time : 12.73; system time : 3.14; real time : 27
```

2. После завершения проверки проанализировать полученные данные. Новые файлы можно не принимать во внимание.

```
new : 2
```

Удалённые файлы в отчете можно не учитывать — это объясняется тем, что БД afick снимается для всех контролируемых файлов, а в используемом экземпляре ОС могут использоваться не все пакеты.

```
delete : 6317
```

Интерес в первую очередь представляют изменённые файлы.

```
changed : 1
```

3. Проанализировать подробный отчёт в выводе утилиты выше и оценить, допустимы ли данные изменения файлов.

```
changed file : /etc/afick.conf
        md5                       : 03bf42d0327b3f2fe195d0eca359b1ec       addfc78d9551417
18f78df7587ae3ceb
        filemode                  : 100600        100644
        filesize                  : 924772        924774
```

В приведенном примере был изменен конфигурационный файл утилиты afick. Это считается допустимым изменением, так как на эталонной ОС конфигурация afick по умолчанию не настроена. Скачанный конфигурационный файл, содержащийся в

пакете БД afick, заменил файл, поставляемый с утилитой. Других изменений в системе нет, значит, можно сделать вывод о целостности ОС.

1.7.4 Подсистема криптозащиты каналов связи

Устройство поддерживает следующие решения: Infotecs ViPNet VPN, ТСС Diamond VPN, Код Безопасности Континент АП VPN, OpenVPN, IPSec, PPTP VPN.

Настройка СКЗИ Infotecs ViPNet VPN, ТСС Diamond VPN, Код Безопасности Континент АП VPN, осуществляется согласно инструкции производителя СКЗИ.

1.7.5 Подсистема аудита

В устройстве реализована подсистема аудита, которая позволяет осуществлять аудит:

- запуск и завершение работы системы;
- чтение, запись и изменение прав доступа к файлам;
- инициация сетевых соединений;
- попытки неудачной авторизации в системе;
- изменение сетевых настроек;
- изменение информации о пользователях и группах;
- запуск и остановка приложений;
- выполнение системных вызовов

Подсистема реализована на базе сервиса **auditd**. Просмотр результатов аудита осуществляется утилитами:

- **aureport** - инструмент для генерации итоговых отчетов на основе логов демона аудита;
- **ausearch** - поиск по журналу аудита;
- **auditctl** - инструмент для управления аудитом, предоставляемого Linux ядром.

1.7.5.1 Сервис auditd

1.7.5.1.1 Описание

auditd - это прикладной компонент системы аудита Linux. Он ведёт протокол аудита на диске. Для просмотра протоколов предназначены команды **ausearch** и **aureport.** Команда **auditctl** позволяет настраивать правила аудита. Кроме того, при загрузке загружаются правила из файла */etc/audit.rules*. Некоторые параметры самого демона можно изменить в файле **auditd.conf.**

1.7.5.1.2 Синтаксис

auditd [**-f**] [**-l**] [**-n**]

Таблица 13 – Опции сервиса auditd

Опция	Описание
-f	Не переходить в фоновый режим (для отладки). Сообщения программы будут направляться в стандартный вывод для ошибок (stderr), а не в файл.
-l	Включить следование по символическим ссылкам при поиске конфигурационных файлов.

-n	Не создавать дочерний процесс. Для запуска из inittab

1.7.5.1.3 Сигналы

Таблица 14 – Сигналы сервиса auditd

Опция	Описание
SIGHUP	перезагрузить конфигурацию - загрузить файл конфигурации с диска. Если в файле не окажется синтаксических ошибок, внесенные в него изменения вступят в силу. При этом в протокол будет добавлена запись о событии DAEMON_CONFIG. В противном случае действия службы будут зависеть от параметров space_left_action, admin_space_left_action, disk_full_action, disk_error_action файла auditd.conf.
SIGTERM	прекратить обработку событий аудита и завершить работу, о чём предварительно занести запись в протокол.
SIGUSR1	создать новый файл для протокола, перенумеровав старые файлы или удалив часть из них, в зависимости от параметра max_log_size_action.

1.7.5.1.4 Файлы

/etc/audit/auditd.conf - файл конфигурации демона аудита **/etc/audit/audit.rules** - правила аудита (загружается при запуске службы)

1.7.5.2 Утилита ausearch

Программа **ausearch** является инструментом поиска по журналу аудита. **ausearch** может также принимать данные со стандартного ввода (stdin) до тех пор, пока на входе будут необработанные данные логов. Все условия, указанные в параметрах, объединяются логическим И. К примеру, при указании **-m** и **-ui** в качестве параметров будут показаны события, соответствующие заданному типу и идентификатору пользователя.

1.7.5.2.1 Синтаксис

ausearch [опции]

1.7.5.2.2 Сигналы

Таблица 15 – Сигналы сервиса ausearch

Опция	Описание
-a, **--event** *audit-event-id*	Искать события с заданным *идентификатором события*. Сообщения обычно начинаются примерно так: msg=audit(1116360555.329:2401771). Идентификатор события - это число после ':'. Все события аудита, связанные с одним системным вызовом имеют одинаковый идентификатор.
-c, **--comm** *comm-name*	Искать события с заданным *comm name*. comm name - имя исполняемого файла задачи.

-f, **--file** *file-name*	Искать события с заданным *именем файла*.
-ga, **--gid-all** *all-group-id*	Искать события с заданным эффективным или обычным *идентификатором группы*.
-ge, **--gid-effective** *effective-group-id*	Искать события с заданным *эффективным идентификатором группы* или именем группы.
-gi, **--gid** *group-id*	Искать события с заданным *идентификатором группы* или именем группы.
-h, **--help**	Справка
-hn, **--host** *host-name*	Искать события с заданным *именем узла*. Имя узла может быть именем узла, полным доменным именем или цифровым сетевым адресом.
-i, **--interpret**	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет оттранслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущен **ausearch**. Т.е. если вы переименовали учетные записи пользователей или не имеете таких же учетных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение.
-if, **--input** *file-name*	Использовать указанный *файл* вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
-k, **--key** *key-string*	Искать события с заданным *ключевым словом*.
-m, **--message** *message-type | comma-sep-message-type-list*	Искать события с заданным *типом*. Вы можете указать *список значений, разделенных запятыми*. Можно указать несуществующий в событиях тип **ALL**, который позволяет получить все сообщения системы аудита. Список допустимых типов большой и будет показан, если указать эту опцию без значения. Тип сообщения может быть строкой или числом. В списке значений этого параметра в качестве разделителя используются запятые и пробелы недопустимы.
-o, **--object** *SE-Linux-context-string*	Искать события с заданным *контекстом* (объектом).
-p, **--pid** *process-id*	Искать события с заданным *идентификатором процесса*.
-pp, **--ppid** *parent-process-id*	Искать события с заданным *идентификатором родительского процесса*.
-r, **--raw**	Необработанный вывод. Используется для извлечения записей для дальнейшего анализа.
-sc, **--success** *syscall-name-or-value*	Искать события с заданным *системным вызовом*. Вы можете указать его номер или имя. Если вы указали имя, оно будет проверено на машине, где запущен **ausearch**.
-se, **--context** *SE-Linux-context-string*	Искать события с заданным *контекстом SELinux* (stcontext/subject или *tcontext*/object).

-su, **--subject** *SE-Linux-context-string*	Искать события с заданным контекстом SELinux - *scontext* (subject).
-sv, **--success** *success-value*	Искать события с заданным *флагом успешного выполнения*. Допустимые значения: **yes (успешно)** и **no**(неудачно).
-te, **--end** [*end-date*] [*end-time*]	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (**today**). Если не указано время, то подразумевается текущий момент (**now**). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: **now** (сейчас), **recent**, **today**, **yesterday**, **this-week**, **this-month**, **this-year**. **today** означает первую секунду после полуночи текущего дня. **recent** - 10 минут назад. **yesterday** - первую секунду после полуночи предыдущего дня. **this-week** означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. **localtime**). **this-month** означает первую секунду после полуночи первого числа текущего месяца. **this-year** означает первую секунду после полуночи первого числа первого месяца текущего года.
-ts, **--start** [*start-date*] [*start-time*]	Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (**today**). Если не указано время, то подразумевается полночь (**midnight**). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: **now** (сейчас), **recent**, **today**, **yesterday**, **this-week**, **this-month**, **this-year**. **today** означает первую секунду после полуночи текущего дня. **recent** - 10 минут назад. **yesterday** - первую секунду после полуночи предыдущего дня. **this-week** означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. **localtime**). **this-month** означает первую секунду после полуночи первого числа текущего месяца. **this-year** означает первую секунду после полуночи первого числа первого месяца текущего года.
-tm, **--terminal** *terminal*	Искать события с заданным *терминалом*. Некоторые демоны (такие как cron и atd) используют имя демона как имя терминала.
-ua, **--uid-all** *all-user-id*	Искать события, у которых любой из идентификатора пользователя, эффективного идентификатора пользователя

	или loginuid (auid) совпадают с заданным *идентификатором пользователя*.
-ue, **--uid-effective** *effective-user-id*	Искать события с заданным *эффективным идентификатором пользователя*.
-ui, **--uid** *user-id*	Искать события с заданным *идентификатором пользователя*.
-ul, **--loginuid** *login-id*	Искать события с заданным *идентификатором пользователя*. Все программы, которые его используют, должны использовать pam_loginuid.
-v, **--verbose**	Показать версию и выйти
-w, **--word**	Совпадение с полным словом. Поддерживается для имени файла, имени узла, терминала и контекста SELinux.
-x, **--executable** *executable*	Искать события с заданным *именем исполняемой программы*.

1.7.5.3 Утилита aureport

aureport - это инструмент, который генерирует итоговые отчеты на основе логов демона аудита. **aureport** может также принимать данные со стандартного ввода (stdin) до тех пор, пока на входе будут необработанные данные логов. В шапке каждого отчета для каждого столбца есть заголовок - это облегчает понимание данных. Все отчеты, кроме основного итогового отчета, содержат номера событий аудита. Используя их, вы можете найти полные данные о событии с помощью **ausearch -a** *номер события*. Если в отчете слишком много данных, можно задать время начала и время окончания для уточнения временного промежутка. Отчеты, генерируемые **aureport**, могут быть использованы как исходный материал для получения более развернутых отчетов.

1.7.5.3.1 Синтаксис

aureport [*опции*]

1.7.5.3.2 Сигналы

Таблица 16 – Сигналы сервиса aureport

Опция	Описание
-au, **--auth**	Отчет о всех попытках аутентификации
-a, **--avc**	Отчет о всех avc сообщениях
-c, **--config**	Отчет о изменениях конфигурации
-cr, **--crypto**	Отчет о событиях, связанных с шифрованием
-e, **--event**	Отчет о событиях
-f, **--file**	Отчет о файлах
--failed	Для обработки в отчетах выбирать только неудачные события. По умолчанию показываются и удачные и неудачные события.
-h, **--host**	Отчет о хостах

Опция	Описание
-i, **--interpret**	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет оттранслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущен **aureport**. Т.е. если вы переименовали учетные записи пользователей или не имеете таких же учетных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение.
-if, **--input** *файл*	Использовать указанный *файл* вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
-l, **--login**	Отчет о попытках входа в систему
-m, **--mods**	Отчет об изменениях пользовательских учетных записей.
-ma, **--mac**	Отчет о событиях в системе обеспечивающей мандатное управление доступом - Mandatory Access Control (MAC).
-p, **--pid**	Отчет о процессах
-r, **--response**	Отчет о реакциях на аномальные события
-s, **--syscall**	Отчеты о системных вызовах
--success	Для обработки в отчетах выбирать только удачные события. По умолчанию показываются и удачные и неудачные события.
--summary	Генерировать итоговый отчет, который дает информацию только о количестве элементов в том или ином отчете. Такой режим есть не у всех отчетов.
-t, **--log**	Этот параметр генерирует отчет о временных рамках каждого отчета.
-te, **--end** [*дата*] [*время*]	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (**today**). Если не указано время, то подразумевается текущий момент (**now**). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: **now** (сейчас), **recent**, **today**, **yesterday**, **this-week**, **this-month**, **this-year**. **today** означает первую секунду после полуночи текущего дня. **recent** - 10 минут назад. **yesterday** - первую секунду после полуночи предыдущего дня. **this-week** означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. **localtime**). **this-month** означает первую секунду после полуночи первого числа текущего месяца. **this-year** означает первую секунду после полуночи первого числа первого месяца текущего года.

Опция	Описание
-tm, **--terminal**	Отчет о терминалах
-ts, **--start** [*дата*] [*время*]	Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (**today**). Если не указано время, то подразумевается полночь (**midnight**). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: **now** (сейчас), **recent**, **today**, **yesterday**, **this-week**, **this-month**, **this-year**. **today** означает первую секунду после полуночи текущего дня. **recent** - 10 минут назад. **yesterday** - первую секунду после полуночи предыдущего дня. **this-week** означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. **localtime**). **this-month** означает первую секунду после полуночи первого числа текущего месяца. **this-year** означает первую секунду после полуночи первого числа первого месяца текущего года.
-u, **--user**	Отчет о пользователях
-v, **--version**	Вывести версию программы и выйти
-x, **--executable**	Отчет о исполняемых объектах

1.7.5.4 Утилита auditctl

auditctl используется для контроля поведения, получения состояния и добавления/удаления правил аудита, предоставляемого Linux ядром версии 2.6.

1.7.5.4.1 Синтаксис

auditctl [*опции*]

1.7.5.4.2 Сигналы

Таблица 17 – Сигналы сервиса auditctl

Опция	Описание
-b *backlog*	Установить максимальное количество доступных для аудита буферов, ожидающих обработки (значение в ядре по умолчанию - 64). Если все буфера заняты, то флаг сбоя будет выставлен ядром для его дальнейшей обработки.
-e [**0**..**2**]	Установить флаг блокировки. **0** позволит на время отключить аудит, включить его обратно можно, передав **1** как параметр. Если установлено значение опции **2**, то защитить конфигурацию аудита от изменений. Каждый, кто захочет воспользоваться этой возможностью, может поставить эту команду последней в audit.rules. После этой команды все

Опция	Описание
	попытки изменить конфигурацию будут отвергнуты с уведомлением в журналах аудита. В этом случае, чтобы задействовать новую конфигурацию аудита, необходимо перезагрузить систему аудита.
-f [**0**..**2**]	Установить способ обработки для флага сбоя. **0**=silent **1**=printk **2**=panic. Эта опция позволяет определить каким образом ядро будет обрабатывать критические ошибки. Например, флаг сбоя выставляется при следующих условиях: ошибки передачи в пространство демона аудита, превышение лимита буферов, ожидающих обработки, выход за пределы памяти ядра, превышение лимита скорости выдачи сообщений. Значение по умолчанию: **1**. Для систем с повышенными требованиями к безопасности, значение **2** может быть более предпочтительно.
-h	Краткая помощь по аргументам командной строки.
-i	Игнорировать ошибки при чтении правил из файла.
-l	Вывести список всех правил по одному правилу в строке.
-k *ключ*	Установить на правило ключ фильтрации. Ключ фильтрации - это произвольная текстовая строка длиной не больше 31 символа. Ключ помогает уникально идентифицировать записи, генерируемые в хода аудита за точкой наблюдения.
-m *текст*	Послать в систему аудита пользовательское сообщение. Это может быть сделано только из-под учетной записи root.
-p [**r**|**w**|**x**|**a**]	Установить фильтр прав доступа для точки наблюдения. **r**=чтение, **w**=запись, **x**=исполнение, **a**=изменение атрибута. Не путайте эти права доступа с обычными правами доступа к файлу - они определяют типы системных вызовов, которые выполняют данные действия. Заметьте, системные вызовы read и write не включены в этот набор, поскольку логи аудита были бы перегружены информацией о работе этих вызовов.
-r *частота*	Установить ограничение скорости выдачи сообщений в секунду (**0** - нет ограничения). Если эта *частота* не нулевая и она превышается в ходе аудита, флаг сбоя выставляется ядром для выполнения соответствующего действия. Значение по умолчанию: 0.
-R *файл*	Читать правила из *файла*. Правила должны быть расположены по одному в строке и в том порядке, в каком они должны исполняться. Следующие ограничения накладываются на файл: владельцем должен быть root и доступ на чтение должен быть только у него. Файл может содержать комментарии, начинающиеся с символа '#'. Правила, расположенные в файле, идентичны тем, что набираются в командной строке, без указания 'auditctl'.
-s	Получить статус аудита.

Опция	Описание
-a *список*,*действие*	Добавить правило с указанным *действием* к концу *списка*. Заметьте, что запятая разделяет эти два значения. Отсутствие запятой вызовет ошибку. Ниже описаны имена доступных списков:
task	Добавить правило к списку, отвечающему за процессы. Этот список правил используется только во время создания процесса - когда родительский процесс вызывает fork() или clone(). При использовании этого списка вы можете использовать только те поля, которые известны во время создания процесса: uid, gid и т.д.
entry	Добавить правило к списку, отвечающему за точки входа системных вызовов. Этот список применяется когда необходимо создать событие для аудита, привязанное к точкам входа системных вызовов.
exit	Добавить правило к списку, отвечающему за точки выхода из системных вызовов. Этот список применяется когда необходимо создать событие для аудита, привязанное к точкам выхода из системных вызовов.
user	Добавить правило, отвечающего за список фильтрации пользовательских сообщений. Этот список используется ядром, чтобы отфильтровать события приходящие из пользовательского пространства, перед тем как они будут переданы демону аудита. Необходимо отметить, что только следующие поля могут быть использованы: uid, auid, gid и pid. Все остальные поля будут обработаны, как если бы они не совпали.
exclude	Добавить правило к списку, отвечающего за фильтрацию событий определенного типа. Этот список используется, чтобы отфильтровывать ненужные события. Например, если вы не хотите видеть avc сообщения, вы должны использовать этот список. Тип сообщения задается в поле msgtype. Ниже описаны доступные *действия* для правил:
never	Аудит не будет генерировать никаких записей. Это может быть использовано для подавления генерации событий. Обычно необходимо подавлять генерацию в верху списка, а не внизу, т.к. событие инициируется на первом совпавшем правиле.
always	Установить контекст аудита. Всегда заполнять его во время входа в системный вызов, и всегда генерировать запись во время выхода из системного вызова.
-A *список*,*действие*	Добавить правило с указанным *действием* в начало *списка*.
-d *список*,*действие*	Удалить правило с указанным *действием* из *списка*. Правило удаляется только в том случае, если полностью совпали и имя системного вызова и поля сравнения.

Опция	Описание
-D	Удалить все правила и точки наблюдения.
-S [*Имя или номер системного вызова*|**all**]	Любой *номер* или *имя* системного вызова может быть использован. Также возможно использование ключевого слова *all*. Если какой-либо процесс выполняет указанный системный вызов, то аудит генерирует соответствующую запись. Если значения полей сравнения заданы, а системный вызов не указан, правило будет применяться ко всем системным вызовам. В одном правиле может быть задано несколько системных вызовов - это положительно сказывается на производительности, поскольку заменяет обработку нескольких правил.
-F [*n*=*v* | *n***!**=*v* | *n*<*v* | *n*>*v* | *n*<=*v* | *n*>=*v* | *n***&***v* | *n***&**=*v*]	Задать поле сравнения для правила. Атрибуты поля следующие: объект, операция, значение. Вы можете задать до 64 полей сравнения в одной команде. Каждое новое поле должно начинаться с **-F**. Аудит будет генерировать запись, если произошло совпадение по всем полями сравнения. Допустимо использование одного из следующих 8 операторов: равно, не равно, меньше, больше, меньше либо равно, больше либо равно, битовая маска (*n***&***v*) и битовая проверка (*n***&**=*v*). Битовая проверка выполняет операцию 'and' над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию 'and'. Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя - программа автоматически получит идентификатор пользователя из его имени. То же самое можно сказать и про имя группы. Поля сравнения могут быть заданы для следующих объектов:
a0, a1, a2, a3	Четыре первых аргумента, переданных системному вызову. Строковые аргументы не поддерживаются. Это связано с тем, что ядро должно получать указатель на строку, а проверка поля по значению адреса указателя не желательна. Таким образом, вы должны использовать только цифровые значения.
arch	Архитектура процессора, на котором выполняется системный вызов. Используйте 'uname -m', чтобы определить архитектуру. Если вы не знаете архитектуру вашей машины, но хотите использовать таблицу 32-х битных системных вызовов, и ваша машина поддерживает 32 бита, вы можете использовать **b32**. Подобно этому **b64** может быть использовано для использования таблицы 64-х битных системных вызовов.
auid	Это аббревиатура: audit uid - идентификатор пользователя, использованный для входа в систему.
devmajor	Главный номер устройства (Device Major Number)
devminor	Вспомогательный номер устройства (Device Minor Number)

Опция	Описание
egid	Действительный идентификатор группы
euid	Действительный идентификатор пользователя
exit	Значение, возвращаемое системным вызовом при выходе.
fsgid	Идентификатор группы, применяемый к файловой системе.
fsuid	Идентификатор пользователя, применяемый к файловой системе.
gid	Идентификатор группы
Идентификатор группы	**inode**
inode	Номер inode
key	Альтернативный способ установить ключ фильтрации. Смотри выше описание опции **-k**.
msgtype	Используется для проверки совпадения с числом, описывающим тип сообщения. Может быть использован только в списке **exclude**.
obj_user	Имя пользователя-владельца ресурса (в контексте SELinux)
obj_role	Роль ресурса (в контексте SELinux)
obj_type	Тип ресурса (в контексте SELinux)
obj_lev_low	Нижний уровень ресурса (в контексте SELinux)
obj_lev_high	Верхний уровень ресурса (в контексте SELinux)
path	Полный путь к файлу для точки наблюдения. Смотри ниже описание опции "**-w**". Может быть использован только в списке **exit**.
perm	Фильтр прав доступа для файловых операций. Смотри выше описание опции "**-p**". Может быть использован только в списке **exit**.
pers	Персональный номер операционной системы.
pid	Идентификатор процесса
ppid	Идентификатор родительского процесса.
subj_user	Имя пользователя-владельца процесса (в контексте SELinux)
subj_role	Роль процесса (в контексте SELinux)
subj_type	Тип процесса (в контексте SELinux)
subj_sen	Чувствительность процесса (в контексте SELinux)
subj_clr	Допуск процесса (в контексте SELinux)
sgid	Установленный идентификатор группы
success	Если значение, возвращаемое системным вызовом, больше либо равно 0, данный объект будет равен "true/yes", иначе "false/no". При создании правила используйте 1 вместо "true/yes" и 0 вместо "false/no".

Опция	Описание
suid	Установленный идентификатор пользователя
uid	Идентификатор пользователя
-w *путь*	Добавить точку наблюдения за файловым объектом, находящемуся по указанному *пути*. Вы не можете добавлять точку наблюдения к каталогу верхнего уровня - это запрещено ядром. Групповые символы (wildcards) также не могут быть использованы, попытки их использования будут генерировать предупреждающее сообщение. Внутренне точки наблюдения реализованы как слежение за inode. Таким образом, если вы установите точку наблюдения за каталогом, вы увидите файловые события, которые в действительности будут означать обновления метаданных этой inode, и вы можете не увидеть событий, непосредственно связанных с файлами. Если вам необходимо следить за всеми файлами в каталоге, рекомендуется создавать индивидуальную точку наблюдения для каждого файла. В противоположность к правилам аудита системных вызовов, точки наблюдения не оказывают влияния на производительность, связанную с количеством правил, посылаемых в ядро.
-W *путь*	Удалить точку наблюдения за файловым объектом, находящемуся по указанному *пути*.

1.7.5.4.3 Примеры использования для контроля поведения, получения состояния

Чтобы увидеть все системные вызовы, используемые определенным процессом:

auditctl -a entry,always -S all -F pid=1005

Чтобы увидеть все файлы, открытые определенным пользователем:

auditctl -a exit,always -S open -F auid=510

Чтобы увидеть неудачные попытки вызова системной функции 'open':

auditctl -a exit,always -S open -F success!=0

1.7.5.4.4 Создание правил

Список опций команды auditctl для создания правил (подробное описание опций приведено в таблице **17**):

- **-l** — вывести список имеющихся правил;
- **-a** — добавить новое правило;
- **-d** — удалить правило из списка;
- **-D** — удалить все имеющиеся правила.

Чтобы создать новое правило, нужно выполнить команду вида:

$ auditctl -a <список>, <действие> -S <имя системного вызова> -F <фильтры>

Сначала после опции -a указывается список, в который нужно добавить правило. Всего существует 5 таких списков:

- task — события, связанные с созданием новых процессов;
- entry — события, которые имеют место при входе в системный вызов;
- exit — события, которые имеют место при выходе из системного вызова;
- user — события, использующие параметры пользовательского пространства;
- exclude — используется для исключения событий.

Затем указывается, что нужно делать после наступления события. Здесь возможны два варианта: always (события будут записываться в журнал) и never (не будут).

После опции -S идёт имя системного вызова, при котором событие нужно перехватить (open, close и т.п.).

После опции -F указываются дополнительные параметры фильтрации. Например, если нам требуется вести аудит обращений к файлам из каталога /etc, правило будет выглядеть так:

$ auditctl -a exit,always -S open -F path =/etc/

Можно установить и дополнительный фильтр:

$ auditctl -a exit,always -S open -F path =/etc/ -F perm = aw

Аббревиатура aw означает следующее: a — изменение атрибута (attribute change), w — запись (write). Формулировка perm = aw указывает, что для директории /etc нужно отслеживать все факты изменения атрибутов (a — attribute change) и w (w — write).

При настройке слежения за отдельными файлами можно опустить опцию -S, например:

$ auditctl -a exit,always -F path =/etc/ -F perm = aw

1.7.5.5 Файлы правил

Правила можно не только задавать через командную строку, но и прописывать в файле etc/audit/audit.rules.
Начинается этот файл с так называемых метаправил, в которых задаются общие настройки журналирования:

удаляем все ранее созданные правила
-D

```
# задаём количество буферов, в которых будут храниться сообщения
-b 320

# указываем, что делать в критической ситуации (например, при переполнении буферов): 0 - ничего не делать; 1 - отправлять сообщение в dmesg, 2 -  отправлять ядро в панику
-f 1
```

Далее следуют пользовательские правила. Их синтаксис предельно прост: достаточно просто перечислить соответствующие опции команды auditctl. Рассмотрим пример типового конфигурационного файла:

```
# отслеживать системные вызовы unlink () и rmdir()
-a exit,always -S unlink -S rmdir

# отслеживать системные вызовы open () от пользователя с UID 1001
-a exit,always -S open -F loginuid=1001

# отслеживать доступ к файлам паролей и групп и попытки их изменения:
-w /etc/group -p wa
-w /etc/passwd -p wa
-w /etc/shadow -p wa
-w /etc/sudoers -p wa

# отслеживать доступ к следующей директории:
-w /etc/my_directory -p r

# закрыть доступ к конфигурационному файлу для предотвращения изменений
-e 2
```

Изменения конфигурации вступят в силу после перезапуска демона auditd:

```
$ sudo service auditd restart
```

1.8 Web-интерфейс

1.8.1 Подключение к web-интерфейсу

Управление через web-интерфейс возможно через любой стандартный интернет-браузер, поддерживающий HTTP 1.0. Например, Opera, Firefox, IE или Chrome.

Для входа в web-интерфейс наберите в адресной строке интернет-браузера (Рисунок 3) IP-адрес роутера (по умолчанию 192.168.1.1).

Рисунок 3 – Адресная строка интернет-браузера

При наличии связи с устройством, в окне интернет-браузера появится запрос авторизации (Рисунок 4). Введите логин и пароль (пароль по умолчанию – root) и нажмите кнопку «Вход» или клавишу «Enter».

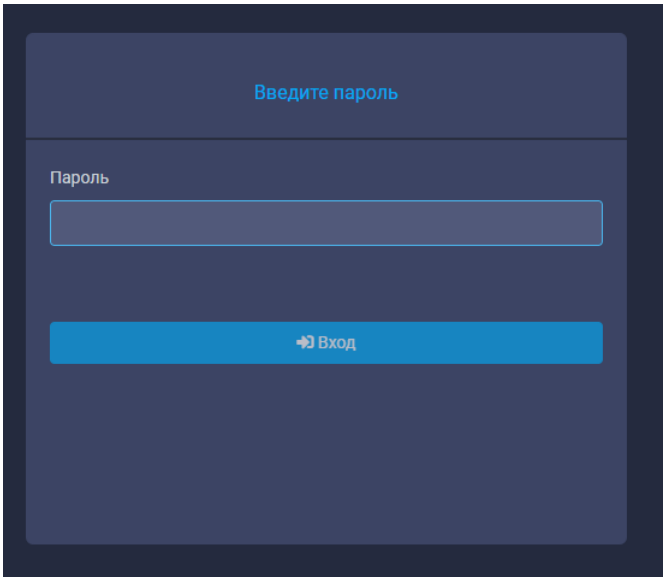


Рисунок 4 – Окно авторизации для доступа к web-интерфейсу

После корректного ввода логина и пароля открывается доступ к основному интерфейсу управления роутером (Рисунок 5).

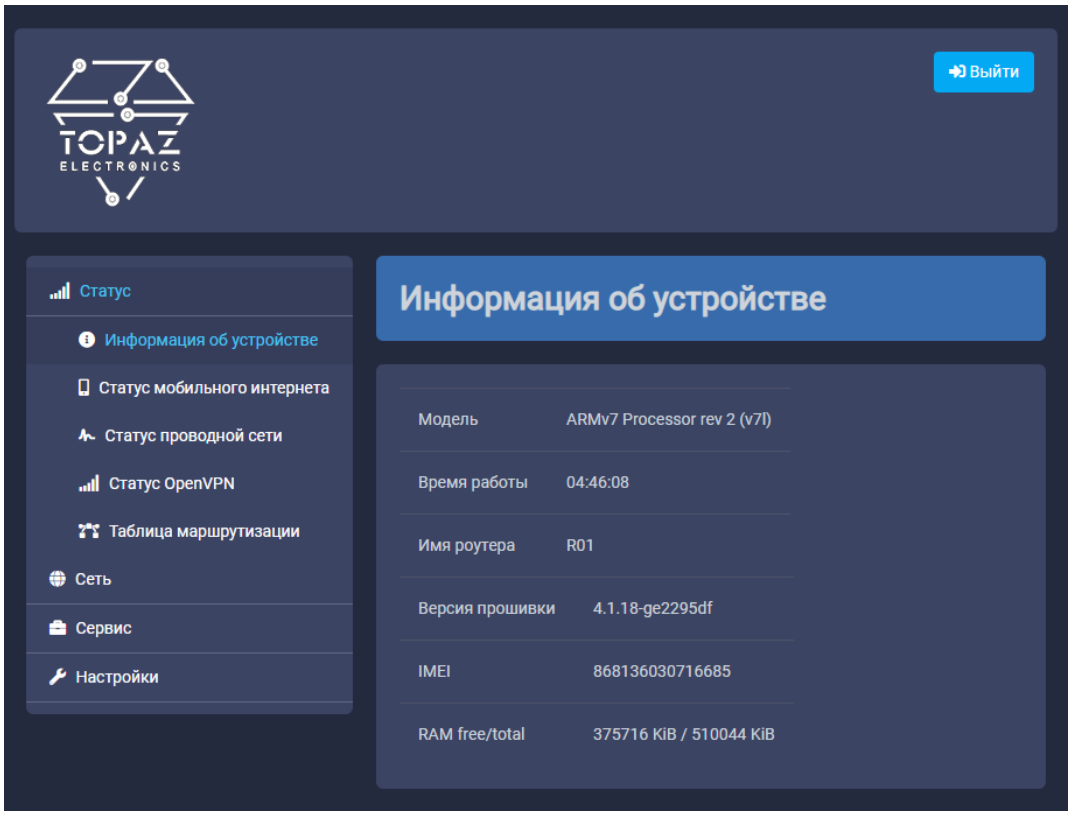


Рисунок 5 – Основное окно web-интерфейса

При редактировании настроек разделов, если в разделе присутствует кнопка Сохранить, то сохранение внесенных изменений происходит по нажатию данной кнопки. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

1.8.2 Раздел Статус

На вкладке **Статус** приведена информация о состоянии роутера и его сервисов для быстрой диагностики устройства. В данном разделе приводится подробное описание полей и значений данной вкладки.

1.8.2.1 Информация об устройстве

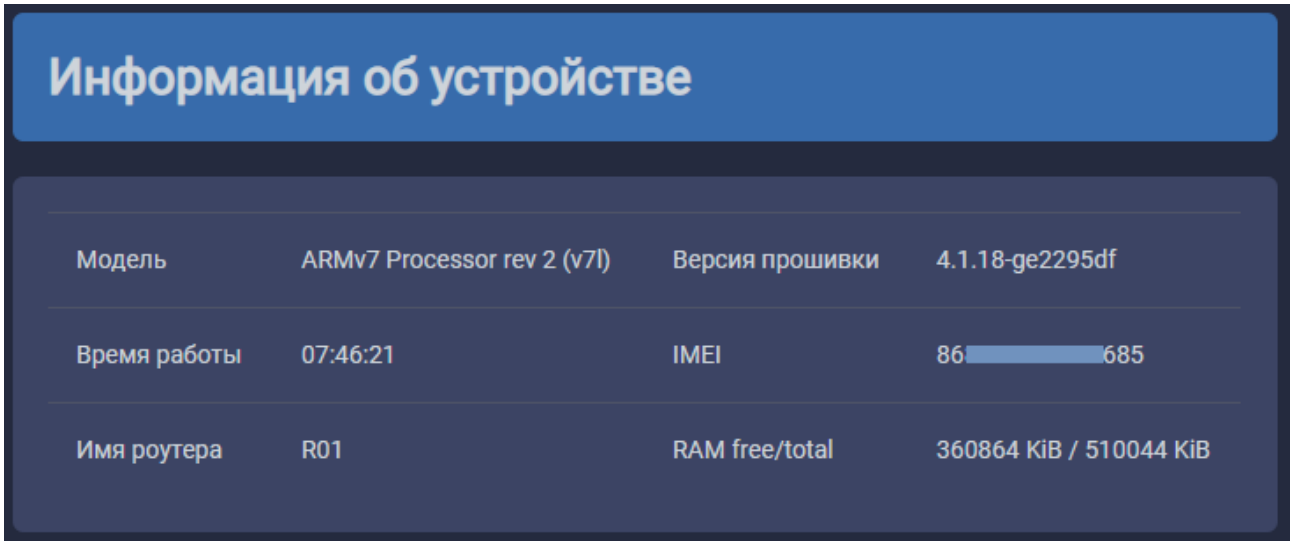


Рисунок 6 – Пример информации в разделе Информация об устройстве

Таблица 18 – Поля в разделе Информация об устройстве

Поле	Описание
Модель	Выводит модель роутера
Время работы	Время работы роутера с последней перезагрузки
Имя роутера	Имя устройства(можно задать в разделе **Настройки → Имя устройства**)
Версия прошивки	Версия установленной прошивки
IMEI	Международный идентификатор мобильного оборудования (International Mobile Equipment Identity) данного устройства
RAM free/total	Количество свободной оперативной памяти/общий объем оперативной памяти (Кб)

1.8.2.2 Статус мобильного интернета

В данном разделе приведена информация о состоянии подключения по каналу сотовой сети.

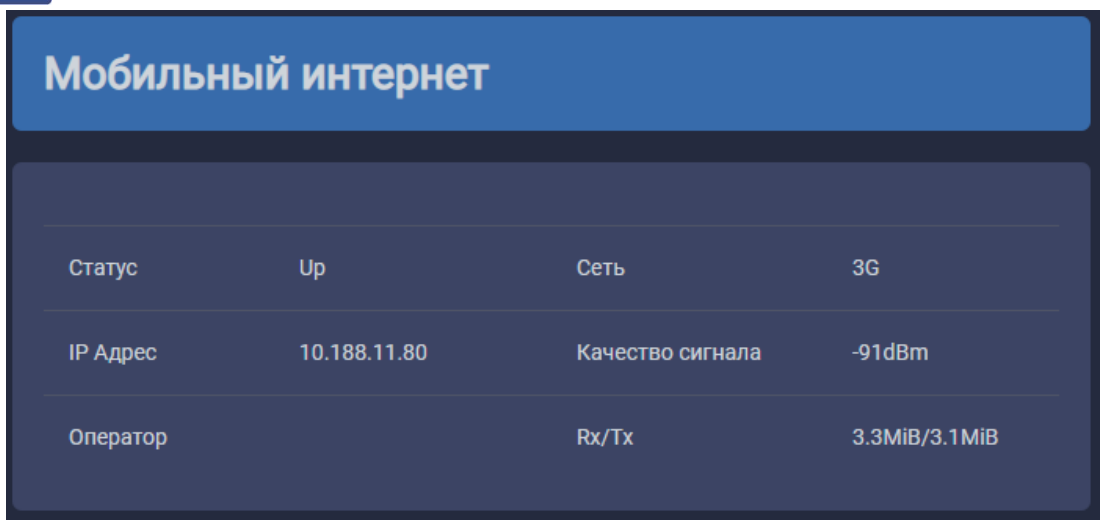


Рисунок 7 – Пример информации в разделе Статус мобильного интернета

Таблица 19 – Поля раздела Статус мобильного интернета

Поле	Описание
Статус	Статус подключения к сотовой сети: **Up** — SIM-карта зарегистрирована в сети сотового оператора и готова к работе; **Down** — SIM-карта не зарегистрирована в сети и не работает.
IP Адрес	IP-адрес сим карты, выдаваемый оператором сотовой сети
Оператор	Имя оператора сотовой сети
Сеть	Тип сотовой сети по которой в данный момент осуществляется передача данных: 2G, 3G, 4G
Качество сигнала	Уровень сигнала сотовой сети в дБм.
Rx/Tx	Счетчик принятых и отправленных данных (Мб)

1.8.2.3 Статус проводной сети

В данном разделе приведена информация о состоянии проводной сети.

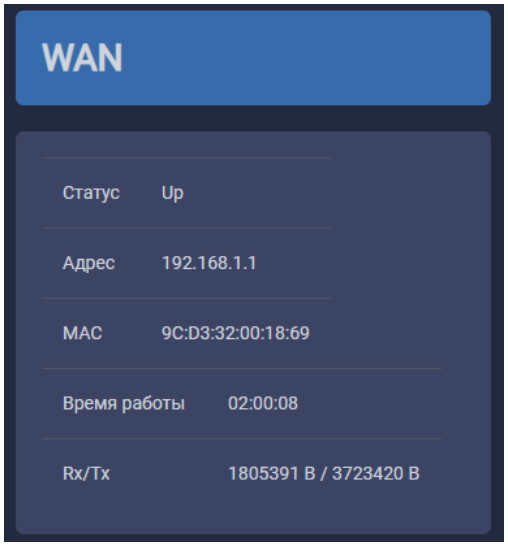


Рисунок 8 – Пример информации в разделе Local Network

Таблица 20 – Поля раздела Статус проводной сети

Поле	Описание
Статус	Указывает о наличии физического подключения к порту: **Up** — подключение есть; **Down** — подключения нет
Адрес	IP-адрес порта
MAC	MAC-адрес порта
Время работы	Время работы порта
Rx/Tx	Счетчик принятых/отправленных данных (байт)

1.8.2.4 Таблица маршрутизации

В данном разделе содержится информация по таблице маршрутизации. Выводятся все существующие на данный момент маршруты.

Назначение	Шлюз	Маска	Интерфейс
0.0.0.0	10.64.64.64	0.0.0.0	ppp0
10.64.64.64	0.0.0.0	255.255.255.255	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	lan-0
192.168.3.0	0.0.0.0	255.255.255.0	lan10-1

Рисунок 9 – Пример информации в разделе Таблица маршрутизации

1.8.3 **Раздел Сеть**

В данном разделе находятся сетевые настройки

1.8.3.1 Локальная сеть

Данный раздел предназначен для настройки Ethernet-портов роутера в рамках LAN/VLAN. В роутерах TOPAZ имеется возможность настроить WAN-порт таким образом, чтобы он работал, как локальный Ethernet-порт.

Первой позицией данного раздела являются настройки интерфейса конфигурирования.

В данном разделе можно объединить Ethernet-порты в VLAN (виртуальную локальную сеть). Чтобы добавить новый VLAN, нажмите на кнопку **Добавить LAN** внизу страницы, а чтобы удалить – нажмите кнопку **Удалить**, в соответствующей группе настроек.

Если настройки VLAN заданы неверно, то web-интерфейс не позволит сохранить вновь добавленный VLAN.

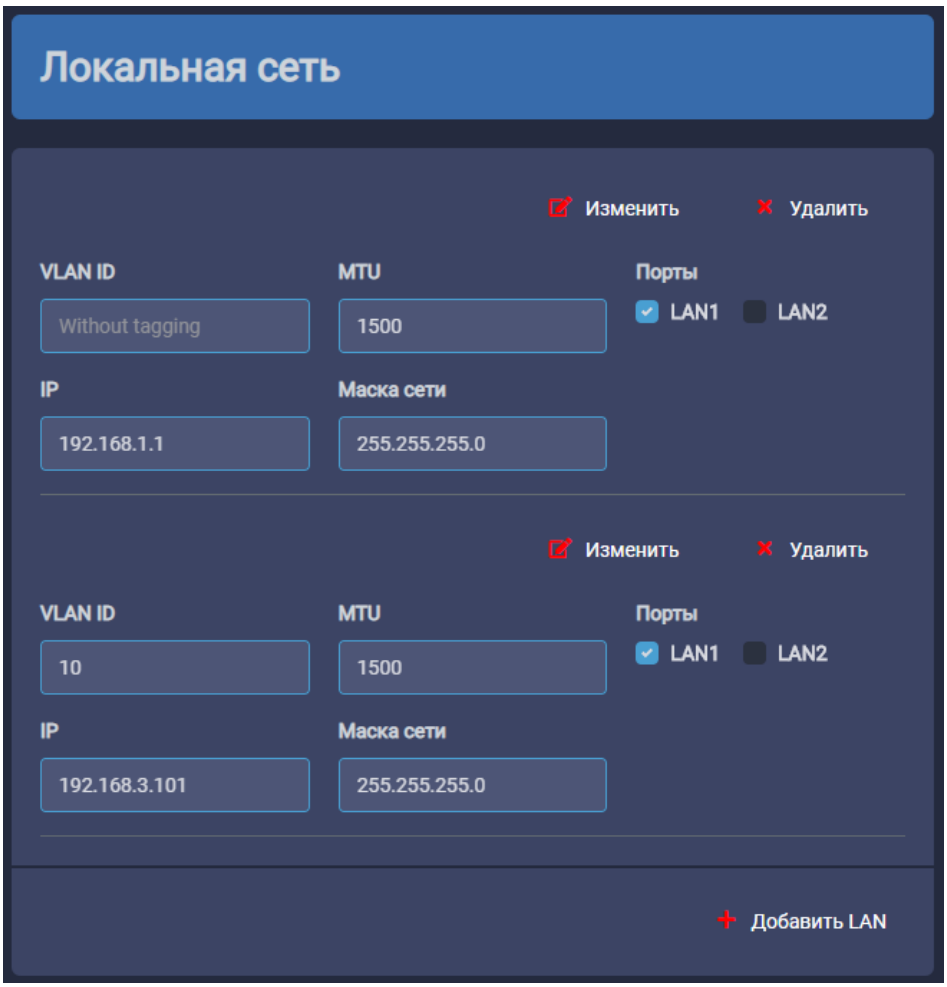


Рисунок 10 – Раздел Локальная сеть

Таблица 21 – Поля в разделе Локальная сеть

Поле	Описание
VLAN ID	Номер VLAN. По умолчанию VLAN ID задается устройством автоматически, однако у пользователя есть возможность задать его вручную. Для интерфейса конфигурирования VLAN ID не задан.
MTU	Максимальный размер полезного блока данных одного пакета. Рекомендуемое значение 1500.
Порты	Выбор физических портов, объединенных в VLAN.
IP	IP-адрес роутера для созданного VLAN
Маска сети	Маска сети роутера для созданного VLAN

1.8.3.2 WAN

Раздел WAN предназначен для настройки WAN-порта роутера. В роутерах TOPAZ имеется возможность настроить локальные порты таким образом, чтобы они работали, как WAN-порты.

На рисунке ниже приведен пример создания VLAN на основе WAN-порта роутера.

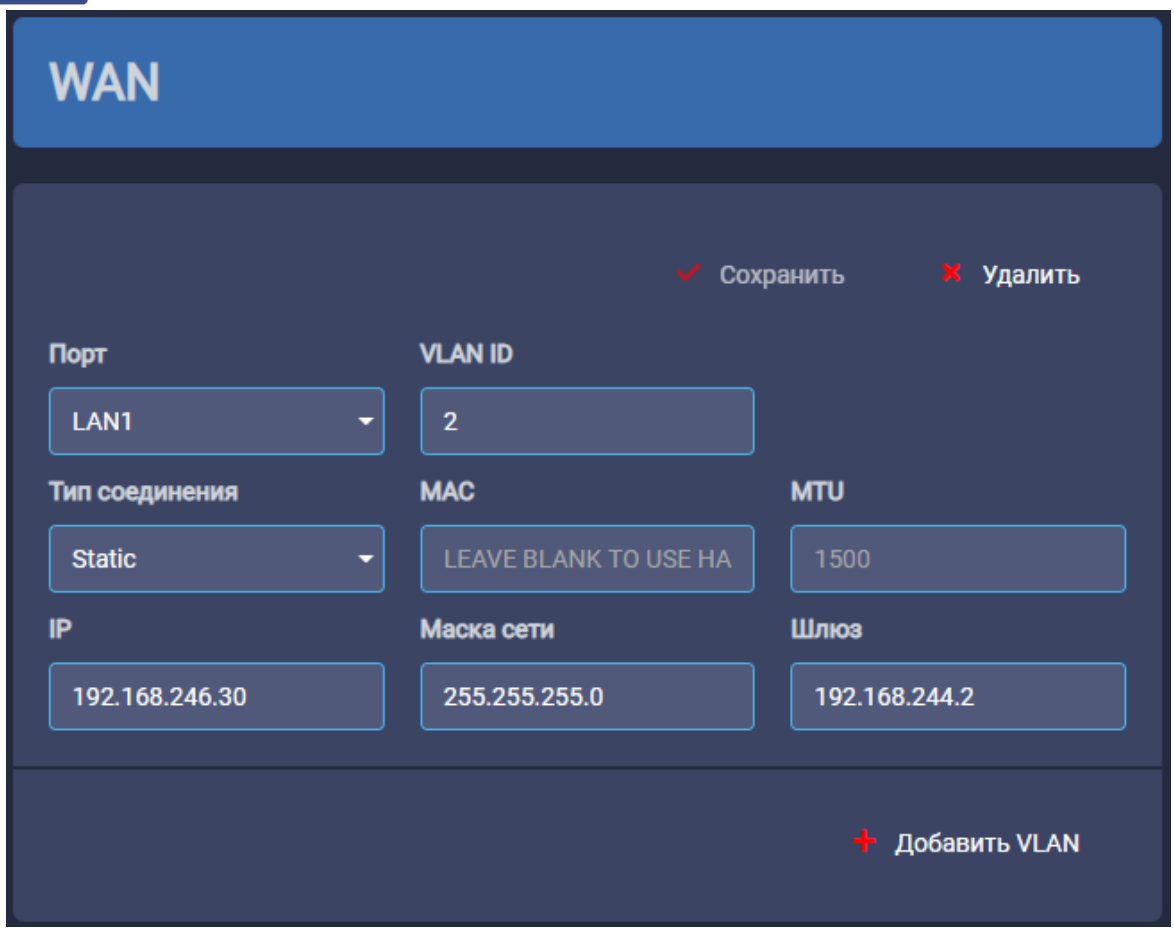


Рисунок 11 – Раздел WAN

В данном примере настроен один WAN-порт, группа настроек виртуальной сети «wan» (название задается автоматически). Чтобы добавить новый VLAN, нажмите на кнопку **Добавить VLAN** внизу страницы, а чтобы удалить – нажмите кнопку **Удалить**, в соответствующей группе настроек. Для сохранения выполненных настроек, используйте кнопку **Сохранить**.

Тип подключения DHCP означает, что роутер должен получить IP-адрес, маску и адреса DNS- серверов от внешнего DHCP-сервера. Тип подключения Static необходим для ручной установки сетевых настроек WAN-порта. Тип подключения PPPoE необходим при использовании протокола с авторизацией на сервере PPPoE.

Таблица 22 – Поля в разделе WAN

Поле	Описание
Порт	Выбор порта устройства, который будет назначен на VLAN.
VLAN ID	Номер VLAN. Изначально задается автоматически, можно переназначить вручную.
Тип соединения	Тип подключения к внешним сетям, через WAN-порт: [A] Static – соединение с ручными настройками; [B] DHCP – соединение с получением настроек от DHCP-сервера; [C] PPPoE – соединение с авторизацией на сервере PPPoE.

Дополнительные настройки (в зависимости от выбранного типа соединения):		
Поле	**Тип**	**Описание**
MAC	[A][B][C]	MAC-адрес роутера для созданного VLAN. Если поле оставить пустым, то будет использоваться MAC-адрес, установленный производителем. Данное поле рекомендуется оставлять пустым, либо вводимый адрес

		должен являться уникальным в сети.
IP	[A]	IP-адрес роутера для созданного VLAN
Маска сети	[A]	Маска сети роутера для созданного VLAN
Шлюз	[A]	Шлюз роутера для созданного VLAN
MTU	[A]	Метрика сетевого интерфейса
Логин	[C]	Логин, который указывается при PPPoE-соединении
Пароль	[C]	Пароль, который указывается при PPPoE-соединении
Имя концентратора доступа	[C]	Имя концентратора доступа, который указывается при PPPoE- соединении

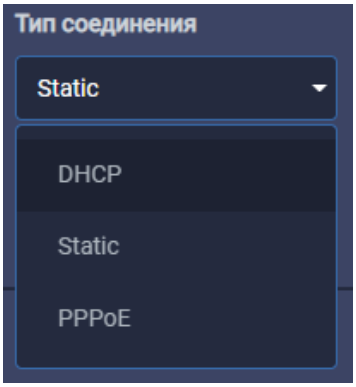


Рисунок 12 – Выбор типа соединения для WAN-порта

1.8.3.3 Мобильный интернет

Данный раздел предназначен для настройки мобильного Интернета на устройстве. На страннице раздела представлены две группы настроек – для SIM1 и SIM2.

Чтобы включать или отключать работу роутера с SIM-картой, необходимо поставить или снять галочку напротив пункта **Включить SIM1** (или SIM2).

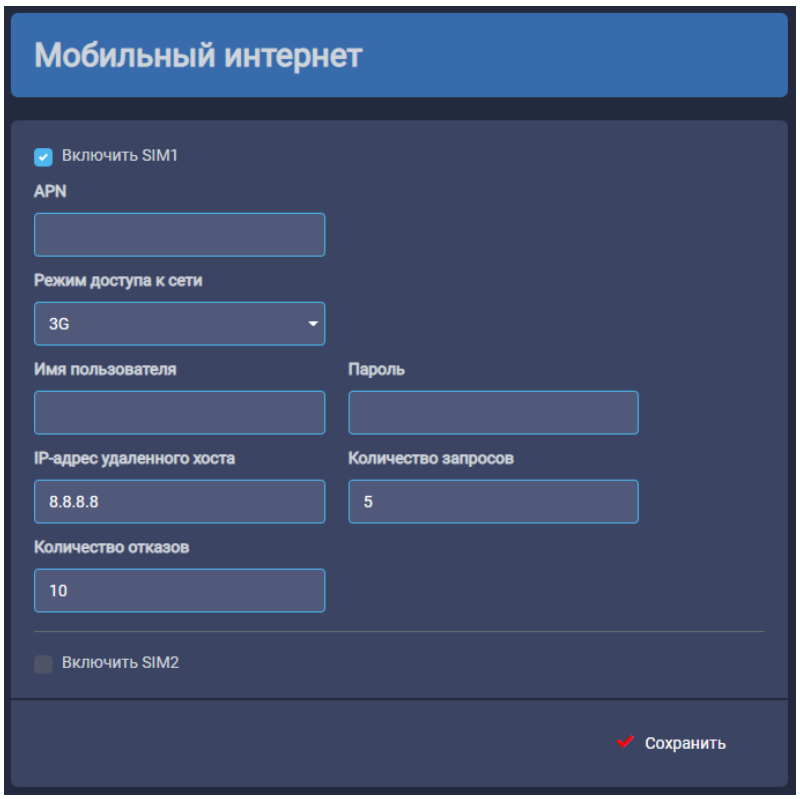


Рисунок 13 – Параметры SIM-карты раздела Мобильный интернет

Таблица 23 – Параметры SIM-карты

Поле	Описание
APN	Имя сотовой сети (APN). Необходимо, если у SIM-карты корпоративный тариф или выделенная сотовая сеть внутри провайдера
Режим доступа к сети	Выбор приоритетного режима работы с сотовыми сетями: LTE – работа в сети LTE; 2G – работа в сети 2G; 3G – работа в сети 3G.
Имя пользователя	Имя пользователя для доступа в сотовую сеть провайдера
Пароль	Пароль для доступа в сотовую сеть провайдера
IP-адрес удаленного хоста	IP-адрес удаленного хоста для проверки работы соединения
Количество запросов	Количество ICMP пакетов отправляемых при проверке доступности IP-адреса удаленного хоста.
Количество отказов	Количество неудачных ICMP запросов, приводящее к перезагрузке роутера.

1.8.3.4 Маршрутизация

Данный раздел предназначен для настройки приоритетов WAN-портов, режим их работы и настройки статических маршрутов. На рисунке ниже представлен пример настроек роутера.

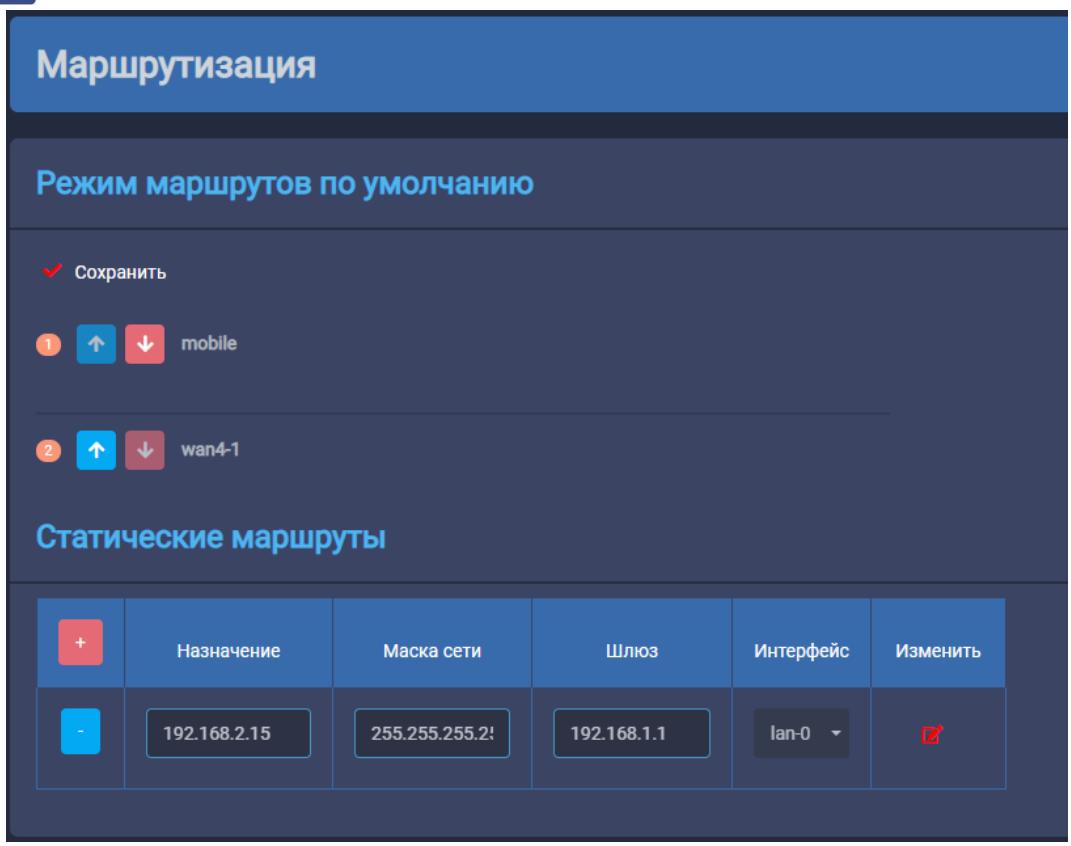


Рисунок 14 – Раздел Маршрутизация

Роутер резервирует подключение между WAN-портами последовательно и в порядке, указанном пользователем в подразделе **Режим маршрутов по умолчанию**. С помощью стрелок можно перемещать выбранный WAN-порт вверх или вниз в зависимости от приоритетов пользователя.

В подразделе **Статические маршруты** можно задать параметры статической маршрутизации. Добавление нового маршрута осуществляется нажатием кнопки (**плюс**) в первом столбце таблицы, удаление маршрута - кнопки (**минус**) напротив маршрута.

Таблица 24 – Настройки маршрутов

Поле	Описание
Назначение	IP-адрес или подсеть назначения маршрута
Маска сети	Маска сети
Шлюз	IP-адрес шлюза маршрута
Интерфейс	Выбор интерфейса, через который будет работать маршрут

1.8.3.5 DNS

В данном разделе можно указать адреса DNS-серверов. Добавление нового адреса происходит по кнопке (**плюс**) в первом столбце таблицы, удаление адреса по кнопке (**минус**) напротив маршрута. На рисунке ниже представлен пример настроек с двумя адресами.

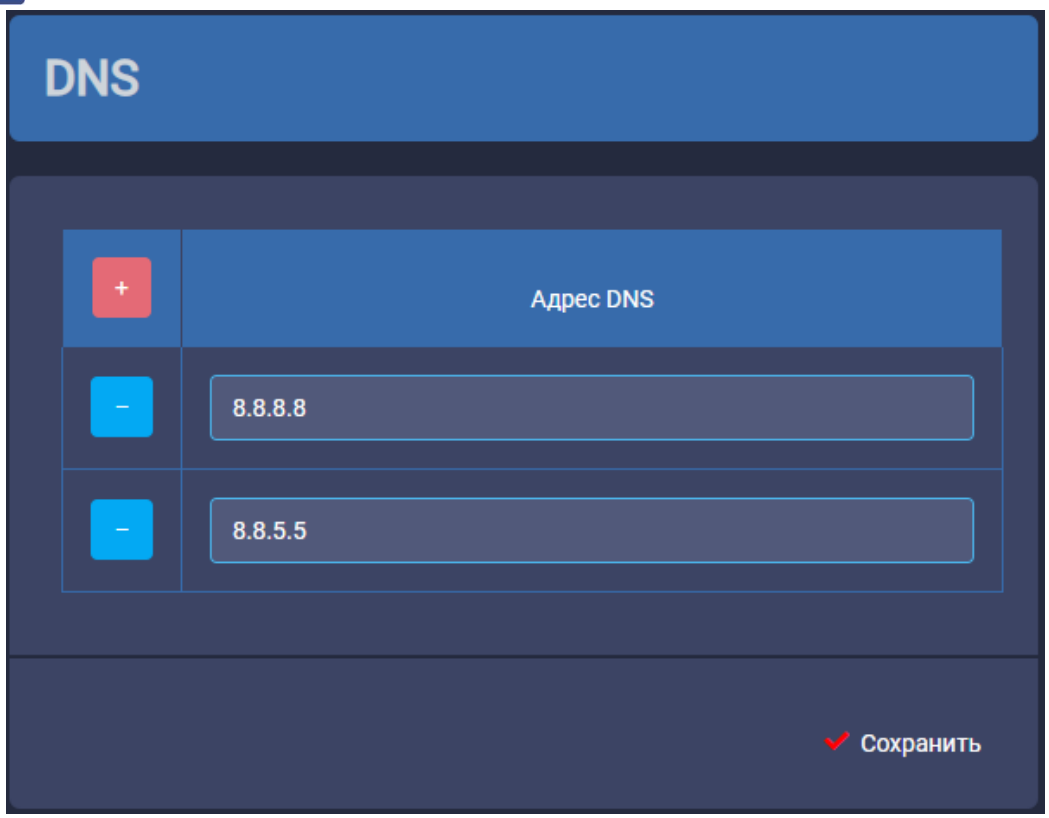


Рисунок 15 – Раздел DNS

1.8.3.6 PPTP клиент

В данном разделе приведены настройки подключения по PPTP в режиме клиента. На рисунке ниже приведен пример настройки подключения.

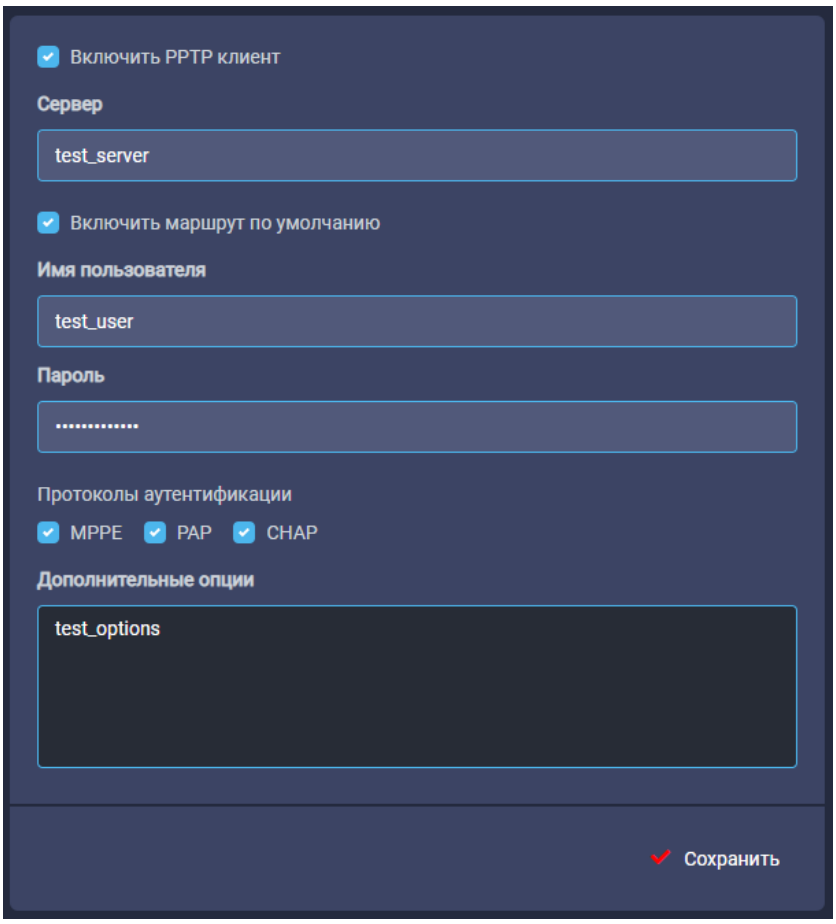


Рисунок 16 – Настройки PPTP клиента

Чтобы построить туннель, поставьте галочку напротив **Включить PPTP клиент** и задайте необходимые настройки. Туннель будет работать через любой, активный на данный момент времени, WAN-порт.

Таблица 25 – Настройки PPTP

Поле	Описание
Сервер	IP-адрес сервера, к которому будет выполняться подключение
Включить маршрут по умолчанию	Включение/выключение установки маршрута по умолчанию через данный туннель
Имя пользователя	Имя пользователя для подключения к PPTP-серверу
Пароль	Пароль для подключения к PPTP-серверу
Протоколы аутентификации	Выбор методов шифрования трафика: MPPE, PAP, CHAP.
Дополнительные опции	Указание дополнительных опций для работы туннеля, при необходимости

1.8.3.7 Switch

Данный раздел предназначен для управления Ethernet-портами роутера. На рисунке ниже приведен пример настройки портов роутера 2Tx.

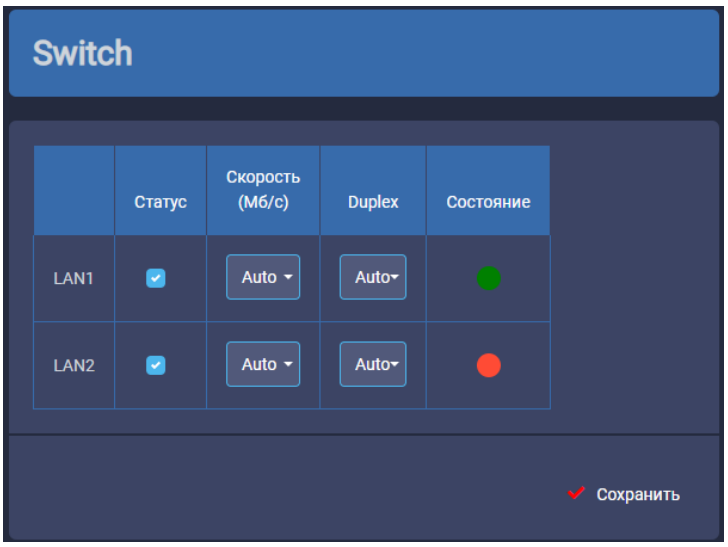


Рисунок 17 – Раздел Switch

Таблица 26 – Настройки портов Ethernet

Поле	Описание
Статус	Включение/выключение работы порта
Скорость	Выбор скорости работы порта: Auto (выбор скорости устройством), 10, 100, 1000 Мбит/с
Duplex	Выбор режима работы порта: – Auto – автоматический режим; – Full – передача и прием данных одновременно; – Half – передача и прием данных по очереди.
Состояние	Цветовой индикатор состояния порта – зеленый – LINK UP – красный – LINK DOWN

1.8.3.8 OpenVPN-туннели

Данный раздел предназначен для создания туннелей OpenVPN. OpenVPN туннель может быть двух типов: Ethernet Bridging (L2) и Routing (L3). Для настройки OpenVPN-туннеля в веб-интерфейсе роутера:

1) Зайдите в раздел **Сеть → OpenVPN-туннели**;
2) Поставьте галочку напротив пункта **Включить OpenVPN Tunnel**;
3) Выберите в поле **Устройство** значение **TAP (L2)** или **TUN (L3)**;
4) Задайте необходимые настройки.

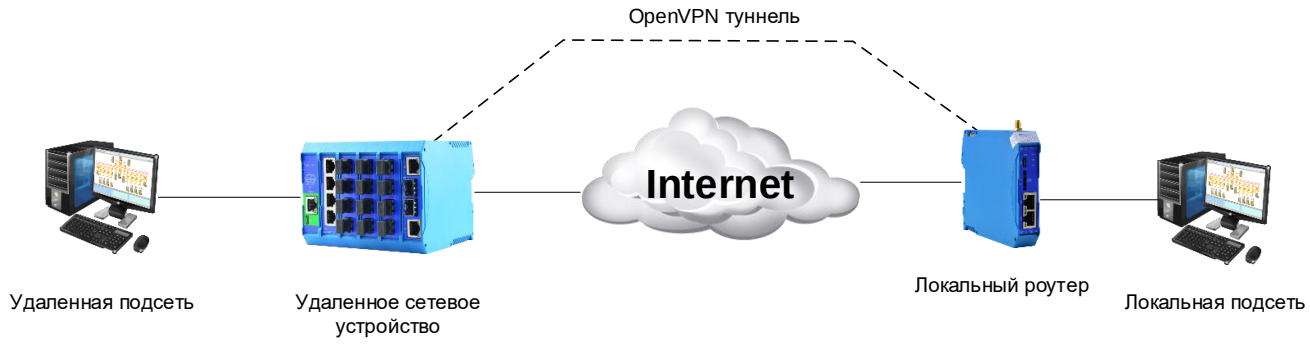


Рисунок 18 – Схема сети OpenVPN в общем виде

В таблице ниже приведено описание основных настроек туннелей OpenVPN, общих для L2 и L3.

Таблица 27 – Основные настройки OpenVPN-туннелей

Поле	Описание
Устройство	Выбор виртуального интерфейса (TAP или TUN)
Транспортный протокол	Выбор транспортного протокола: UDP, TCP Server, TCP Client.
Удаленный IP-адрес	IP-адрес удаленного сетевого устройства, с которым роутер будет инициировать соединение (указывается если **Transport Protocol** = **TCP Client**)
Порт	Номер порта, через который будет работать туннель
Метод авторизации	Метод авторизации (в данном примере – **none**)
Создание моста	Создание моста с локальными интерфейсами роутера (дополнительные настройки см. в таблице 29)
Интервал (сек)	Время в секундах, через которое будут отсылаться ICMP-пакеты для проверки доступности удаленного сетевого устройства (и соответственно работы туннеля)
Время ожидания	Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-туннель, если ответ от удаленного устройства не будет получен
LZO	Включение или отключение сжатия данных, проходящих через туннель
Уровень логирования	Уровень логирования. Малое значение означает, что будут выводиться только основные сообщения. Высокое значение – вывод как основных сообщений, так и детальной информации.

Выбор сетевого протокола

Туннель может работать по двум сетевым протоколам: UDP и TCP. Для протокола TCP есть возможность работать по методу сервера, когда роутер ожидает подключения извне, так и по методу клиента, когда роутер инициирует подключение с другим сетевым устройством.

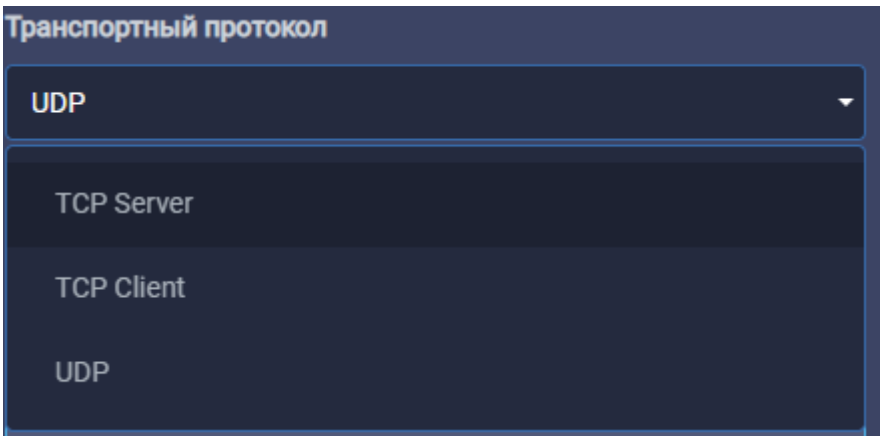


Рисунок 19 – Выбор транспортного протокола

При выборе протокола передачи данных следует учитывать, что по протоколу UDP туннель будет работать быстрее всего, так как при использовании протокола TCP Server роутер будет ожидать установления соединения от удаленного устройства.

Выбор метода авторизации

Для обоих типов туннеля доступно четыре варианта настройки туннеля, различающиеся по методу авторизации (рисунок 20):

- без авторизации (none);
- с авторизацией по общему ключу (Shared secret);
- в роли сервера OpenVPN (TLS Server);
- в роли клиента OpenVPN (TLS Client).

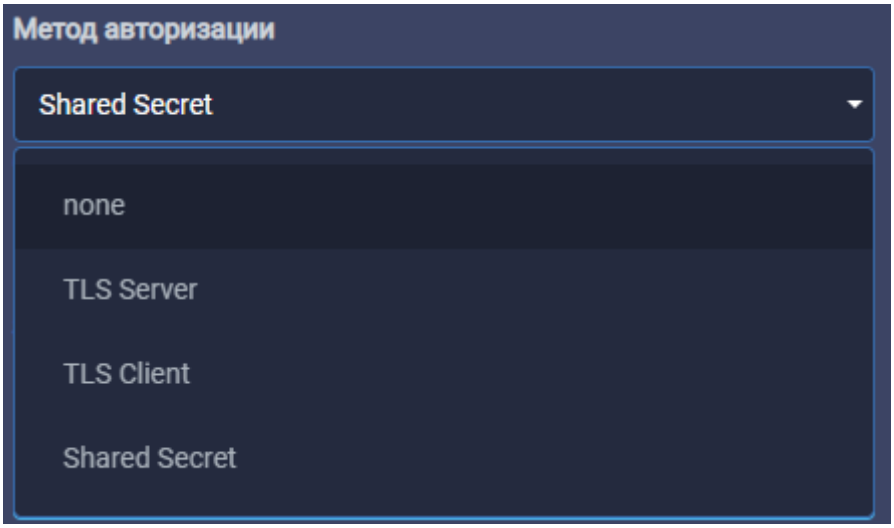


Рисунок 20 – Метод авторизации OpenVPN

Настройка туннеля без авторизации

Для настройки OpenVPN-туннеля без авторизации между сетевыми устройствами, в веб-интерфейсе роутера в поле **Метод авторизации** выберите значение **none**.

Настройка туннеля с авторизацией по ключу (Метод авторизации: Shared Secret)

При выборе данного метода авторизации, к основным настройкам добавляется поле **Shared Secret**, в котором необходимо указать общий ключ. Сам ключ необходимо заранее сгенерировать и распространить на устройствах участниках.

Для настройки OpenVPN-туннеля с авторизацией по общему ключу между сетевыми устройствами, в веб-интерфейсе роутера в поле **Метод авторизации** выберите значение **Shared Secret** и добавьте заранее сгенерированный ключ в поле **Shared Secret**.

Настройка туннеля с авторизацией по протоколу TLS

При выборе данного метода авторизации, к основным настройкам добавляется поле поля для указания сертификатов и ключей: **CA Certificate**, **DH Parameter** (в режиме сервера), **Local Certificate**, **Local Private Key**. Ключи и сертификаты необходимо получить либо от сертификационного центра, либо создать свой собственный сертификационный центр и создать на его основе требуемые ключи и сертификаты. Для работы туннеля понадобятся файлы, указанные в таблице ниже.

Таблица 28 – Ключи и сертификаты для авторизации по протоколу TLS

Поле	Файл	Описание
CA Certificate	ca.crt	Сертификат удостоверяющего центра
DH Parameter	dh1024.pem	Файл Диффи-Хелмана для защиты передаваемых данных от расшифровки. Необходим только когда роутер выступает в роли TLS сервера

Local Certificate	server.crt	Сертификат сервера OpenVPN
Local Private Key	server.key	Приватный ключ сервера OpenVPN, секретный

Из полученных файлов необходимо будет скопировать зашифрованные данные, которые начинаются строкой “BEGIN CERTIFICATE”, а заканчиваются “END CERTIFICATE”, и вставить текст в соответствующие поля согласно таблице 28.

Дополнительная конфигурация

Поле **Дополнительная конфигурация** позволяет указывать конфигурационные параметры, которые роутер будет передавать, подключающемуся к нему сетевому устройству. Пункты и их расшифровка, которые указываются в данном поле, можно посмотреть на официальном сайте OpenVPN по адресу: https://openvpn.net/index.php/open-source/documentation/howto.html#server

OpenVPN лог

В поле **OVPN Log** отображается состояние созданного OpenVPN туннеля. Текст «Initialization Sequence Completed» в данном поле означает, что OpenVPN туннель был успешно создан.

1.8.3.8.1 Создание туннелей OpenVPN Ethernet Binding

В данном разделе рассматривается создание туннеля OpenVPN типа Ethernet Bridging (Layer 2). Данный тип туннеля OpenVPN характеризуется общим адресным пространством между устройствами, а маршрутизаторы, на которых создается OpenVPN, прозрачны для остальных сетевых устройств. Данный туннель создаётся на базе виртуального сетевого интерфейса TAP.

В примерах настройки туннелей используется следующая схема сети:

Пример настроек OpenVPN без авторизации приведен на рисунке ниже.

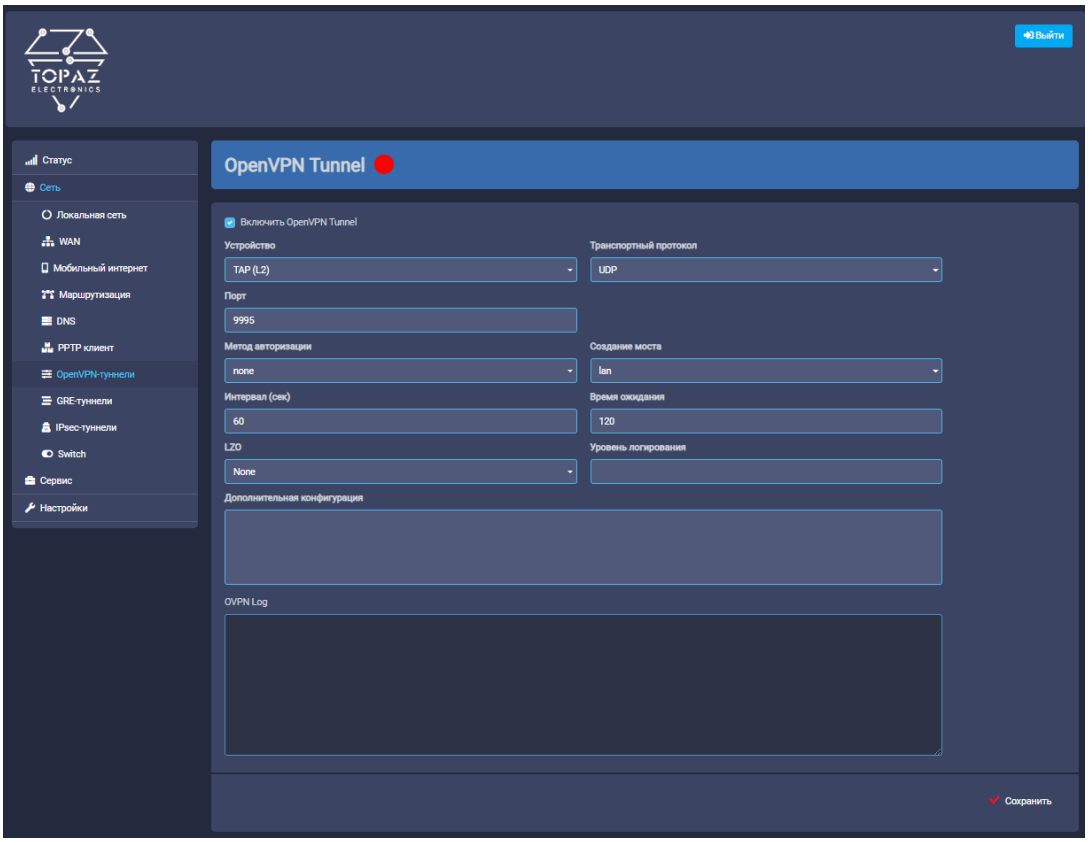


Рисунок 21 – Настройка OpenVPN (без авторизации), базовая TAP (L2)

Пример настроек для авторизации по ключу приведен на рисунке ниже.

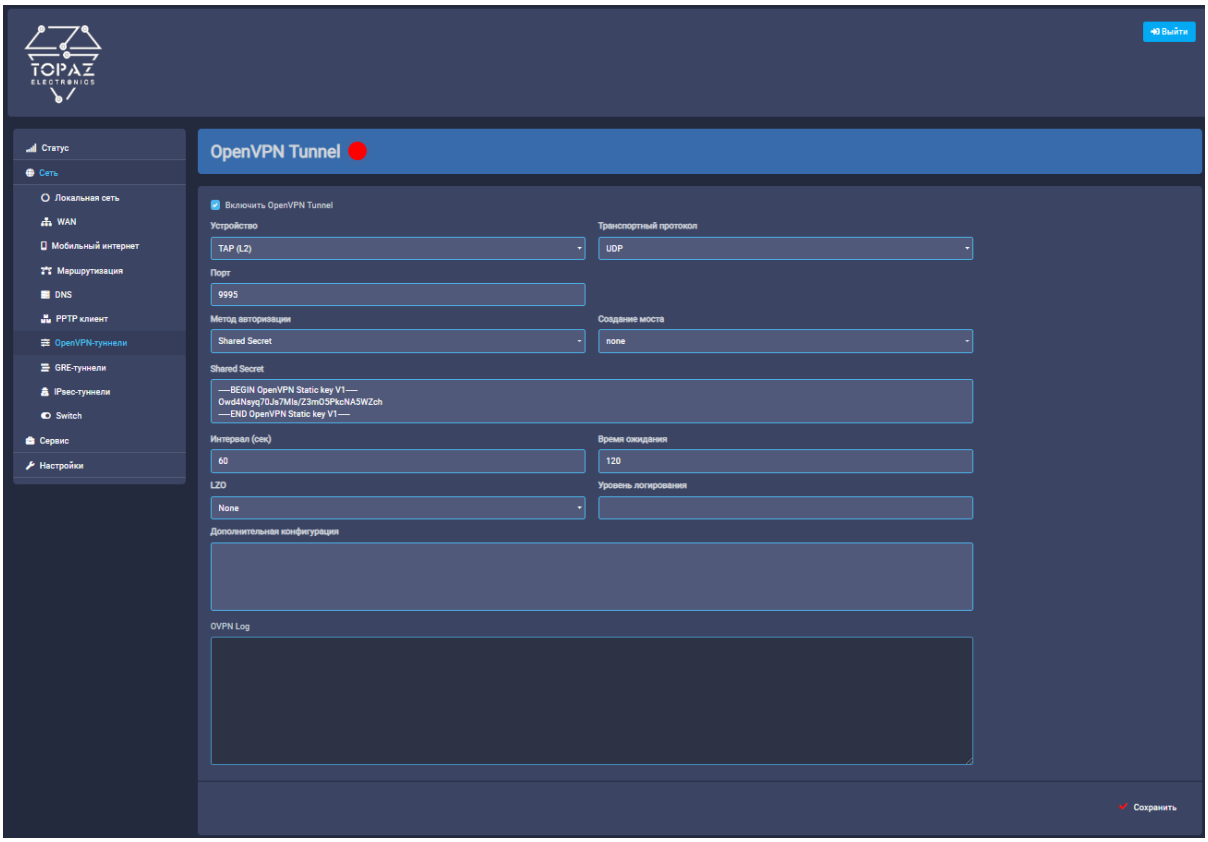


Рисунок 22 – Настройка OpenVPN (Shared Secret), базовая TAP (L2)

1.8.3.8.2 Создание туннелей OpenVPN Routing

В данном разделе рассматривается туннель OpenVPN типа Routing (Layer 3). Данный тип туннеля OpenVPN характеризуется маршрутизацией пакетов между сетями на разных концах туннеля, находящимися за сетевыми устройствами, и устанавливающими туннель между собой. Данный вид туннеля создается на базе виртуального сетевого интерфейса TUN.

Поле **Создание моста** не активно в данной конфигурации, из-за специфики работы OpenVPN с маршрутизацией.

Таблица 29 – Настройки OpenVPN-туннель→ TUN (L3)

Поле	Описание
IP-адрес туннеля	IP-адрес туннеля на данном устройстве с учётом маски сети.
Удаленный IP-адрес туннеля	Удаленный IP-адрес туннеля (устройство на другом конце туннеля) с учётом маски сети.
IP-адрес удаленной сети	IP-адрес удаленной сети (на другом конце туннеля), который необходим для создания маршрута в таблице маршрутизации
Маска удаленной сети	Маска удаленной сети (на другом конце туннеля)

Пример настроек OpenVPN без авторизации приведен на рисунке ниже.

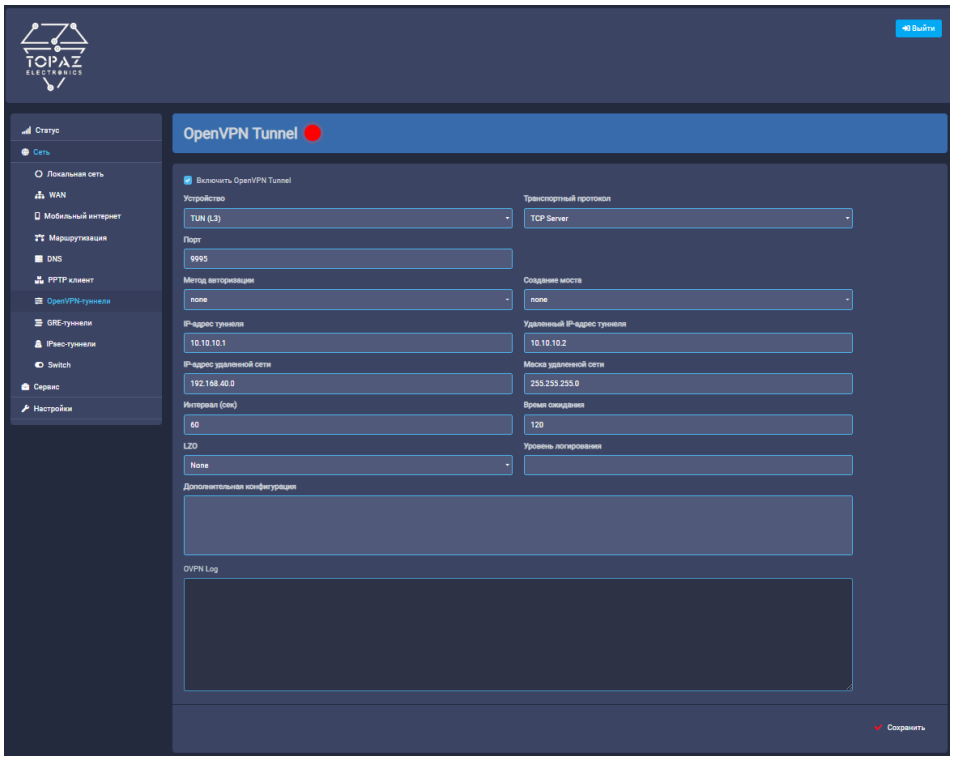


Рисунок 23 – Настройка OpenVPN (без авторизации), базовая TUN (L3)

Пример настроек для авторизации по ключу приведен на рисунке ниже.

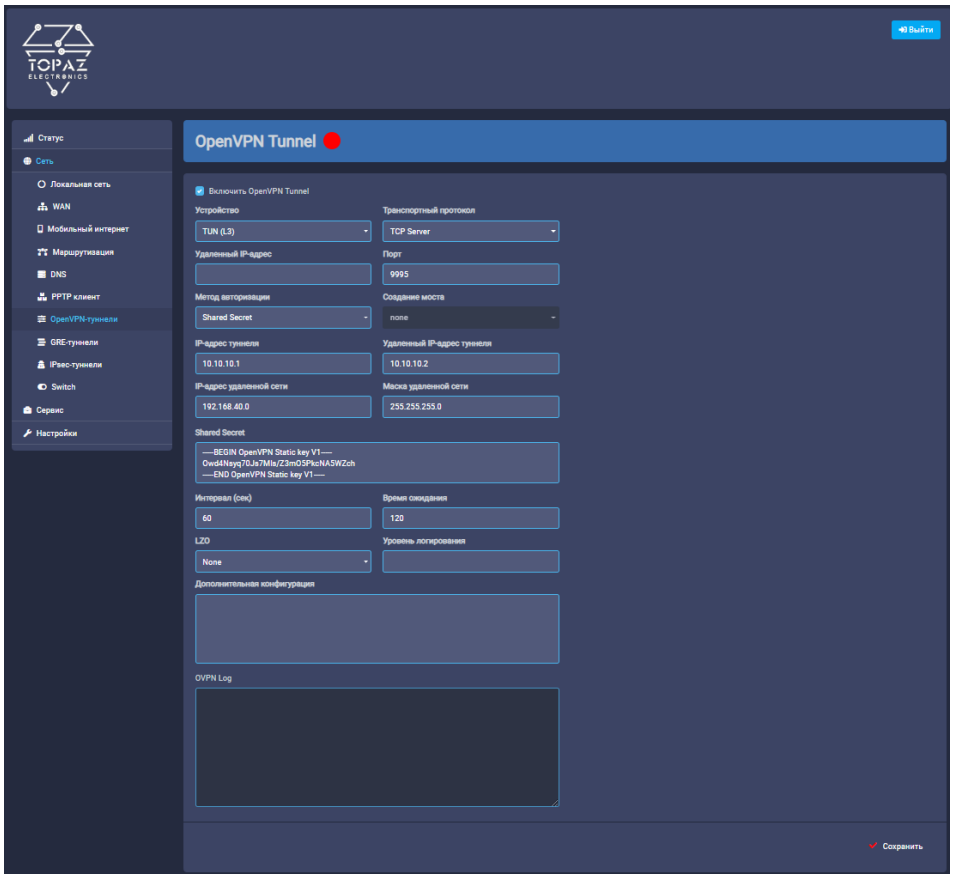


Рисунок 24 – Настройка OpenVPN (Shared Secret), базовая TUN (L3)

Пример настроек для авторизации TLS Client приведен на рисунке ниже.

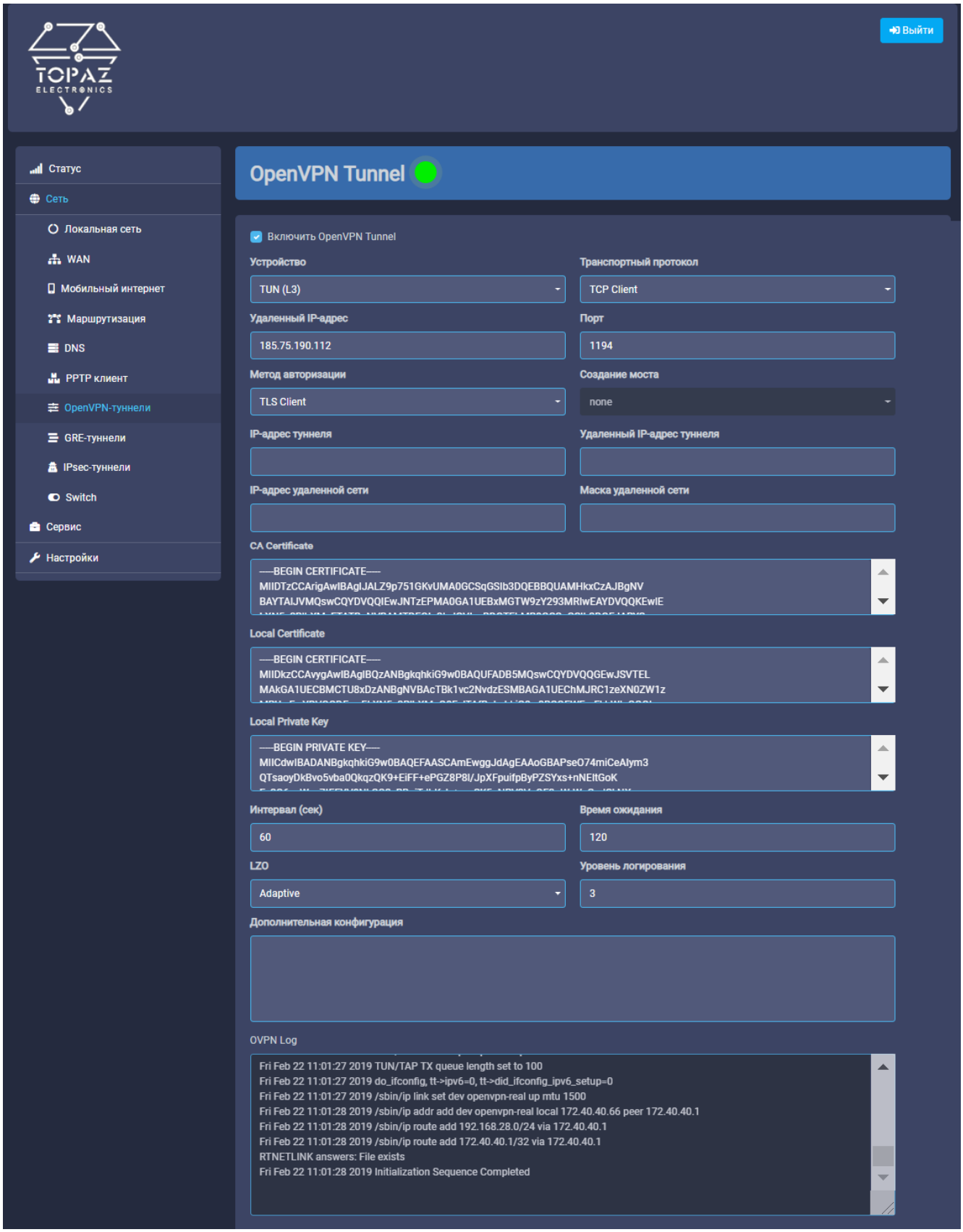


Рисунок 25 – Настройка OpenVPN (TLS Client), базовая TUN (L3)

1.8.3.9 GRE-туннели

Данный раздел предназначен для настройки GRE-туннелей.

Настройка GRE-туннеля (на примере двух роутеров TOPAZ)

Для настройки GRE-туннеля, в веб-интерфейсе роутера:

1) Зайдите в раздел **Сеть** → **Локальная сеть**;
2) Укажите IP-адрес локального пользователя в поле IP;
3) Укажите маску сети в поле Маска сети;

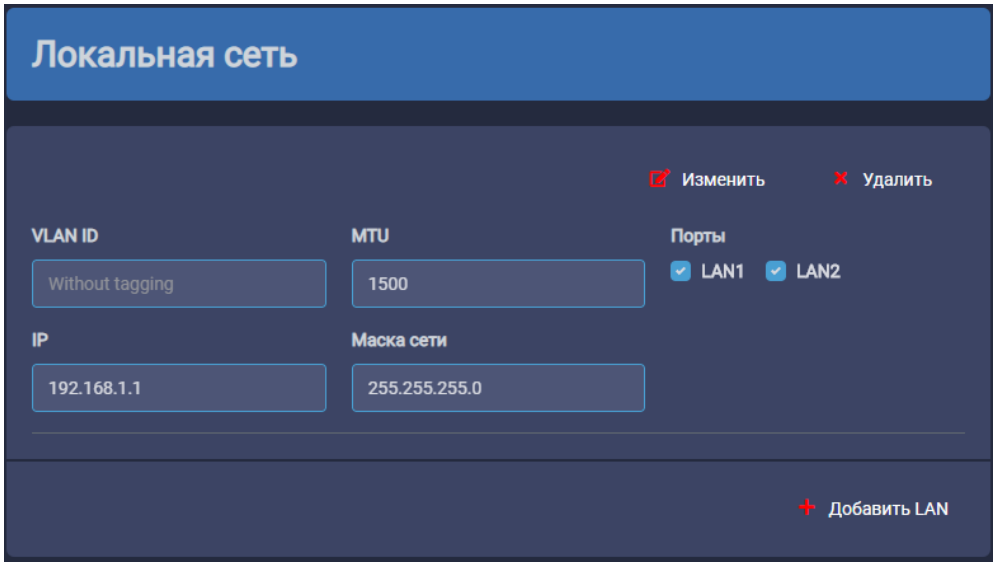


Рисунок 26 – Настройка локальной сети

Далее необходимо настроить WAN-порт роутера:

1) Зайдите в раздел **Сеть** → **WAN**;
2) Укажите тип подключения в поле Тип соединения (**Static** – статический адрес, **DHCP** – адрес, получаемый по DHCP).

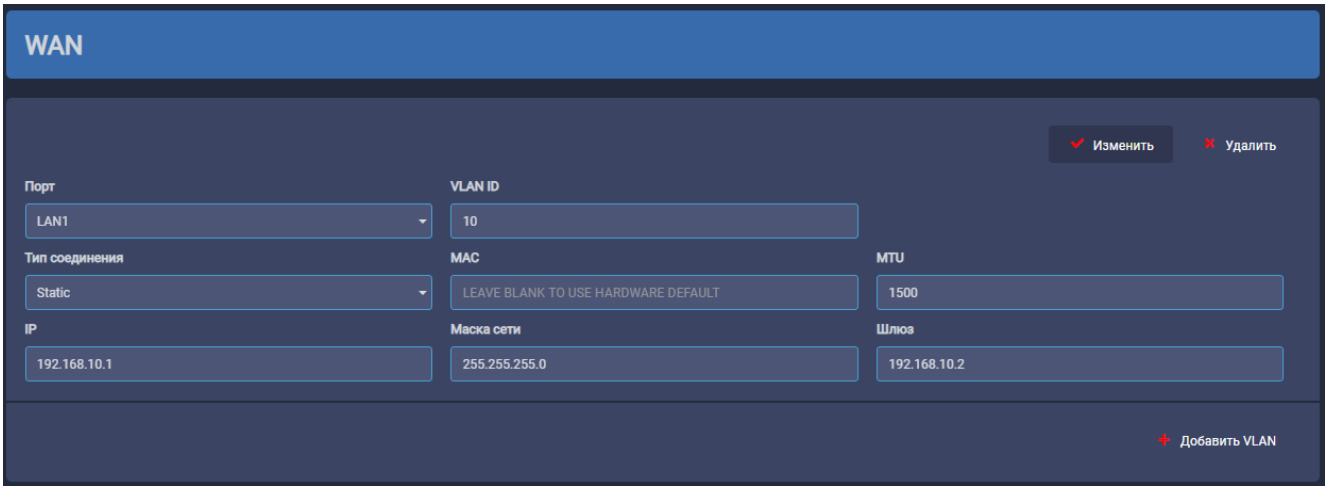


Рисунок 27 – Настройка WAN

Далее необходимо настроить GRE-туннель:

1) Зайдите в раздел **Сеть** → **GRE Tunnels**;
2) Добавьте новый туннель, нажав на кнопку **Добавить**;
3) Введите имя туннеля (на выбор пользователя) в поле **Имя**;

4) Выберите локальный интерфейс, через который будет работать туннель в поле **Локальный адрес** (поскольку в данном примере показана настройка через WAN-порт, то соответственно – 192.168.10.1);
5) Укажите IP-адрес порта удаленного устройства, с которым будет построен туннель, в поле **Удаленный адрес**;
6) Выберите на каком уровне будет работать туннель в поле **Тип** (**L2** или **L3**);
7) Выберите в каком интерфейсе будет работать GRE-туннель, выбрав значение в поле **Интерфейс**
8) Укажите IP-адрес пользовательского интерфейса в поле **Туннельный IP** и маску сети в поле **Маска сети**;
9) Укажите маску сети в поле **Маска сети** (для туннеля L2) или IP-адрес соседа в поле **Туннельный IP соседа** (для туннеля L3)
10) Выберите правило работы межсетевого экрана (firewall), если необходимо, выбрав значение в поле **Имя зоны** (правила можно настроить вручную в разделе **Сервис → Firewall**);
11) При необходимости, поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Запретить фрагментацию**.

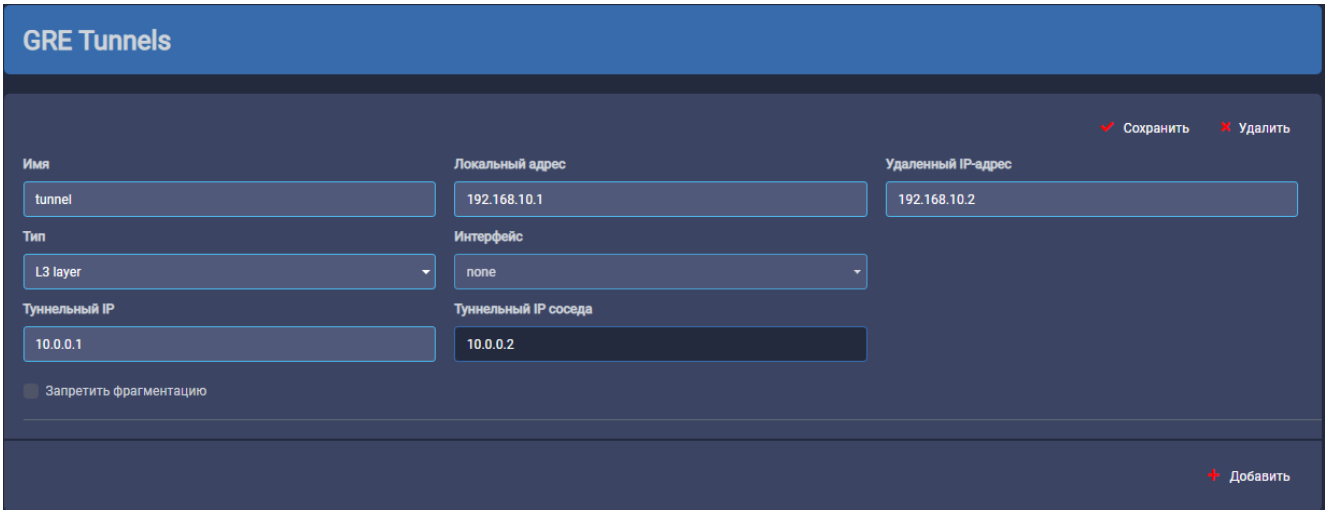


Рисунок 28 – Пример настройки GRE-туннеля уровня L3

1.8.3.10 IPsec-туннели

Данный раздел предназначен для создания IPsec-туннелей.

В роутерах TOPAZ создание туннелей IPsec реализовано с помощью программного компонента **strongSwan**. Для того, чтобы задать настройки IPsec необходимо указать текст конфигурационных файлов:

- strongswan.conf – для подключения криптографических алгоритмов и дополнительных функций.
- ipsec.conf – определяет параметры IPSEC-соединений и параметры подключений в целом;
- ipsec.secrets – служит для хранения ссылок на сертификаты и ключи авторизации;

А также указать файл сертификата VPN **vpn-server-cert.pem** и файл ключа сервера **ipsec vpn-server-key.pem**

Пример содержания конфигурационных файлов IPsec-туннеля

Файл strongswan.conf

```
charon {
  load = curl test-vectors aes des sha1 sha2 md5 pem pkcs1 gmp random x509 revocation hmac xcbc cmac ctr ccm gcm stroke kernel-netlink socket-default updown eap-identity
}
```

Файл ipsec.conf

```
config setup  / основные параметры IPsec
      strictpolicy=no
      charonstart=yes
      plutostart=no
      charondebug="ike 2, knl 3, cfg 0"
conn %default  / основные параметры всех IPsec-туннелей
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    dpdaction=restart
    dpdelay=30s
    dpdtimeout=180s
conn rw / название IPsec-туннеля
  left=<external_IP> / адрес внешнего интерфейса
  leftsubnet=<subnet/prefix> / подсеть, к которой предоставляется доступ
  leftid=<external_IP>
  leftcert=/etc/ipsec.d/certs/servercert.pem / файл сертификата, используемый для установки IKE SA
  leftauth=pubkey / авторизация с помощью сертификата RSA
  right=%any / разрешение подключения с любого IP-адреса
  rightauth=pubkey / авторизация клиента по сертификату RSA
  rightsourceip=<subnet/prefix>  / указание пула IP-адресов для выдачи клиенту
  auto=add / подключение инициируется клиентом
  keyexhcnage=ikev2
  type=tunnel
```

Файл ipsec.secrets

```
: RSA /etc/ipsec.d/private/serverkey.pem "password"
```

1.8.4 Раздел Сервис

1.8.4.1 DHCP

Данный раздел предназначен для управления DHCP-сервером. На рисунке ниже приведен пример настройки DHCP-сервера.

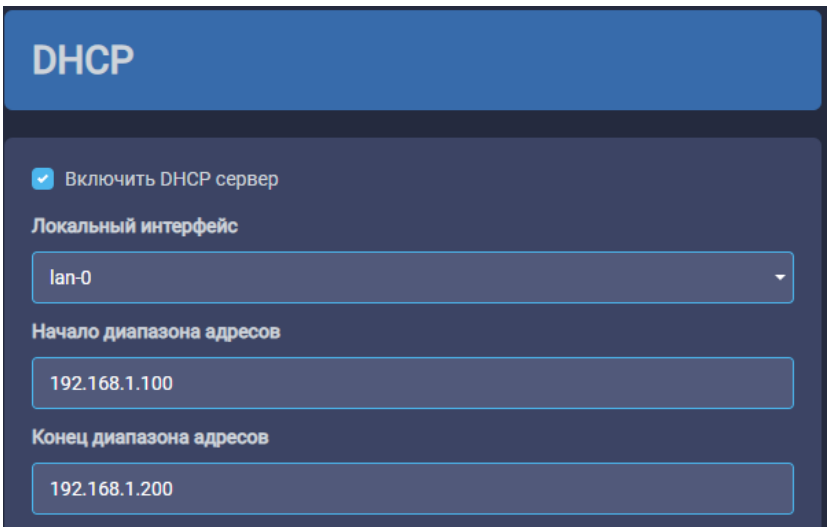


Рисунок 29 – Настройки DHCP-сервера

Для включения DHCP-сервера требуется поставить галочку напротив пункта **Включить DHCP сервер** и указать настройки для его работы. Описание настроек DHCP-сервера приведены в таблице ниже.

Таблица 30 – Настройки DHCP-сервера

Поле	Описание
Локальный интерфейс	Выбор интерфейса на котором будет работать DHCP-сервер.
Начало диапазона адресов	Адрес, с которого начнется диапазон раздаваемых адресов. Например, для указания диапазона с адреса 192.168.1.100 (где, например, 192.168.1.0 – адрес сети, в которой работает устройство) и выше.
Конец диапазона адресов	Конец диапазона адресов, определяющий размер раздаваемого адресного пространства. Например, при **Начало диапазона адресов** = 192.168.1.100 и **Конец диапазона адресов** = 192.168.1.200, размер адресного пространства будет 100.

Ниже отображается таблица, в которой перечислены клиенты, подключенные к DHCP-серверу.

Рисунок 30 – Список DHCP-клиентов

1.8.4.2 MAC фильтр

Данный раздел предназначен для установки и настройки фильтра по MAC-адресам. На рисунке ниже приведен пример настройки фильтра.

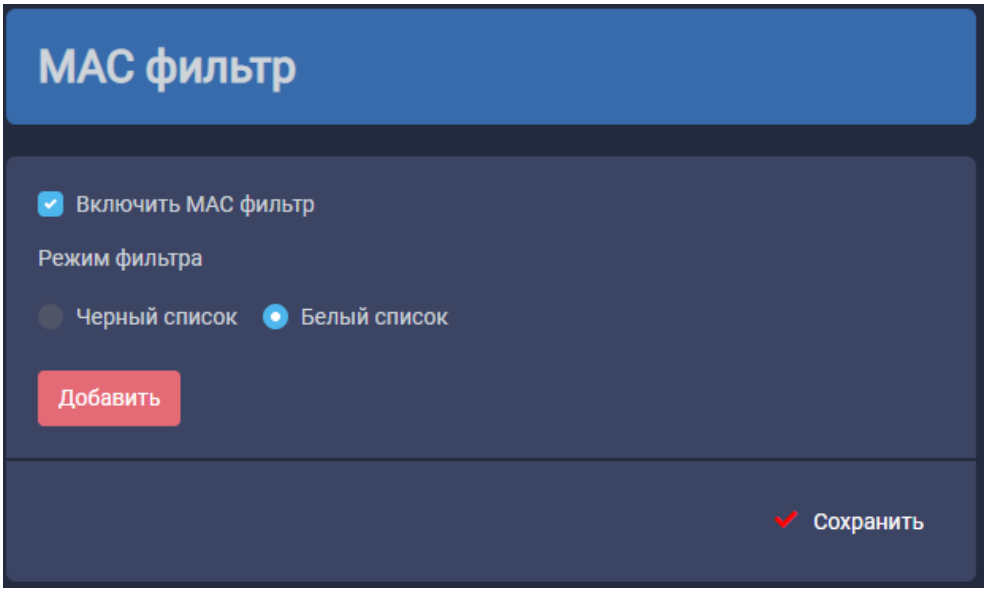


Рисунок 31 – Настройка MAC фильтра

Чтобы задействовать фильтр, поставьте галочку напротив **Включить MAC фильтр**. Далее необходимо будет выбрать принцип, по которому будет работать фильтрация, выбрав одно из значений в подразделе **Режим фильтра**:

- Черный список – адреса, добавленные в данный список, будут блокироваться, со всеми остальными адресами работа будет разрешена;
- Белый список – работа с адресами, указанными в данном списке, будет разрешена, все остальные адреса будут блокироваться.

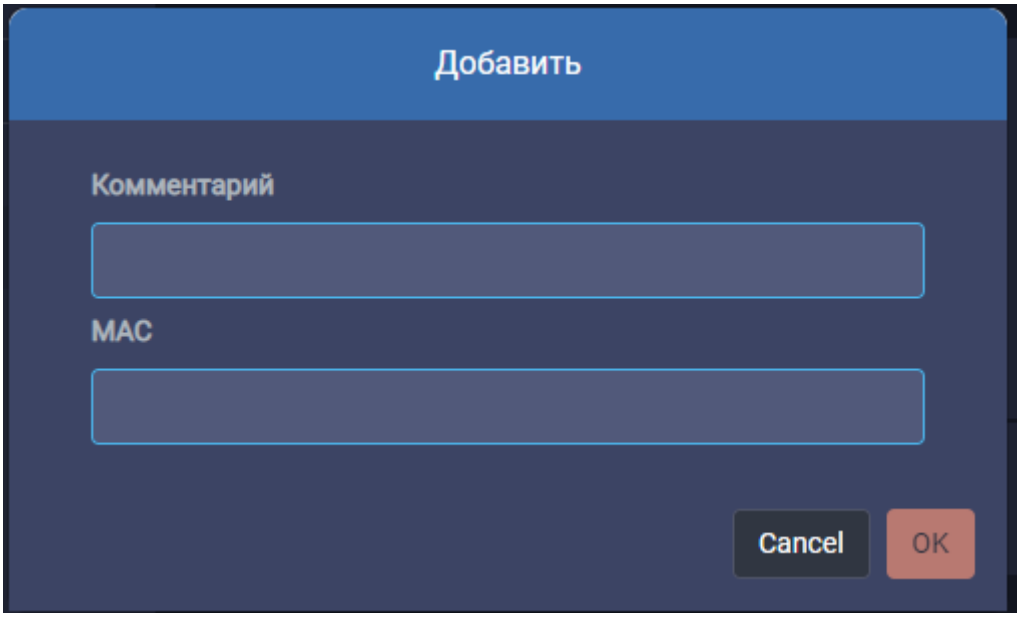


Рисунок 32 – Окно добавления MAC-адреса

1.8.4.3 Firewall

Данный раздел предназначен для настройки межсетевого экрана (файрволла). Настройки разбиты на три подгруппы: **Список зон**, **Контроль трафика**, **Firewall**. На рисунке ниже приведен пример настройки межсетевого экрана.

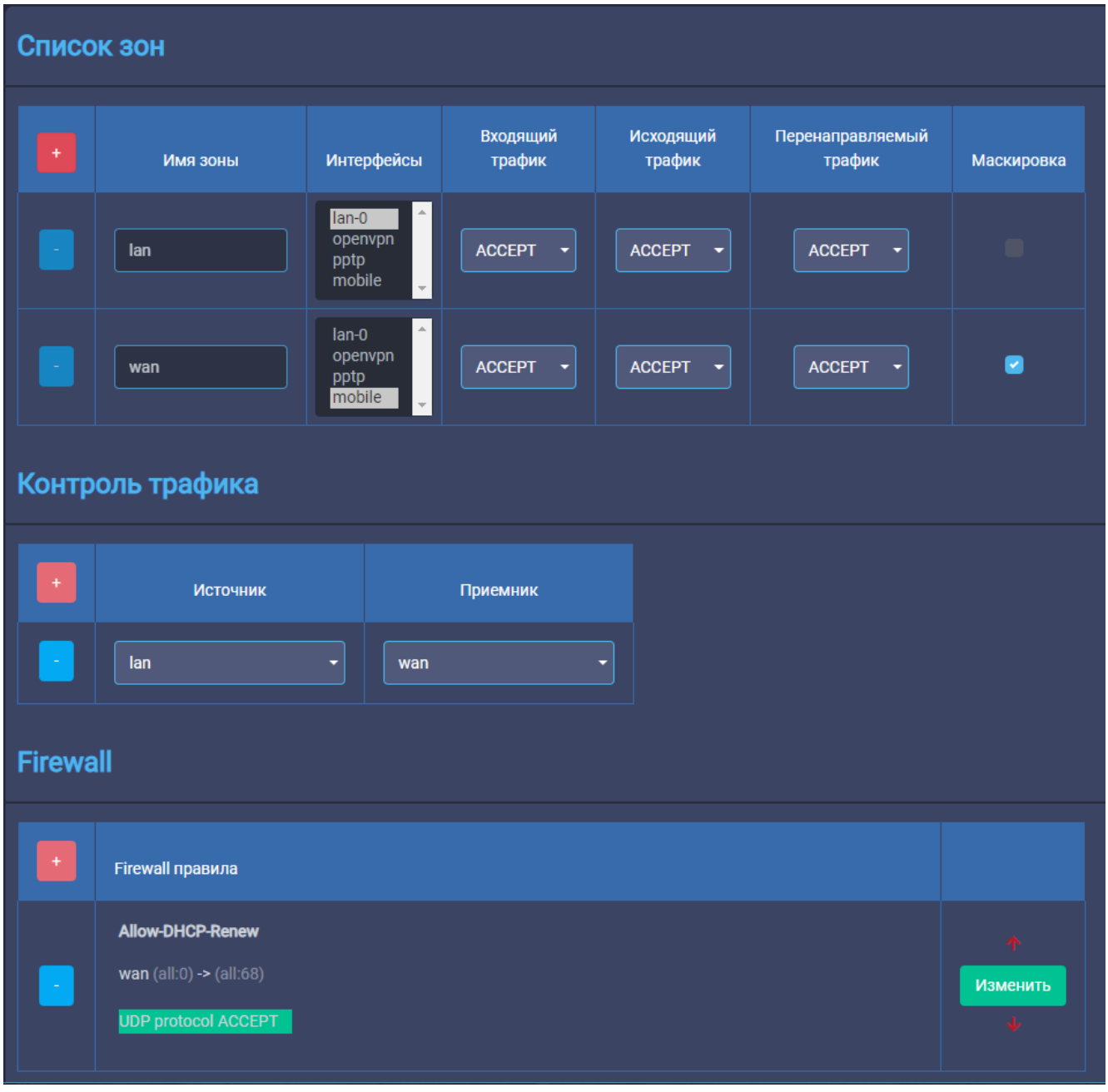


Рисунок 33 – Настройка раздела Firewall

Список зон

Подгруппа настроек **Список зон** отвечает за разбиение на зоны, в которых можно объединять интерфейсы между собой и назначать правила для входящего, исходящего и перенаправляемого трафика.

Таблица 31 – Настройки правил для зон

Поле	Описание
Имя зоны	Имя зоны (по умолчанию, две зоны – LAN и WAN)
Интерфейсы	Выбор интерфейсов роутера, которые будут входить в зону. Для

Поле	Описание
	добавления нескольких интерфейсов в одну зону, интерфейсы выделяются с зажатой кнопкой CTRL.
Входящий трафик	Выбор действия для входящего трафика: **Accept** – принимать, **Reject** – отклонять, **Drop** – отбрасывать, **Notrack** – не отслеживать.
Исходящий трафик	Выбор действия для исходящего трафика: **Accept** – принимать, **Reject** – отклонять, **Drop** – отбрасывать, **Notrack** – не отслеживать.
Перенаправляемый трафик	Выбор действия для перенаправляемого трафика: **Accept** – принимать, **Reject** – отклонять, **Drop** – отбрасывать, **Notrack** – не отслеживать.
Маскировка	Включение/выключение маскировки (маскарадинга) трафика, то есть работы службы NAT

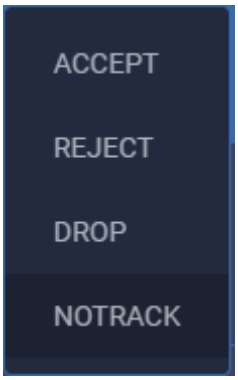


Рисунок 34 – Вариант выбора действий для трафика

Варианты действий для пакетов (поля **Input**, **Output**, **Forward**):

- **Accept** —пакеты трафика принимаются и обрабатываются через межсетевой экран;
- **Reject** — пакеты трафика отклоняются, с ответом;
- **Drop** — пакеты трафика отклоняются без ответа;
- **Notrack** — пакеты трафика принимаюся без обработки межсетевым экраном (соединение не отслеживается).

Контроль трафика

Подгруппа настроек **Контроль трафика** отвечает за контроль трафика между зонами, которые создаются в подгруппе **Список зон**. Можно настроить перенаправление трафика от одного интерфейса к другому, если распределить эти интерфейсы в различные зоны.

В примере на рисунке 33 в зону **LAN** входит интерфейс **lan-0**, а в зону **WAN** – **mobile**.

Правило **LAN → WAN** означает, что трафик с интерфейса **lan-0** (локальные порт) разрешено перенаправлять на WAN-порт и интерфейс SIM-карт. Это правило создано по умолчанию, и если его убрать, то передача трафика от локальных портов в зону **WAN** станет невозможной.

На рисунке ниже приведен внешний вид подраздела **Контроль траффик**а, где:

- **Источник** – интерфейс, являющийся источником траффика;
- **Приемник** – интерфейс, являющийся приемником трафика.

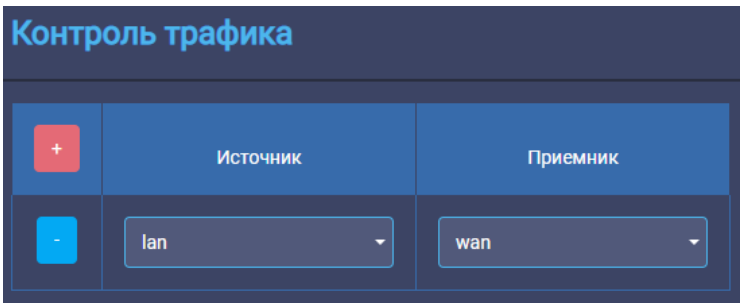


Рисунок 35 – Настройки подраздела Контроль траффика

Firewall

Подраздел **Firewall** отвечает за создание правил для межсетевого экрана. Правила задаются для сетевых протоколов и интерфейсов. Например, указывается направление движение через интерфейсы – «wan(all:all) → (all:68)» (все адреса и порты от зоны WAN на все остальные адреса с портом 68), протокол – UDP, и действие – «Accept» (принимать и обрабатывать).

Добавление нового правила осуществляется нажатием кнопки + (**плюс**) в первом столбце таблицы, удаление маршрута - кнопки - (**минус**) напротив маршрута.

Для редактирования правил используется кнопка **Изменить** напротив соответствующего правила. Изменение приоритета правил, то есть положение в очереди выполнения, где сначала выполняются «верхние» правила, осуществляется посредством кнопок ↑ (**вверх**) и ↓ (**вниз**).

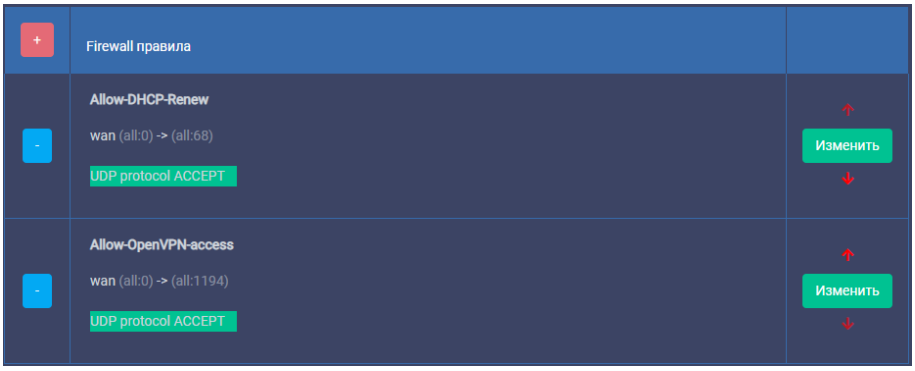


Рисунок 36 – Настройки подраздела Firewall

При добавлении нового правила или редактировании существующего правила, настройки открываются в новом окне, как показано на рисунке ниже.

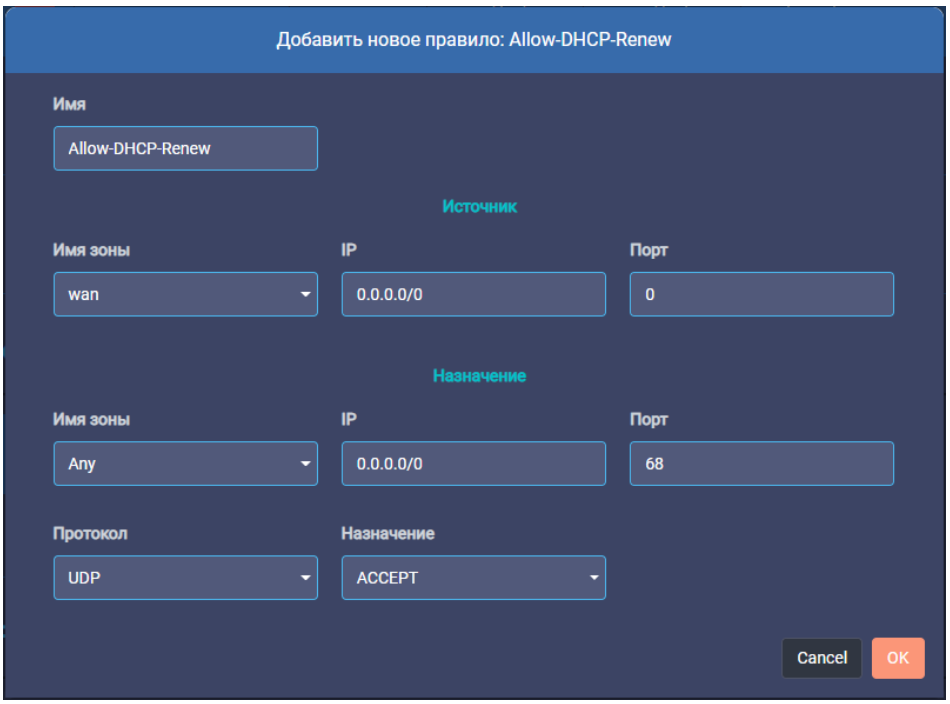


Рисунок 37 – Окно создания нового правила межсетевого экрана

Таблица 32 – Настройки правил для межсетевого экрана

Поле	Описание
Имя	Название правила (произвольное имя на выбор пользователя)
Источник	Подраздел, который отвечает за настройку источника трафика
Назначение	Подраздел, который отвечает за настройку приемника трафика
Имя зоны	Выбор зоны, для которой создается правило. **Any** – любая зона
IP	Ввод диапазона IP-адресов, на которые будет распространятся правило. Адреса вводятся в формате «0.0.0.0/0», в котором, например, «192.168.0.25/150» означает, что правило распространяется на диапазон адресов от 192.168.0.25 до 192.168.0.150. Если значение не указывать, то правило распространяется на любой адрес
Порт	Ввод порта, на который будет распространяться правило. Если значение не указывать, то правило распространяется на любой порт
Протокол	Выбор протокола, на который будет распространяться правило
Назначение	Выбор действия для трафика: **ACCEPT** – принимать, **REJECT** – отклонять, **DROP** – отбрасывать, **NOTRACK** – не отслеживать.

1.8.4.4 Проброс портов

Данный раздел предназначен для настройки проброса портов со стороны WAN-интерфейса на локальные порты роутера. На рисунке ниже приведен пример настройки.

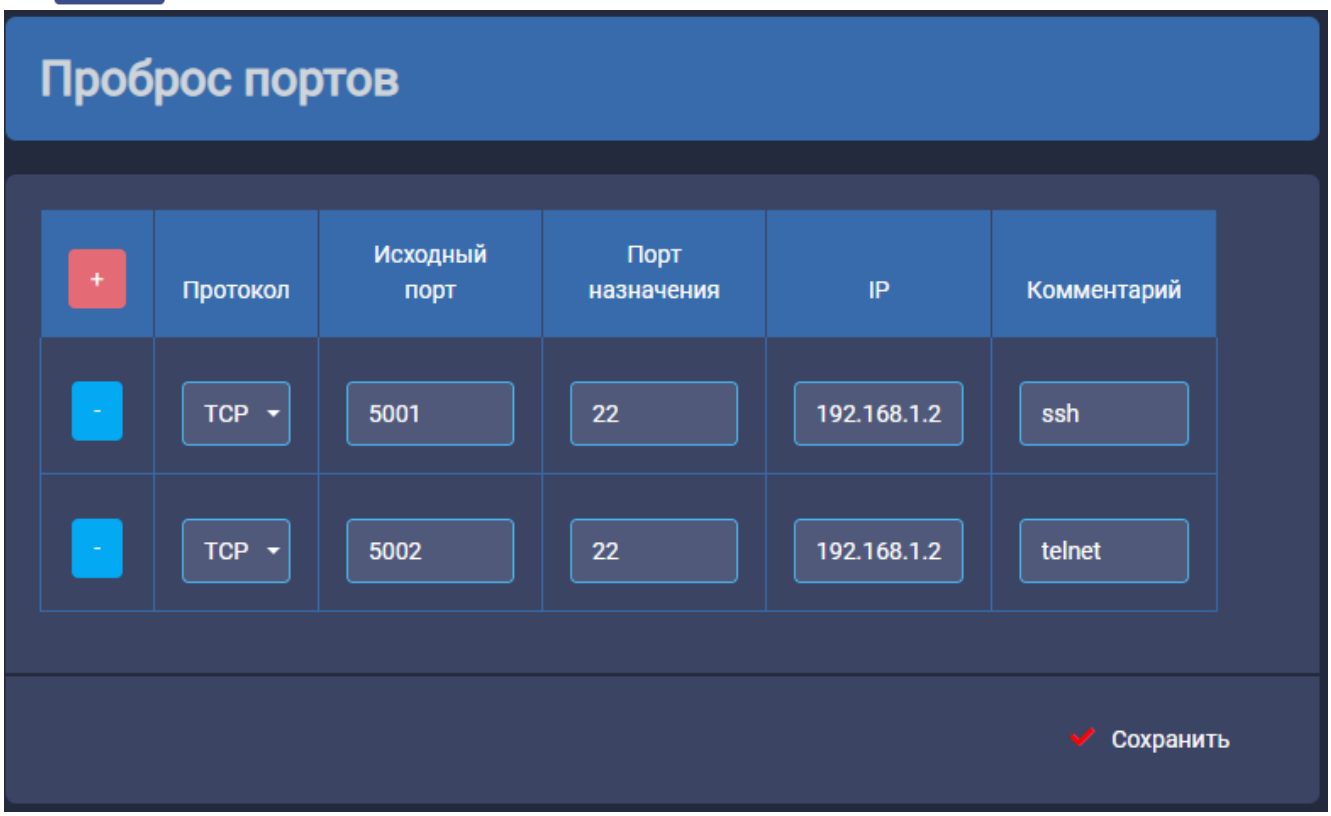


Рисунок 38 – Окно раздела Проброс портов

Таблица 33 – Настройки правил для межсетевого экрана

Поле	Описание
Протокол	Выбор протокола, на который будет распространяться правило: **TCP**, **UDP** или **TCP/UDP** (оба протокола)
Исходный порт	Порт источника трафика, который «прослушивает» роутер на попытки установки соединения
Порт назначения	Порт приемника трафика, на который роутер будет пересылать пакеты
IP	Ввод IP-адреса приемника трафика, на который роутер будет пересылать пакеты
Комментарий	Поле для комментария

1.8.4.5 VRRP

Данный раздел предназначен для настройки сетевого протокола VRRP, применяемый для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Фактически создается виртуальный маршрутизатор (роутер) на базе нескольких физических роутеров, для которых назначается один общий IP-адрес, используемый, как шлюз по умолчанию для компьютеров в сети. **Использование VRRP** увеличивает надежность узла, так как при выходя одного из роутеров из строя, узел на базе виртуального маршрутизатора продолжит функционировать. На рисунке ниже приведен пример настройки VRRP.

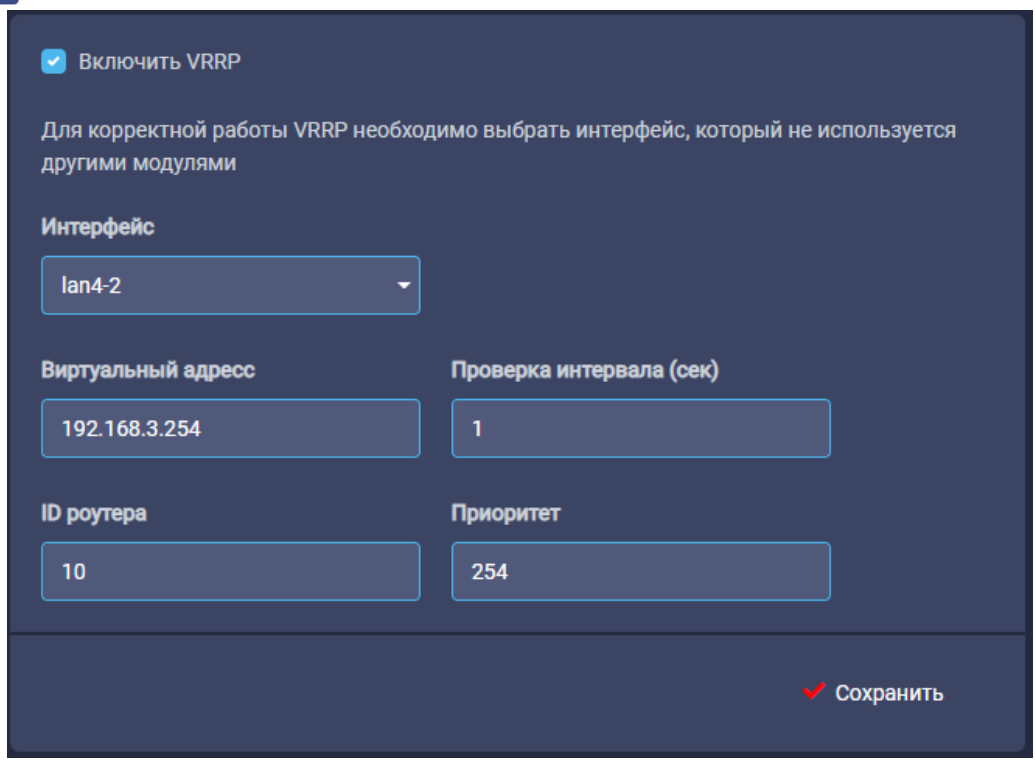


Рисунок 39 – Окно раздела VRRP

Таблица 34 – Настройки VRRP

Поле	Описание
Интерфейс	Выбор интерфейса, через который будет работать VRRP.
Виртуальный адрес	IP-адрес, который будет использоваться для виртуального маршрутизатора
Проверка интервала (сек)	Интервал времени в секундах, через который будет проверяться доступность Master-маршрутизатора
ID роутера	Цифровой идентификатор роутера, значение от «1» до «255»
Приоритет	Приоритет виртуального маршрутизатора, который отправляет пакет, значение от «1» до «255». Чем больше цифра, тем выше приоритет (255 – Master, 1-254 – остальные маршрутизаторы, 0 – выход Master-маршрутизатора из группы)

1.8.4.6 Время

Данный раздел предназначен для настройки текущего времени на устройстве. В поле **Источник данных о времени** позволяет выбрать способ установки текущего времени:

- **auto** – автоматический режим, в котором устройство будет получать данные о текущем времени от внешних серверов — NTP;
- **manual** – установка времени в ручном режиме, на основе данных, внесенных пользователем.

Если в поле **Источник данных о времени** выбран режим **manual**, то для настройки времени необходимо внести данные в соответствующие поля: **Год**, **Месяц**, **День**, **Часы**, **Минуты**, **Секунды**, **Часовой пояс**. На рисунке ниже приведен пример настройки времени в ручном режиме.

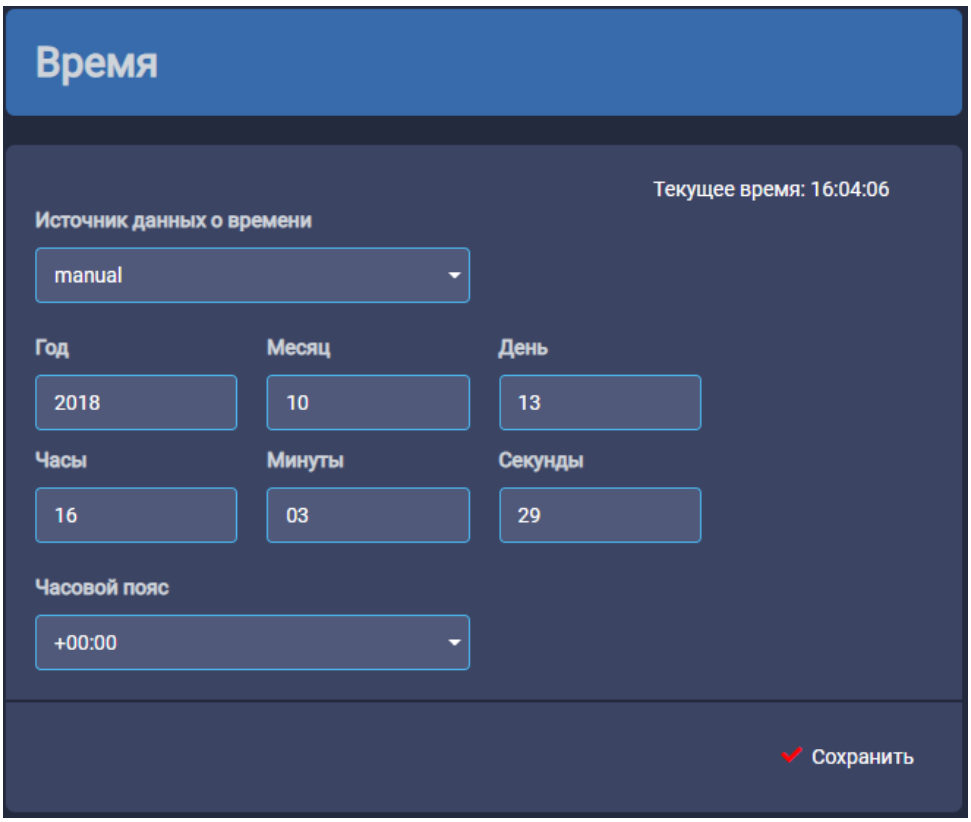


Рисунок 40 – Настройка времени в ручном режиме

Если в поле **Источник данных о времени** выбран режим **auto**, то для настройки времени необходимо указать IP- адреса или доменные имена для двух внешних NTP-серверов, с которых будут браться данные о текущем времени: основной сервер указывается **Основной NTP сервер**, а второстепенный сервер – **Дополнительный NTP сервер**. Дополнительно указывается часовой пояс в поле **Часовой пояс**, если роутер находится в отличном часовом поясе от серверов.

Также на базе роутера можно создать собственный NTP-сервер. Для этого настройте параметры времени и поставьте галочку напротив **Enable NTP server**. В этом случае клиенты локальной сети роутера, чтобы получать данные о текущем времени от этого сервера, должны указывать в настройках времени в поле с указанием сервера адреса этого роутера.

На рисунке ниже приведен пример настройки времени в автоматическом режиме.

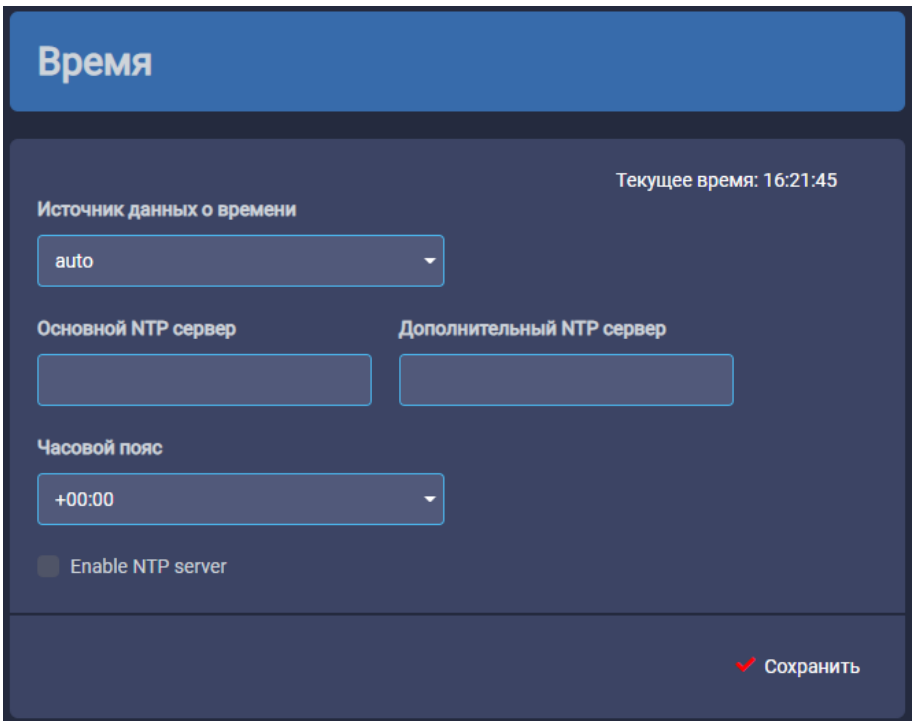


Рисунок 41 – Настройка синхронизации времени в автоматическом режиме

1.8.4.7 SNMP

Данный раздел предназначен для настройки системы мониторинга роутера по протоколу SNMP. С помощью SNMP можно контролировать (проводить мониторинг) подключенные к сети устройства. На рисунках ниже приведены примеры настройки SNMP для двух версий протокола – v2c и v3.

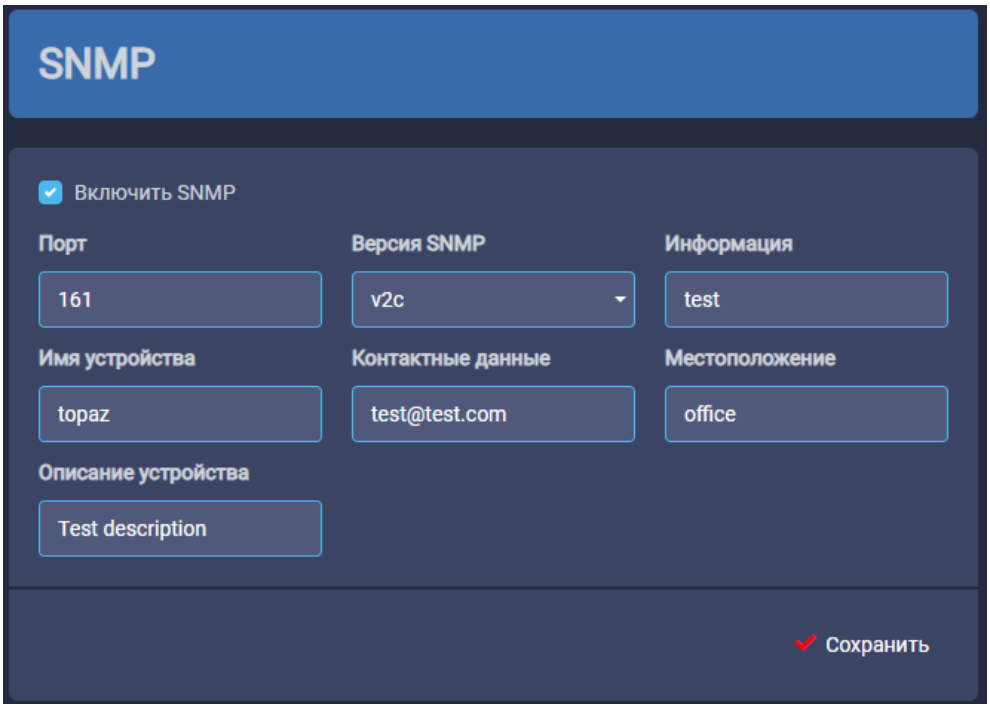


Рисунок 42 – Настройка SNMP v2c

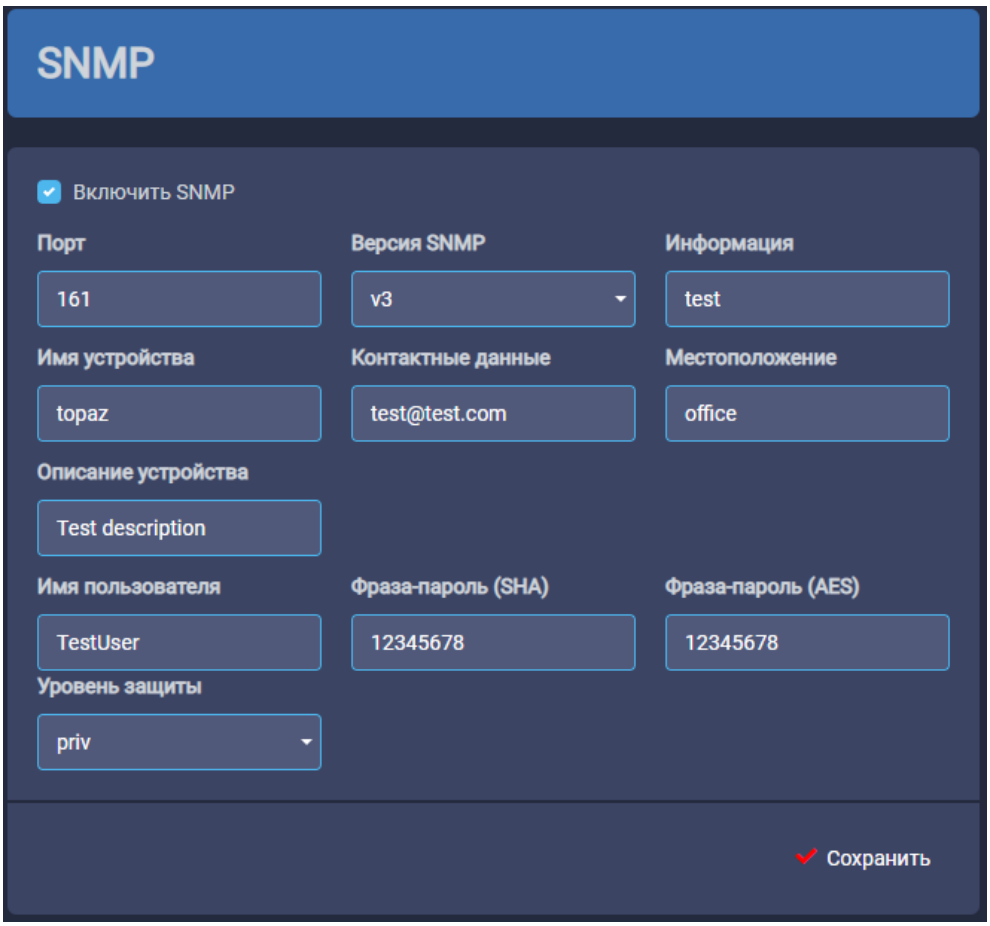


Рисунок 43 – Настройка SNMP v3

Таблица 35 – Настройки SNMP

Поле	Версия	Описание
Порт	v2c, v3	Порт, через который будет работать протокол SNMP. По умолчанию – «161»
Версия SNMP	v2c, v3	Выбор версии протокола: v2c, v3
Информация	v2c, v3	«Общая строка», по которой роутер предоставляет данные для системы мониторинга
Имя устройства	v2c, v3	Имя устройства, которое будет использоваться для идентификации данного устройства в системе мониторинга
Контактные данные	v2c, v3	Контактные данные в виде электронного адреса, телефона или другого вида
Местоположение	v2c, v3	Описание местоположения устройства
Описание устройства	v2c, v3	Описание устройства
Имя пользователя	v3	Имя пользователя для авторизации при контроле роутера по протоколу SNMP
Фраза-пароль (SHA)	v3	Фраза-пароль для шифрования авторизации при контроле роутера по протоколу SNMP, используется алгоритм хэширования SHA
Фраза-пароль (AES)	v3	Фраза-пароль для шифрования передаваемого трафика от роутера к системе мониторинга, при контроле роутера по протоколу SNMP, используется алгоритм шифрования AES

Поле	Версия	Описание
Уровень защиты	v3	Выбор уровня защиты при работу с устройством по протоколу SNMP: **noauth** – авторизация на устройстве не установлена; **auth** – установлена авторизация; **priv** – установлена авторизация и шифрование данных при передаче по протоколу.

1.8.4.8 DynDNS

Данный раздел предназначен для настройки DynDNS – метода автоматического обновления записей DNS-сервера. Данный метод применяется для автоматического определения IP-адреса роутера по его доменному имени, когда роутеру выделяется динамический IP-адрес. На рисунке ниже представлен пример настройки DynDNS.

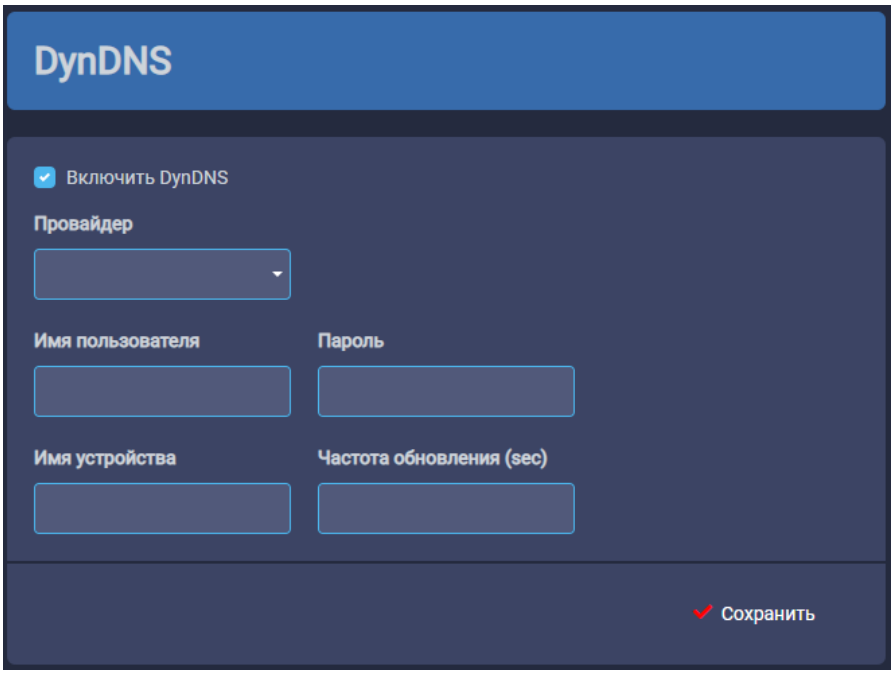


Рисунок 44 – Раздел DynDNS

Таблица 36 – Настройки DynDNS

Поле	Описание
Провайдер	Выбор провайдера услуги динамического DNS. В роутерах TOPAZ предустановлены основные настройки для нескольких распространенных провайдеров. Для настройки собственного сервера, выберите **custom** и пропишите необходимые настройки
Имя пользователя	Имя пользователя для авторизации на сервере DynDNS
Пароль	Пароль для авторизации на сервере DynDNS
Имя устройства	Имя устройства (хоста)
Частота обновления (sec)	Интервал в секундах, через который будет обновляться информация на сервера
Remote URL	Строка URL-адреса с параметрами подключения к серверу DynDNS

В поле **Провайдер** указывается провайдер услуги динамического DNS. В роутерах TOPAZ имеется возможность использовать свой собственный сервис динамического DNS или один из четырех предустановленных распространенных сервисов.

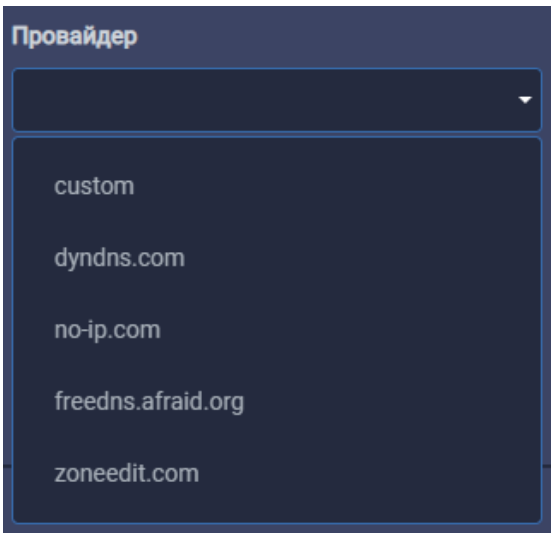


Рисунок 45 – Выбор провайдера

1.8.4.9 Планировщик задач

Данный раздел предназначен для настройки выполнения команд по расписанию. Для этого требуется добавить инструкцию, указать время и саму команду.

Отметка в столбце **Включить** позволяет включать, или отключать выполнение инструкции без ее удаления. Сама команда указывается в поле **Команда**. Время указывается в полях:

- Минуты (минута, от «0» до «59»);
- Часы (час, от «0» до «23»);
- День (день, от «1» до «31»);
- Месяц (месяц, от «1» до «12»);
- Неделя (неделя месяца).

Пример внешнего вида планировщика задачи приведен на рисунке ниже.

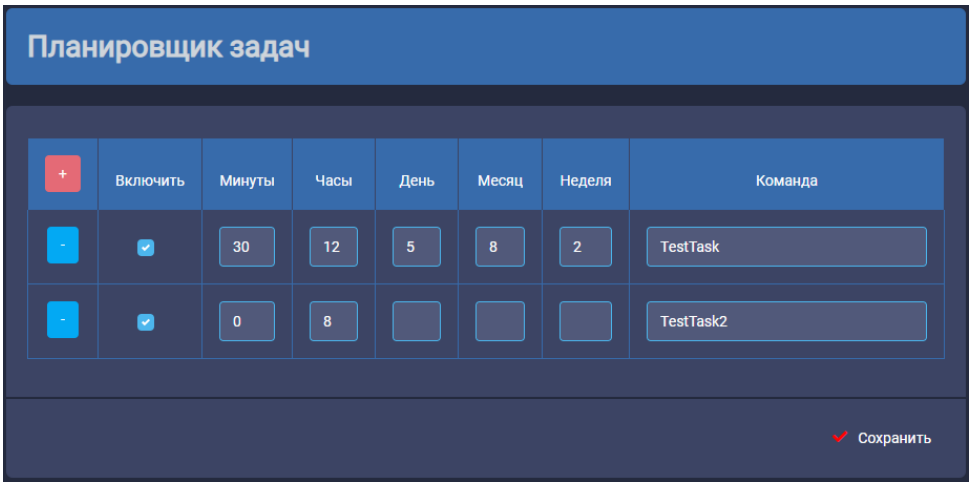


Рисунок 46 – Раздел Планировщик задач

1.8.4.10 SMS команда

Данный раздел предназначен для настройки выполнения команд управления роутером через SMS-сообщения. Для этого требуется добавить инструкцию, указать команду, придумать и указать для команды ключевое слово, и, при желании ограничить доступ к управлению роутером, номер (или номера) мобильного телефона, с которого она может быть отправлена.

Отметка в столбце **Включить** позволяет включать, или отключать выполнение инструкции без ее удаления. Выполняемая команда указывается в поле **Команда**. В качестве SMS-команды можно использовать стандартные команды Linux либо самописные скрипты, предварительно сохраненные в памяти роутера. Для скриптов и команд необходимо указывать их полный путь. На рисунке ниже приведен пример SMS-команды перезагрузки роутера с помощью стандартной консольной команды **reboot**.

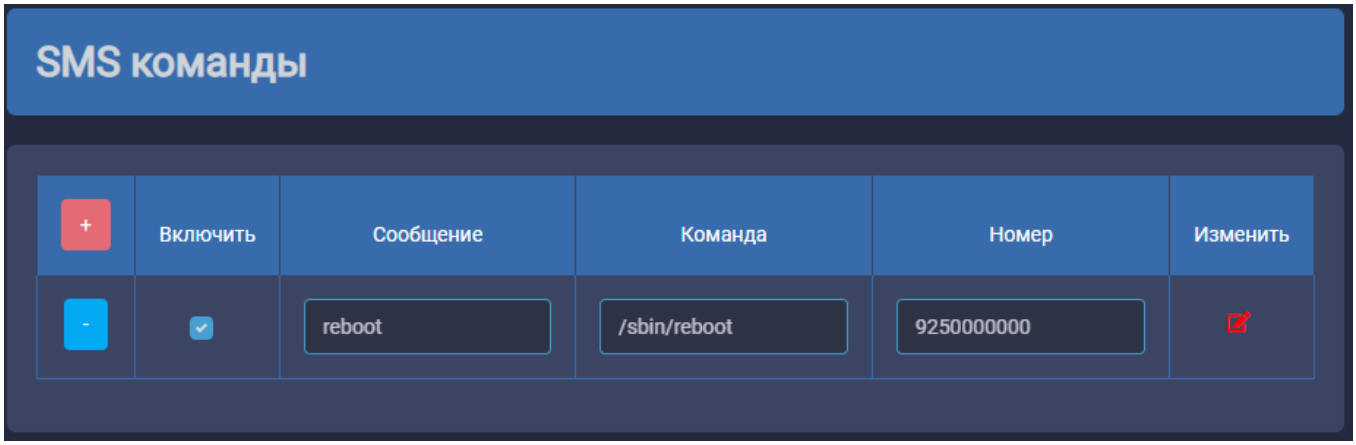


Рисунок 47 – SMS-команда перезагрузки роутера

В поле **Сообщение** указывается ключевая фраза, которая будет содержаться в SMS-сообщении для выполнения команды из поля **Команда**. Это сделано для удобства, чтобы не набирать на телефоне настоящую длинную команду, вместо этого можно отправлять короткие ключевые фразы. Соответственно, ключевые фразы придумывает пользователь на собственное усмотрение.

В поле в столбце **Номер** указывается телефонный номер (если номеров несколько, они разделяются пробелами) в формате **[код оператора][номер]**, с которого можно выполнять команду из поля **Команда**. Если данное поле оставить пустым, то команда при правильном ключевом слове будет выполняться по SMS, пришедшей с любого номера.

1.8.4.11 RS over TCP

Данный раздел предназначен для настройки работы роутера с портами RS-485 (RS-232).

В роутерах TOPAZ работа по стандарту RS-232/RS-485 ограничивается приемом данных по линии Rx и передачей данных по линии Tx. Приняв данные по линии Rx роутер инкапсулирует полученные данные в IP-пакет, и в соответствии с настройками отсылает их на удаленный хост. И наоборот, получив IP-пакет, на указанный в настройках порт, роутер распаковывает IP-пакет и передает его по линии Tx на подключенное устройство.

Для каждого порта RS-485(RS-232) предусмотрены режимы работы:

- **Сервер** — роутер ждет входящего подключения на указанный порт, устанавливается соединения и начинается передача данных;
- **Клиент** — роутер устанавливает соединение по указанному IP-адресу и порту, и начинает передачу данных.
- **Отключить** — работа с портом RS232/485 отключена.

На рисунке ниже приведен пример настройки работы роутера с портом RS-485 в режиме сервера.

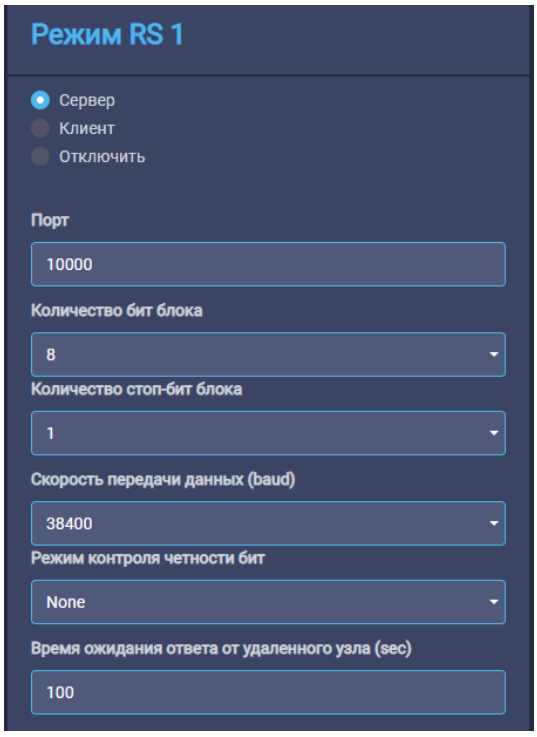


Рисунок 48 – Режим работы с портом RS-485-1 в режиме сервера

На рисунке ниже приведен пример настройки работы роутера с портом RS-485 в режиме клиента.

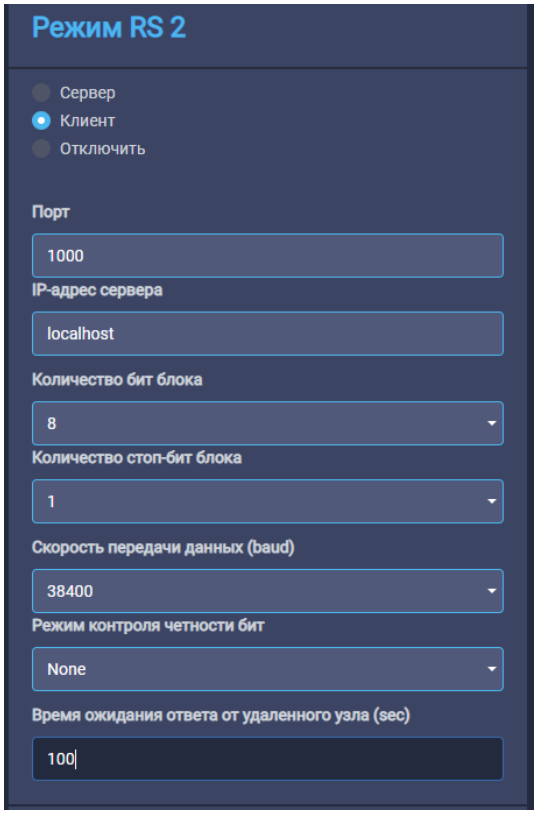


Рисунок 49 – Режим работы с портом RS-485-2 в режиме клиента

Таблица 37 – Настройки портов через TCP (C – клиент, S – сервер)

Поле	Режим	Описание
Порт	C, S	Порт, через который будет осуществляться передача данных
IP-адрес сервера	C	IP-адрес сервера, к которому будет подключаться устройство для передачи данных
Количество бит блоков	C, S	Количество бит блока, используемых при передаче данных: **7**, **8**
Количество стоп-бит блока	C, S	Количество стоп-бит блока, используемые для определения конца блока: **1**, **2**
Скорость передачи данных (baud)	C, S	Скорость передачи данных через порт, в бод
Режим контроля четности бит	C, S	Режим контроля четности бит в передаваемых блоках: – **None** – без проверки; – **Odd** – проверка на нечетность; – **Even** – проверка на четность.
Время ожидания ответа от удаленного узла (sec)	C, S	Время ожидания ответа от удаленного узла, в секундах, при установке соединения или перед отправкой данных

1.8.5 **Раздел Настройки**

1.8.5.1 Доступ

Данный раздел предназначен для настройки доступа управления роутером по протоколу SSH. По умолчанию доступ к устройству по SSH разрешен.

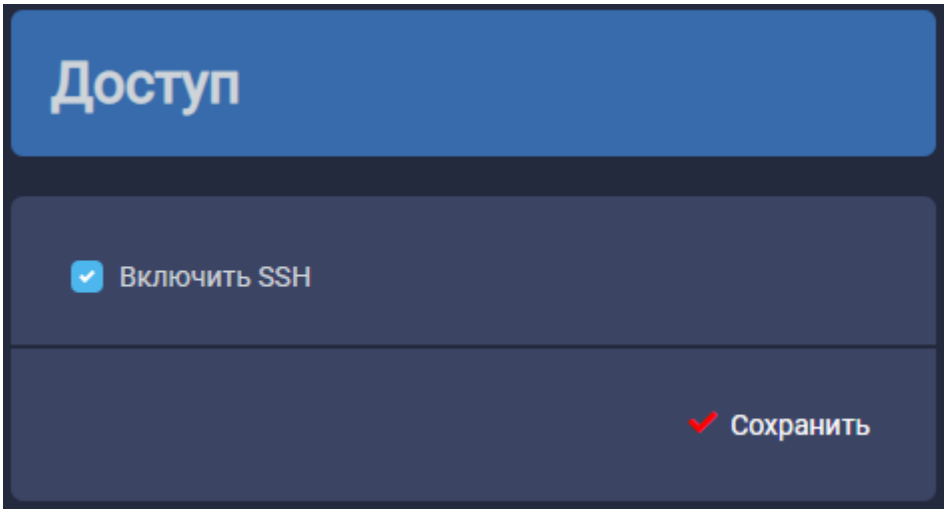


Рисунок 50 – Раздел Доступ

1.8.5.2 Изменить пароль

Данный раздел предназначен для изменения пароля для доступа к устройству через WEB-интерфейс. Для изменения пароля:

- Введите старый пароль доступа к устройству в поле **Старый пароль**;
- Введите новый пароль в поле **Новый пароль**;
- Нажмите кнопку **Сохранить** внизу страницы.

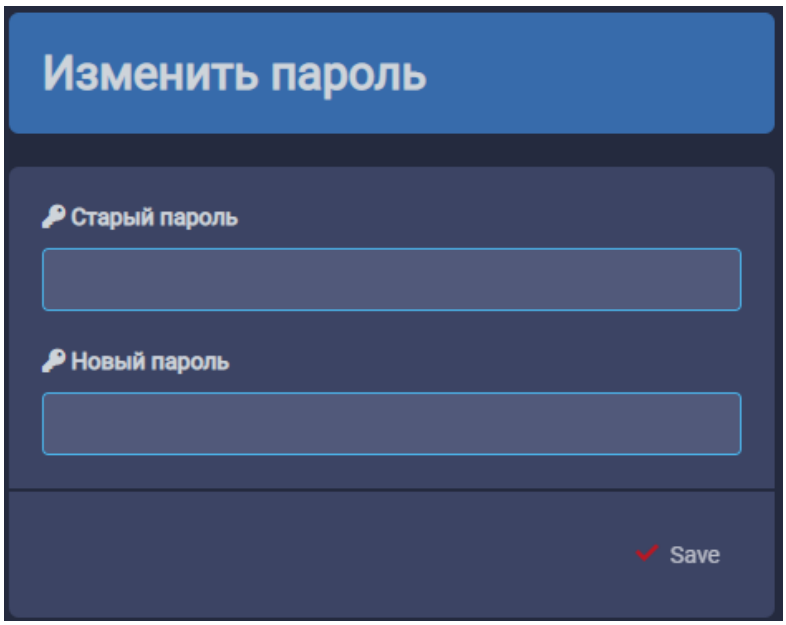


Рисунок 51 – Раздел Изменить пароль

1.8.5.3 Имя устройства

Данный раздел предназначен для изменения названия устройства, которое отображается в веб-интерфейсе.

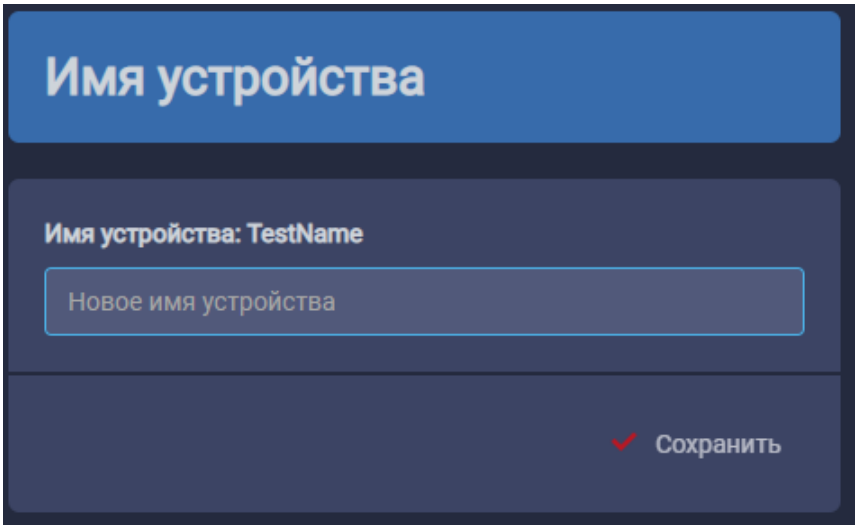


Рисунок 52 – Раздел Имя устройства

1.8.5.4 Отправить SMS

Данный раздел предназначен для отправки SMS-сообщения на указанный номер. SMS-сообщение отправляется через активную в настоящий момент SIM-карту. В роутере должна быть установлена SIM-карта с активной услугой, и необходимым балансом средств, а само устройство должно находиться в зоне покрытия оператора, предоставившего SIM-карту.

Для отправки сообщения в поле **Номер получателя** необходимо указать телефонный номер в формате **[код оператора][номер]**, а в поле **Сообщение** текст сообщения, после чего нажать кнопку **Отправить**.

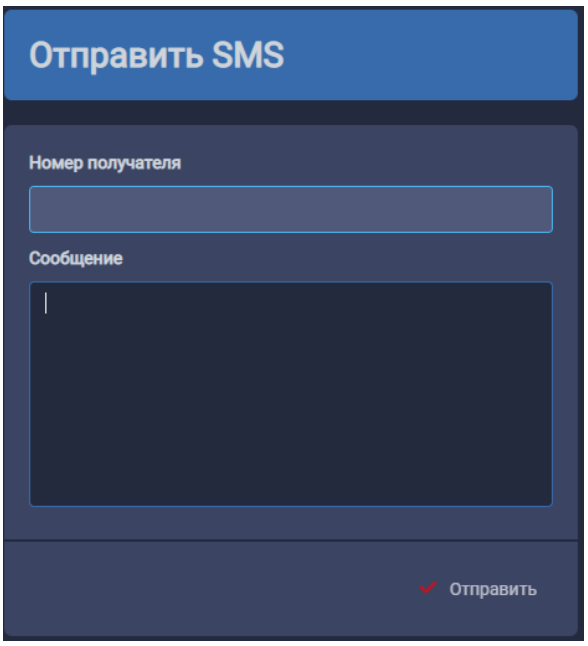


Рисунок 53 – Раздел Отправить SMS

1.8.5.5 Ping

Данный раздел предназначен для проверки соединения с удаленным узлом.
Чтобы проверить соединение:

- Введите IP-адрес удаленного узла в поле **Узел**;
- Введите количество ICMP-пакетов, которые нужно отправить при проверке в поле **Количество**;
- Укажите размер ICMP-пакета в поле **Размер дейтаграммы**;
- Нажмите кнопку **Ping**, внизу страницы, и в главном окне посередине экрана появится результат проверки.

На рисунке ниже представлен пример полей для заполнения.

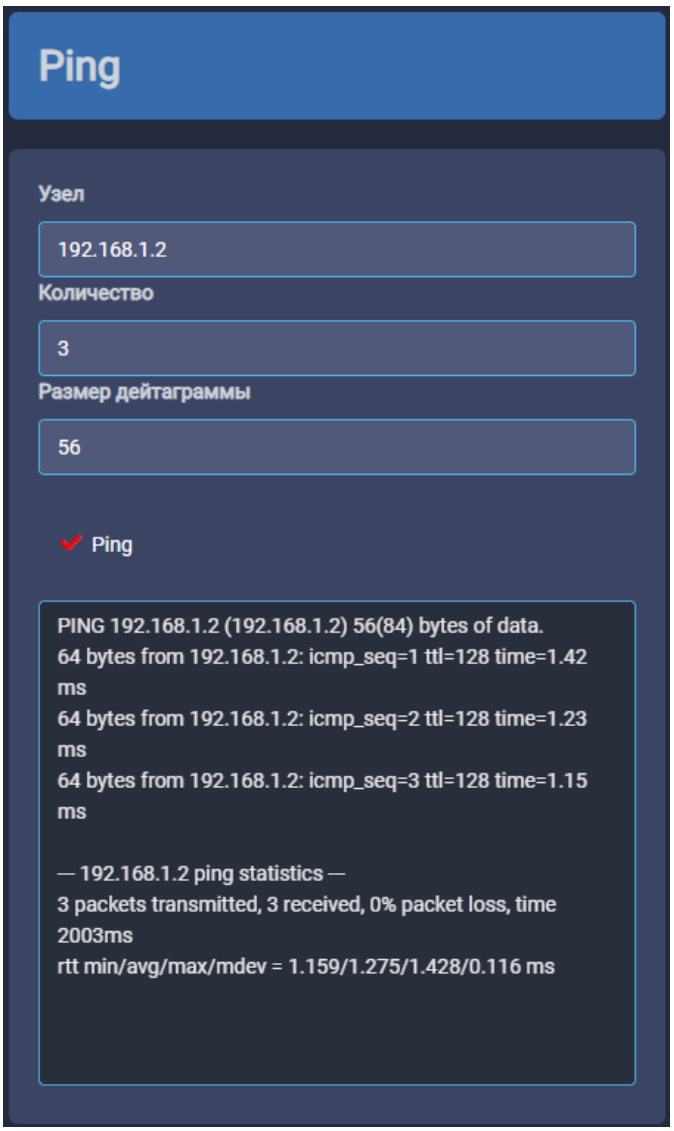


Рисунок 54 – Раздел Ping

1.8.5.6 System Log

Данный раздел предназначен для работы с системным логом устройства. Данные из системного лога устройства можно пересылать по протоколу Syslog на удаленный адрес, для этого:

- Поставьте галочку напротив **Включить удаленное логирование**;
- Укажите удаленный IP-адрес в поле **Удаленный IP-адрес**, а порт в поле Порт;
- Нажмите кнопку **Сохранить**, внизу блока.

С помощью кнопки **Отчет** можно получить файл с полным логом устройства, включающим в себя логи работы и все его настройки. Сам системный лог устройства можно увидеть в центральном окне, как показано на рисунке ниже.

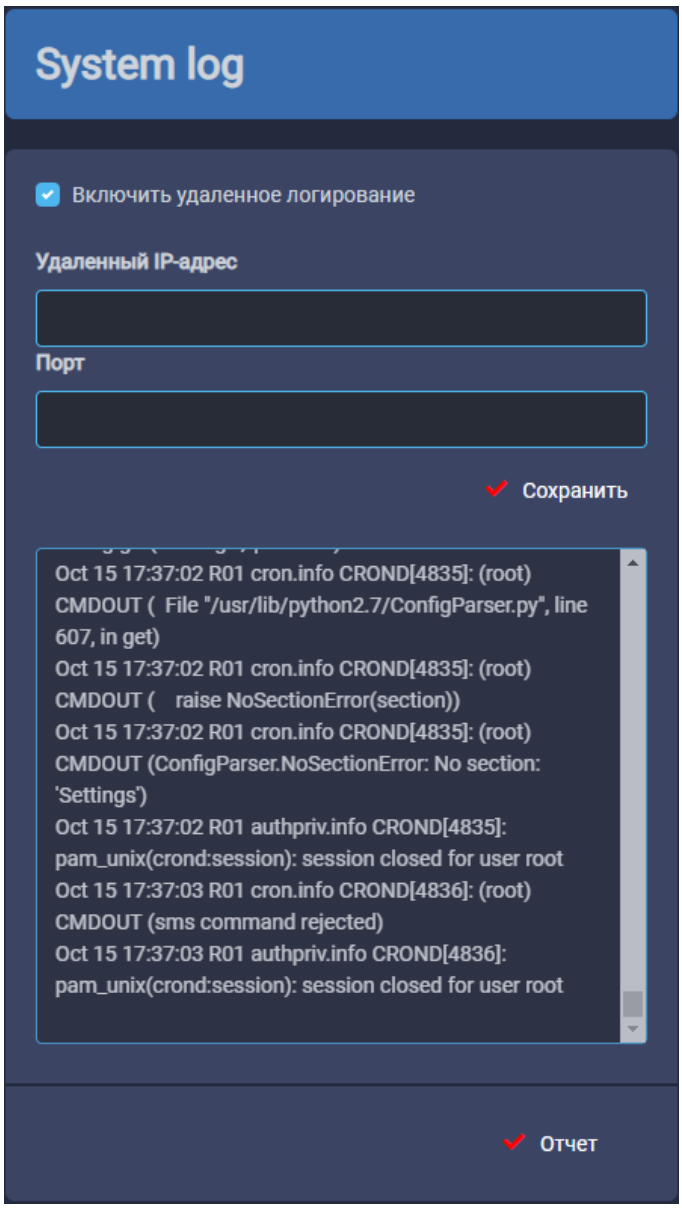


Рисунок 55 – Раздел System log

1.8.5.7 GPIO

Данный раздел предназначен для настройки универсальных каналов дискретного ввода/вывода роутера (при наличии в исполнении). На рисунке ниже приведен пример настройки GPIO.

Рисунок 56 – Раздел GPIO

Данные порты могут работать как на вход, так и на выход. Настройки портов приведены в таблице ниже.

Таблица 38 – Настройки GPIO

Поле	Описание
Имя	Имена входов/выходов (также см. руководство по эксплуатации)
Направление	Выбор направления работы: **IN** – работает, как вход, **OUT** – выход
Уровень выходного сигнала	Уровень выходного сигнала (только для выходов): – **HIGH** – высокий уровень напряжения/тока; – **LOW** – низкий уровень напряжения/тока.
Сбросить	Сброс текущих настроек GPIO, и установка настроек по умолчанию

1.8.5.8 Перезагрузка

Данный раздел предназначен для перезагрузки устройства. Чтобы перезагрузить устройство, нажмите кнопку **Перезагрузить**.

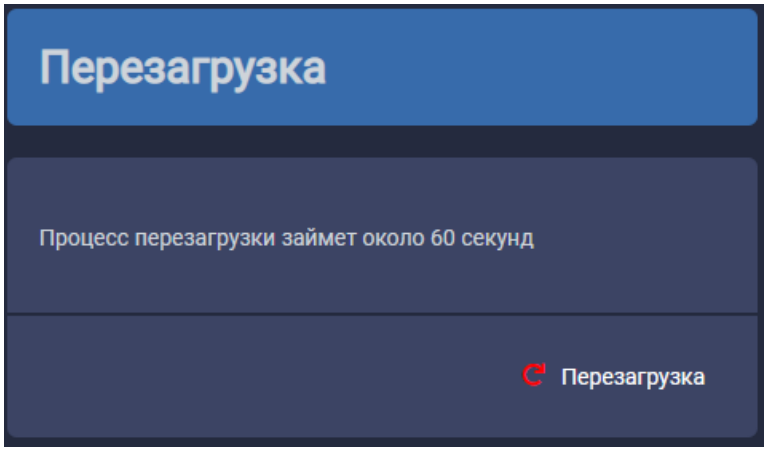


Рисунок 57 – Раздел Перезагрузка

1.8.5.9 Управление и настройка ПО

Данный раздел предназначен для управления настройками роутера. В данном разделе можно произвести сохранение всех сделанных настроек в файл и их восстановление из файла, возможность установить дополнительный программный пакет или сбросить роутер на заводские настройки.

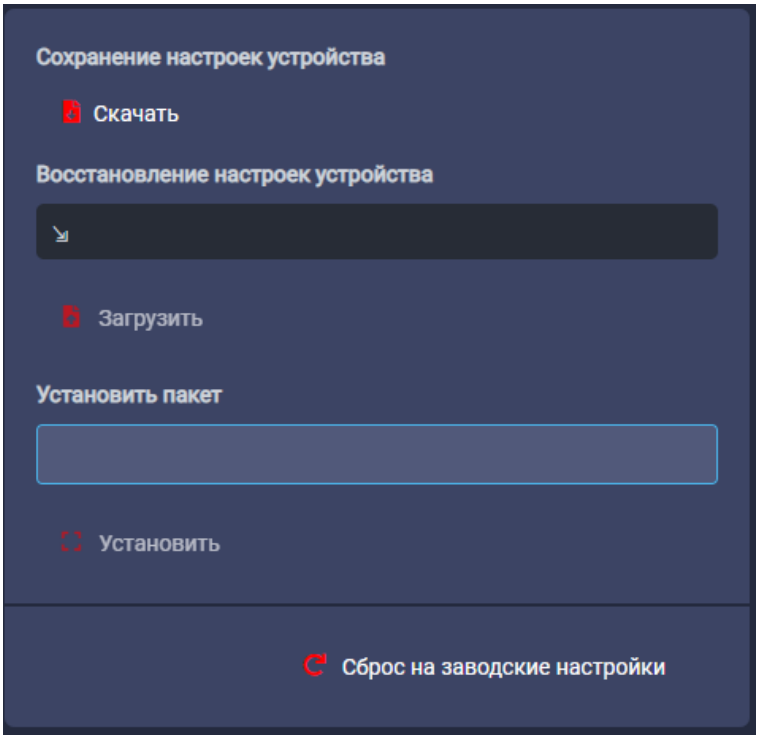


Рисунок 58 – Раздел Управление и настройка ПО

Сохранение настроек устройства

Нажмите кнопку **Скачать** и сохраните полученный файл в компьютере.

Восстановление настроек устройства

Нажмите на поле **Восстановление настроек устройства** и выберите ранее сохраненный файл с настройками, после чего нажмите кнопку **Загрузить**.

Установка дополнительных пакетов на устройство.

Введите расположение и имя файл-пакета в поле **Установить пакет**, а затем нажмите кнопку **Установить**, чтобы использовать пакет в устройстве.

Сброс на заводские настройки

Для сброса на заводские настройки нажмите кнопку **Сброс на заводские настройки**. Данная операция может занять до нескольких минут.

2 МАРКИРОВКА И ПЛОМБИРОВАНИЕ

Вся обязательная информация по маркировке нанесена на лицевой и боковой панели. Маркировка выполнена способом, обеспечивающим ее сохранность на все время эксплуатации устройства. Перечень информации, содержащейся в маркировке на лицевой панели:

- наименование и условное обозначение;
- назначение светодиодов устройства;
- назначение клеммных соединений и разъемов устройства.
- Перечень информации, содержащейся в маркировке на боковой панели:
- наименование и условное обозначение;
- товарный знак;
- порядковый номер по системе нумерации предприятия-изготовителя;
- дата изготовления;

Для предотвращения несанкционированного доступа к внутренним электрическим элементам корпус устройства должен быть опломбирован путем нанесения саморазрушающейся наклейки.

3 УПАКОВКА

Устройства размещается в коробке из гофрированного картона.

Эксплуатационная документация уложена в потребительскую тару вместе с устройством.

В потребительскую тару вложена товаросопроводительная документация, в том числе упаковочный лист, содержащий следующие сведения:

- наименование и условное обозначение;
- дату упаковки;
- подпись лица, ответственного за упаковку.

4 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

Техническое обслуживание устройства заключается в профилактических осмотрах.

При профилактическом осмотре должны быть выполнены следующие работы:

- проверка обрыва или повреждения изоляции проводов и кабелей;
- проверка надежности присоединения проводов и кабелей;
- проверка отсутствия видимых механических повреждений, а также пыли и грязи на корпусе устройства.

Периодичность профилактических осмотров устройства устанавливается потребителем, но не реже 1 раз в год.

Эксплуатация устройства с повреждениями категорически запрещается.

5 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ

Транспортирование устройств должно производиться в упаковке предприятия-изготовителя любым видом транспорта, защищающим от влияний окружающей среды, в том числе авиационным в отапливаемых герметизированных отсеках самолетов.

Размещение и крепление в транспортных средствах упакованных устройств должно обеспечивать его устойчивое положение, исключать возможность ударов друг о друга, а также о стенки транспортных средств.

Укладывать упакованные устройства в штабели следует с правилами и нормами, действующими на соответствующем виде транспорта, чтобы не допускать деформации транспортной тары при возможных механических перегрузках.

При погрузке и выгрузке запрещается бросать и кантовать устройства.

После продолжительного транспортирования при отрицательных температурах приступать к вскрытию упаковки не ранее 12 часов после размещения устройств в отапливаемом помещении.

Устройства следует хранить в невскрытой упаковке предприятия-изготовителя на стеллаже в сухом отапливаемом и вентилируемом помещении, при этом в атмосфере помещения должны отсутствовать пары агрессивных жидкостей и агрессивные газы.

Средний срок сохранности в потребительской таре в отапливаемом помещении, без консервации - не менее 2 лет.

нормальные климатические факторы хранения:

- температура хранения +20 ± 5 ^{0}C;
- значение относительной влажности воздуха: 30-80 %.

Предельные климатические факторы хранения:

- температура хранения от -40 до +70 ^{0}C;
- значение относительной влажности воздуха: верхнее 100% при 30^{0}C.

6 УТИЛИЗАЦИЯ

Устройства не представляют опасности для жизни, здоровья людей и окружающей среды.

Устройства не содержат драгоценных и редкоземельных металлов.

После окончания срока службы, специальных мер по подготовке и отправке устройств на утилизацию не предусматривается.

7 ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ

7.1 Эксплуатационные ограничения и меры безопасности

К эксплуатации устройства должны допускаться лица, изучившие настоящее руководство по эксплуатации и обладающие базовыми знаниями в области средств вычислительной техники.

Устройство может размещаться вне взрывоопасных зон как на открытом воздухе, так и в помещении. При этом устройство должен быть защищен от прямого воздействия атмосферных осадков. Рабочее положение – вдоль DIN-рейки.

Для нормального охлаждения устройства, а также для удобства монтажа и обслуживания, при монтаже устройства сверху и снизу необходимо предусмотреть свободное пространство не менее 40 мм. Принудительная вентиляция не требуется.

- Производитель не несет ответственность за ущерб, вызванный неправильным монтажом, нарушением правил эксплуатации или использованием оборудования не по назначению.
- Во время монтажа, эксплуатации и технического обслуживания оборудования необходимо соблюдать «Правила технической эксплуатации электроустановок потребителей».
- Монтаж и эксплуатацию оборудования должен проводить квалифицированный персонал, имеющий группу по электробезопасности не ниже 3 и аттестованный в установленном порядке на право проведения работ в электроустановках потребителей до 1000 В.
- На лице, проводящем монтаж, лежит ответственность за производство работ в соответствии с настоящим руководством, требованиями безопасности и электромагнитной совместимости.

- В случае возникновения неисправности необходимо отключить питание от устройства, демонтировать и передать его в ремонт производителю.

7.2 Монтаж

7.2.1 Подготовка к монтажу

Распаковывание устройства следует производить после выдержки упаковки в нормальных условиях не менее двух часов.

При распаковывании следует соблюдать следующий порядок операций:

- открыть коробку;
- из коробки извлечь:
  - вкладыш;
  - комплект монтажный;
  - устройство.
- произвести внешний осмотр устройства:
  - проверить отсутствие видимых внешних повреждений корпуса и внешних разъемов;
  - внутри устройства не должно быть незакрепленных предметов;
  - изоляция не должна иметь трещин, обугливания и других повреждений;
  - маркировка устройства, комплектующих изделий должна легко читаться и не иметь повреждений.

7.2.2 Установка на DIN-рейку

Устройство устанавливается в стойку 19” (монтажный кронштейн высотой 3U) или на монтажную рейку (DIN-профиль 35 мм) в следующей последовательности:

- корпус устройства ставится на рейку, цепляясь верхними выступами;
- корпус опускается вниз относительно верхнего выступа до щелчка.

ВНИМАНИЕ! МОНТАЖНАЯ РЕЙКА (МОНТАЖНЫЙ КРОНШТЕЙН) ДОЛЖНА БЫТЬ ЗАЗЕМЛЕНА.

7.2.3 Внешние подключения

Внешние подключения осуществляются с помощью разъемов MSTBT 2,5/4-ST проводами сечением до 1,5 мм^2.

Рисунок 59 – Внешний вид разъема MSTBT 2,5/4-ST

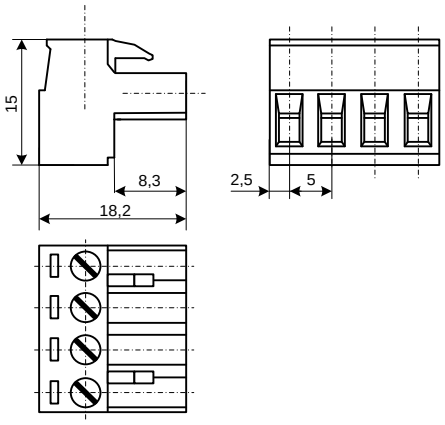


Рисунок 60 – Габаритные размеры разъема MSTBT 2,5/4-ST

ВНИМАНИЕ! ПОДКЛЮЧЕНИЕ К КЛЕММАМ УСТРОЙСТВА ПРОИЗВОДИТЬ ПРИ ОБЕСТОЧЕННОМ ОБОРУДОВАНИИ

ВНИМАНИЕ! ПРИ ПРОВЕРКЕ ГОТОВНОСТИ К РАБОТЕ ПРОВЕРИТЬ ПРАВИЛЬНОСТЬ ПОДКЛЮЧЕНИЙ, КРЕПЛЕНИЕ КЛЕММНИКОВ.

7.2.4 Шина T-BUS

Шина T-BUS представляет собой 5-ти проводную шину, составляемую из произвольного количества единичных Т-образных шинных соединителей ME 22,5 T-BUS 1,5/5-ST-3,81, крепящихся к DIN-рейке с помощью защелок.

Шина T-BUS предназначена для обеспечения питания установленных на ней устройств TOPAZ. Установленные на шине T-BUS устройства, поддерживающие передачу данных по интерфейсу RS-485, также объединяются в единую линию связи RS-485 типа «общая шина».

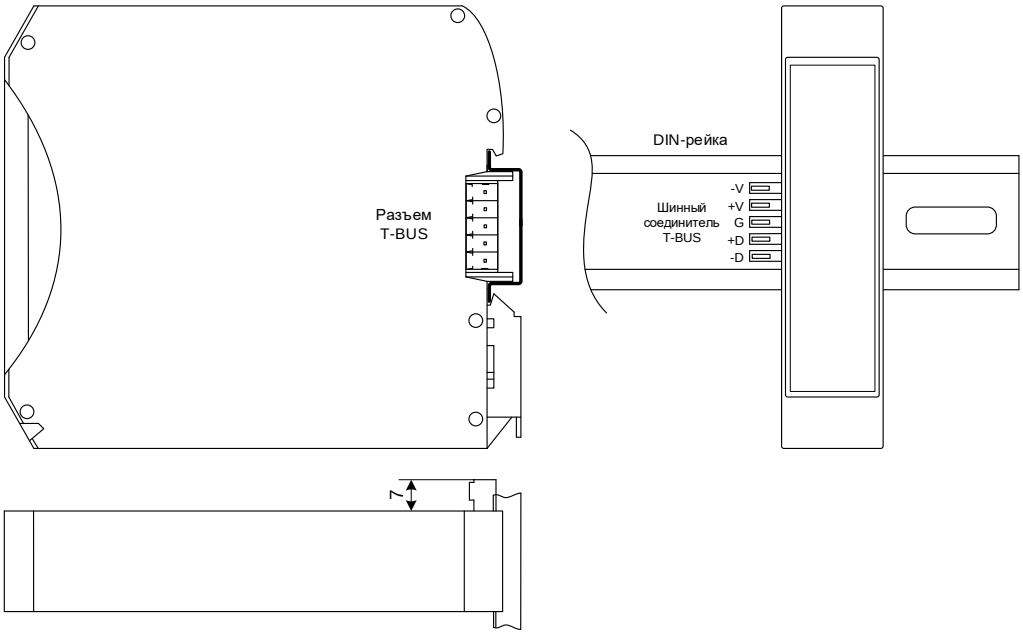


Рисунок 61 – Размещение устройства на DIN-рейке с шиной T-BUS

ВНИМАНИЕ! ПРИ УСТАНОВКЕ УСТРОЙСТВА НА ШИНУ T-BUS НЕОБХОДИМО КОНТРОЛИРОВАТЬ ПОЛОЖЕНИЕ КЛЕММ ШИННОГО СОЕДИНИТЕЛЯ T-BUS ОТНОСИТЕЛЬНО РАЗЪЕМА T-BUS НА ТЫЛЬНОЙ СТОРОНЕ КОРПУСА.

Для подключения к шине T-BUS монтажных проводов используются штекеры MC 1,5/5 ST 3,81 и IMC 1,5/5 ST 3,81. На рисунке ниже приведен внешний вид шиты T-BUS в сборе, где:

A – шинный соединитель ME 22,5 T-BUS 1,5/5-ST-3,81
B – штекер MC 1,5/5-ST-3,81
C – штекер IMC 1,5/5-ST-3,81

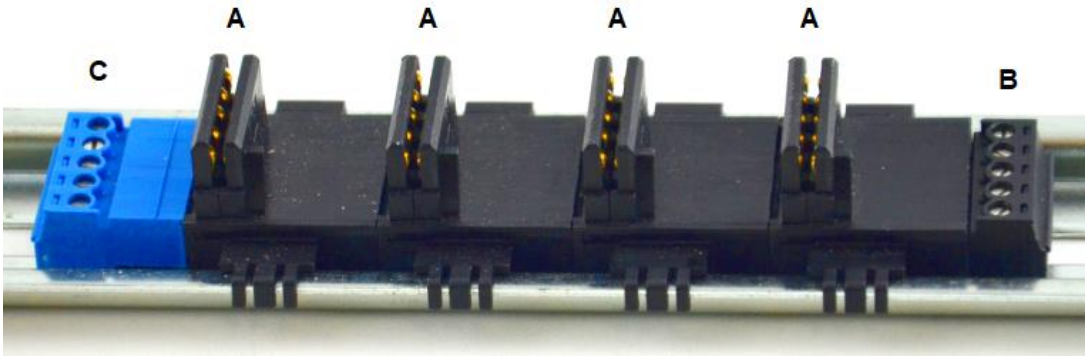


Рисунок 62 – Внешний вид шины T-BUS

Примечание Штекер IMC 1,5/5-ST-3,81 не входит в стандартный комплект поставки устройства.

7.2.5 Подключение питания

Количество и тип каналов питания устройства зависят от исполнения по питанию, согласно заказной кодировке. При наличии напряжения питания на канале питания загорится индикатор **PWR**.

При подключении источника питания постоянного тока к каналу питания 220 В, полярность значения не имеет.

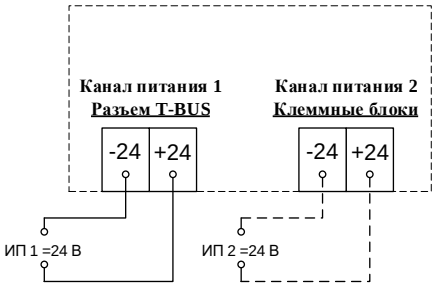


Рисунок 63 – Схема подключения питания каналов 24В

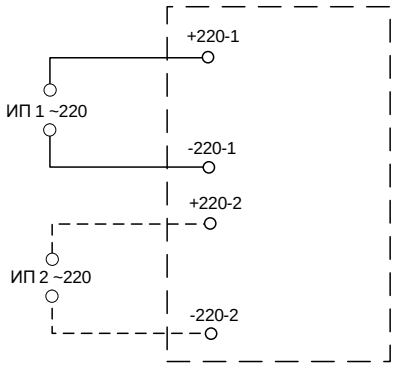


Рисунок 64 – Схема подключения питания каналов 220В

ВНИМАНИЕ! ОДНОВРЕМЕННОЕ ПОДКЛЮЧЕНИЕ К СЕТИ ПИТАНИЯ 24 В И 220 В НЕ ПОДДЕРЖИВАЕТСЯ.

ВНИМАНИЕ! СЕТЬ ПИТАНИЯ (≈/= 220 В) ДОЛЖНА ИМЕТЬ ПРОВОД ЗАЗЕМЛЕНИЯ.

7.2.5.1 Подача питания на шину T-BUS

Рекомендуемое напряжение питания шины T-BUS 24 В. Подача питания на шину T-BUS осуществляется одним из следующих способов:

- от внешнего источника питания, подключенного к шине с помощью штекера;
- от источника питания TOPAZ, установленного на шине.

ВНИМАНИЕ! НЕОБХОДИМО УЧИТЫВАТЬ, ЧТОБЫ НОМИНАЛЬНОЕ ЗНАЧЕНИЕ НАПРЯЖЕНИЯ ПИТАНИЯ ШИНЫ T-BUS ВХОДИЛО В ДОПУСТИМЫЙ ДИАПАЗОН ПИТАНИЯ ДЛЯ КАЖДОГО УСТРОЙСТВА TOPAZ, УСТАНОВЛЕННОГО НА ШИНЕ. НОМИНАЛЬНЫЕ ЗНАЧЕНИЯ И ДОПУСТИМЫЕ ДИАПАЗОНЫ ПИТАНИЯ УСТРОЙСТВ TOPAZ ПРИВЕДЕНЫ В РУКОВОДСТВАХ ПО ЭКСПЛУАТАЦИИ НА СООТВЕТСТВУЮЩИЕ УСТРОЙСТВА.

ВНИМАНИЕ! НЕДОПУСТИМО ПОДАВАТЬ ВНЕШНЕЕ НАПРЯЖЕНИЕ ПИТАНИЯ 110/220 В НА ШИНУ T-BUS, ТАК КАК ЭТО ПРИВЕДЕТ К ВЫХОДУ ИЗ СТРОЯ ПОДКЛЮЧЕННЫХ К НЕЙ УСТРОЙСТВ.

7.2.6 **Подключение к сети Ethernet**

Подключение к сети Ethernet осуществляется, используя промышленные коммутаторы, объединенные в локальную технологическую сеть с кольцевой или иной топологией (рекомендуется применять экранированные кабели и патч-корды).

7.2.6.1 Подключение оптоволоконных портов Ethernet

При подключении устройства по оптическому интерфейсу Ethernet используется две оптоволоконные линии. Одна из оптических линий используется для передачи от устройства 1 к устройству 2, а другая от устройства 2 к устройству 1, формируя, таким образом, полнодуплексную передачу данных.

Необходимо соединить Tx-порт (передатчик) устройства 1 с Rx-портом (приемник) устройства 2, а Rx-порт устройства 1 с Tx-портом устройства 2. При подключении кабеля

рекомендуется обозначить две стороны одной и той же линии одинаковой буквой (A-A, B-B, как показано ниже).

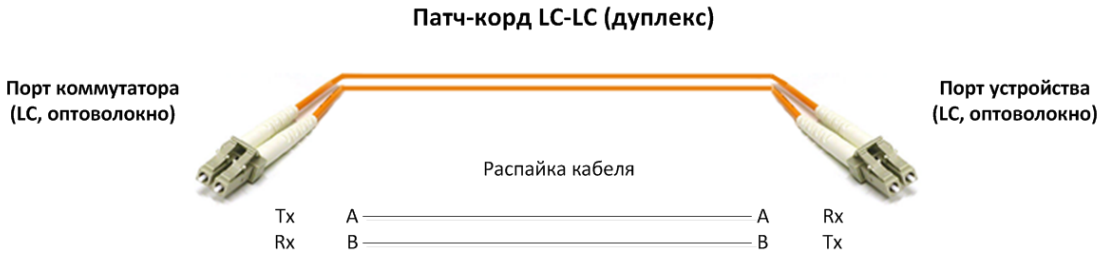


Рисунок 65 – Схема подключения оптоволоконного кабеля

ВНИМАНИЕ! УСТРОЙСТВО ЯВЛЯЕТСЯ ПРОДУКТОМ КЛАССА CLASS 1 LASER/LED. ИЗБЕГАЙТЕ ПРЯМОГО ПОПАДАНИЯ В ГЛАЗ ИЗЛУЧЕНИЯ LASER/LED.

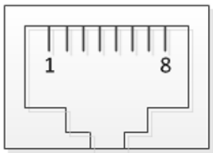
7.2.6.2 Подключение Ethernet-портов 10/100 BaseT(X)

Порты 10/100BaseTX, расположенные на передней панели, используются для подключения Ethernet-устройств.

На рисунке ниже схема расположения контактов для портов MDI (подключение устройств пользователя) и MDI-X (подключение коммутаторов/концентраторов), а также показана распайка прямого и перекрестного Ethernet-кабелей.

Таблица 39 – Назначение контактов

Контакт	Сигнал
порт MDI	
1	Tx+
2	Tx-
3	Rx+
6	Rx-
порт MDI-X	
1	Rx+
2	Rx-
3	Tx+
6	Tx-



8-контактный порт RJ45

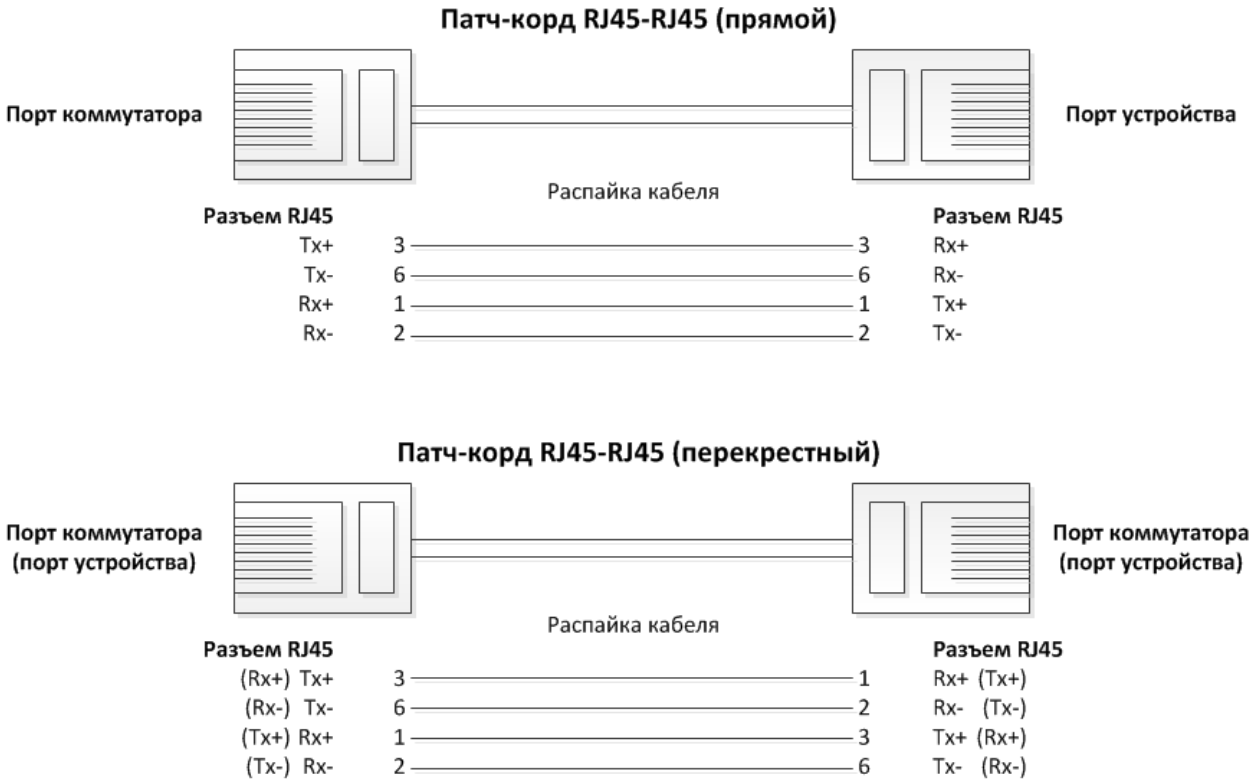


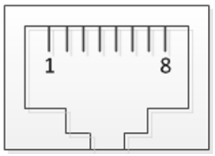
Рисунок 66 – Схема соответствия контактов

7.2.6.3 Подключение Ethernet-порта 1000BaseT(X)

Данные с порта 1000BaseT(X) передаются по дифференциальной сигнальной паре TRD+/- с помощью медных проводов.

Таблица 40 – Назначение контактов

Контакт	Сигнал
порт MDI/MDI-X	
1	TRD (0) +
2	TRD (0) -
3	TRD (1) +
4	TRD (2) +
5	TRD (2) -
6	TRD (1) -
7	TRD (3) +
8	TRD (3) -



8-контактный порт RJ45

7.2.7 Подключение к сетям последовательной передачи

7.2.7.1 Подключение к сетям RS-485

Схема подключения к сетям (общим шинам) RS-485 приведена на рисунке 67. Клеммы подключения к интерфейсу RS-485-1 контроллерной платы устройства дублированы на шине T-BUS.

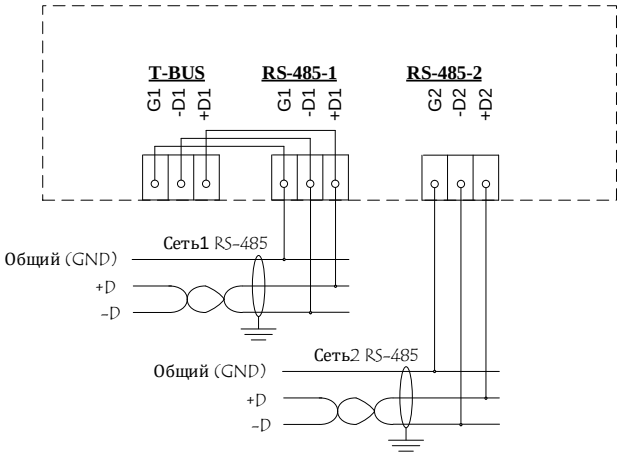


Рисунок 67 – Схема подключения устройства к сетям RS-485

ВНИМАНИЕ! НЕ ИСПОЛЬЗОВАТЬ ЭКРАН КАБЕЛЯ ДЛЯ ПОДКЛЮЧЕНИЯ КОНТАКТА G.

7.2.7.2 Подключение к сетям RS-422

Схема подключения к сети RS-422 приведена на рисунке 68. Назначение контактов клеммных блоков RS-422 приведено на рисунке 69. Сопротивление согласующего резистора (RT) рассчитывается в соответствии с длиной и волновым сопротивлением кабеля.

ВНИМАНИЕ! СХЕМА ПОДКЛЮЧЕНИЯ УСТРОЙСТВА ЗАВИСИТ ОТ ПОДКЛЮЧЕНИЯ ЕГО В КАЧЕСТВЕ ВЕДУЩЕГО (MASTER) ИЛИ ВЕДОМОГО (SLAVE), КАК ПОКАЗАНО НА РИСУНКЕ 68.

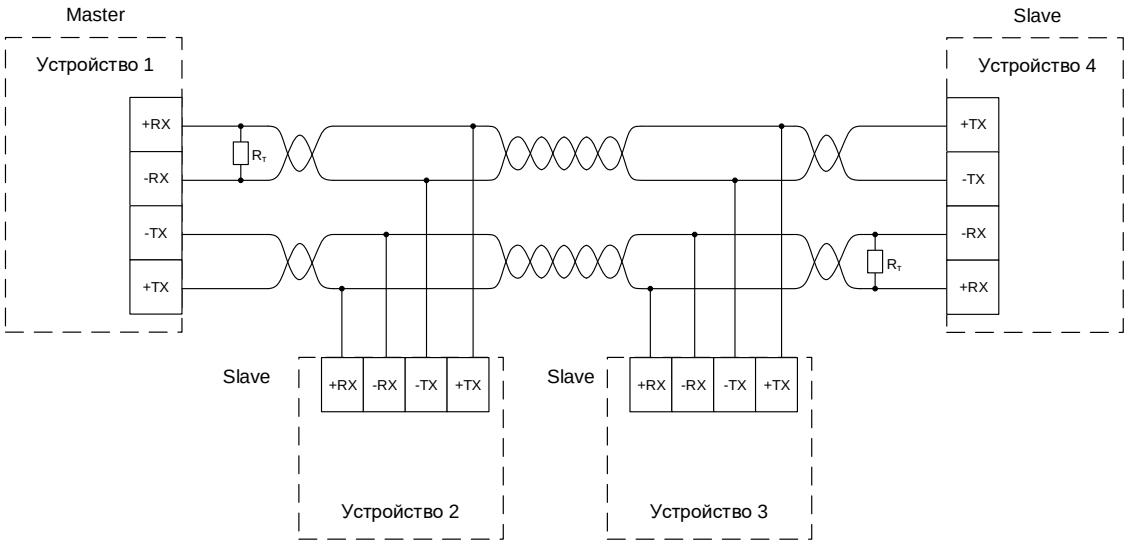


Рисунок 68 – Схема подключения устройств к сети RS-422

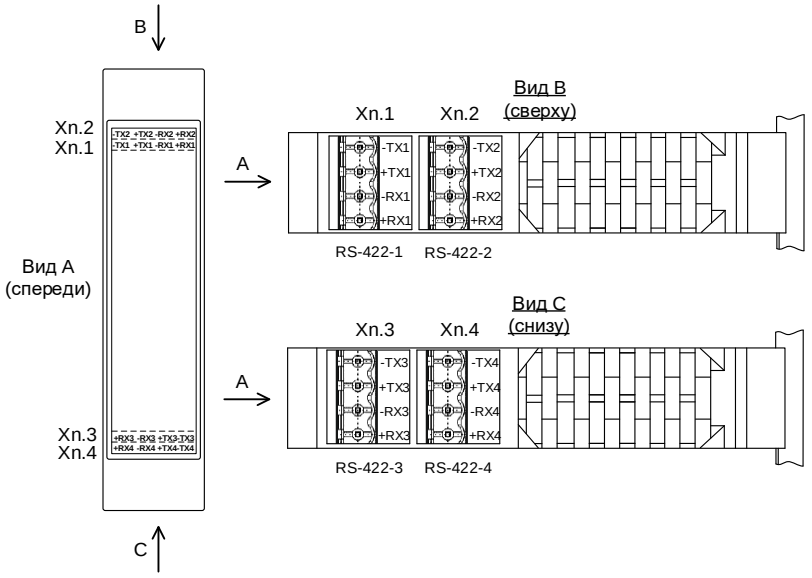


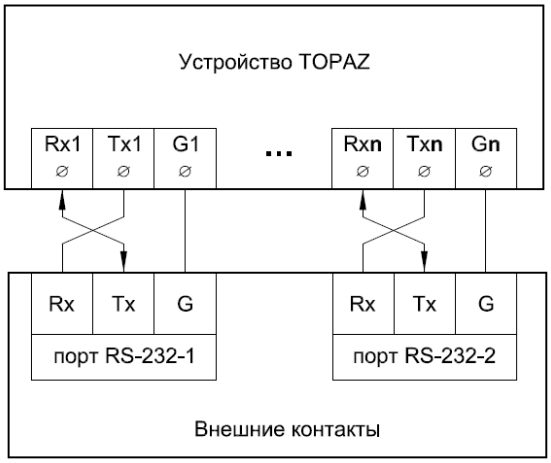
Рисунок 69 – Назначение контактов клеммных блоков RS-422

7.2.7.3 Подключение к сетям RS-232

Подключение по интерфейсу RS-232, в зависимости от исполнения, может осуществляться через следующие виды контактов:

- клеммы, расположенные на верхней и нижней панелях устройства;
- контакты на шине T-BUS (только первый порт);
- вилку DB9, расположенную на передней панели.

Назначение клемм указано на корпусе устройства. На рисунке 70 представлена схема подключения клемм RS-232 устройства TOPAZ к другим устройствам.



n – номер порта RS-232. Количество портов RS-232 определяется заказным обозначением устройства

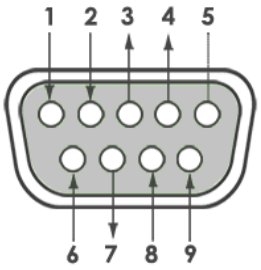
Рисунок 70 – Схема подключение клемм RS-232

ВНИМАНИЕ! ПРИ ИСПОЛЬЗОВАНИИ RS-232 В КАЧЕСТВЕ ПЕРВОГО ПОРТА, НЕОБХОДИМО УЧИТЫВАТЬ, ЧТО НА ШИНЕ T-BUS ТОЖЕ ВЫВЕДЕН ИНТЕРФЕЙС RS-232 (ДЛЯ ИСКЛЮЧЕНИЯ ВОЗМОЖНЫХ КОЛЛИЗИЙ В ПРОЦЕДУРАХ ОБМЕНА ДАННЫМИ).

Назначение контактов вилки DB9 представлено в таблице 41.

Таблица 41 – Назначение контактов вилки DB9

Контакт	Сигнал
1	–
2	Rx
3	Tx
4	–
5	GND
6	–
7	–
8	–
9	–



9-контактная вилка DB9

7.2.8 Подключение каналов дискретного ввода-вывода

7.2.8.1 Режим дискретного ввода

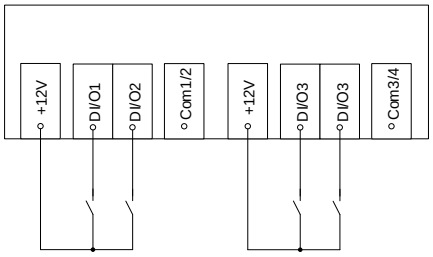


Рисунок 71 – Подключения каналов дискретного ввода с питанием от внутреннего источника питания.

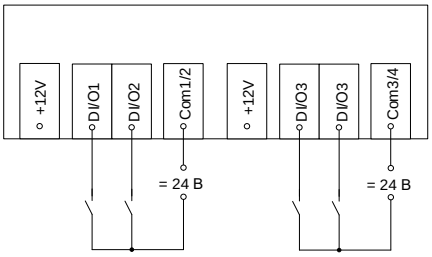


Рисунок 72 – Подключения каналов дискретного ввода с питанием от внешнего источника питания.

7.2.8.2 Режим дискретного вывода

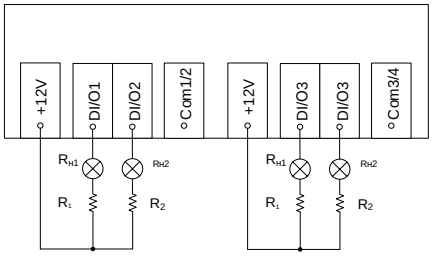


Рисунок 73 – Подключения каналов дискретного вывода с питанием от внутреннего источника питания.

ВНИМАНИЕ! СОПРОТИВЛЕНИЕ РЕЗИСТОРОВ R_1…R_4 ПОДБИРАЮТСЯ В ЗАВИСИМОСТИ ОТ СОПРОТИВЛЕНИЯ НАГРУЗКИ R_{H1}…R_{H4}, ТАКИМ ОБРАЗОМ, ЧТОБЫ СУММАРНЫЙ ТОК НАГРУЗКИ ВСЕХ ЦЕПЕЙ НЕ ПРЕВЫШАЛ МАКСИМАЛЬНЫЙ ТОК НАГРУЗКИ ВНУТРЕННЕГО ИСТОЧНИКА ПИТАНИЯ (0,2 А)

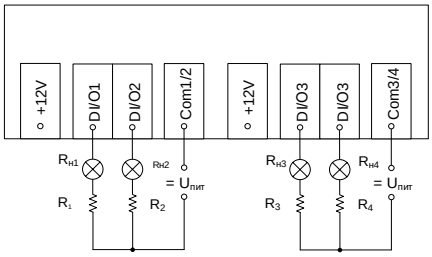


Рисунок 74 – Подключения каналов дискретного вывода с питанием от внешнего источника питания.

ВНИМАНИЕ! ВЫХОДНОЕ НАПРЯЖЕНИЕ ВНЕШНЕГО ИСТОЧНИКА НЕ ДОЛЖНО БЫТЬ БОЛЕЕ 24 В. СОПРОТИВЛЕНИЕ РЕЗИСТОРОВ R_1…R_4 ПОДБИРАЮТСЯ В ЗАВИСИМОСТИ ОТ СОПРОТИВЛЕНИЯ НАГРУЗКИ R_{H1}…R_{H4}, ТАКИМ ОБРАЗОМ, ЧТОБЫ ТОК В ЦЕПИ НЕ ПРЕВЫШАЛ 0,4 А.

7.2.9 **Подключение SIM-карт**

Для обеспечения возможности подключения устройства к сети Интернет через сотовую связь понадобится SIM-карта формата mini-SIM. До установки её в устройство, необходимо отключить в настройках SIM-карты запрос PIN-кода при включении.

7.2.10 **Установка антенны GPS/ГЛОНАСС**

Для присоединения антенны к устройству следует использовать коаксиальный кабель.

ВНИМАНИЕ! ЗАПРЕЩЕНО СОЕДИНЯТЬ ГРОЗОРАЗРЯДНИК АНТЕННЫ С МОЛНИЕОТВОДОМ, УСТАНОВЛЕННЫМ НА КРЫШЕ ЗДАНИЯ.

ВНИМАНИЕ! ЗАПРЕЩЕНО СОЕДИНЯТЬ АНТЕННУ И ЭКРАН КОАКСИАЛЬНОГО КАБЕЛЯ АНТЕННЫ С КОНТУРОМ ЗАЗЕМЛЕНИЯ ОБЪЕКТА, НА КОТОРОМ УСТАНАВЛИВАЕТСЯ УСТРОЙСТВО.

ПРИЛОЖЕНИЕ А

Рисунок А.1 – Внешний вид роутера TOPAZ GSM-LTE-2Tx-2R-2LV

Рисунок А.2 – Внешний вид роутера TOPAZ GSM-LTE-2Tx-2R-DIO4-2LV

Рисунок А.3 – Внешний вид роутера TOPAZ GSM-LTE-2Tx-4RS232-DIO4-2LV

Рисунок А.4 – Внешний вид роутера TOPAZ GSM-LTE-2Tx-2FxS-2RS232-DIO4-2LV

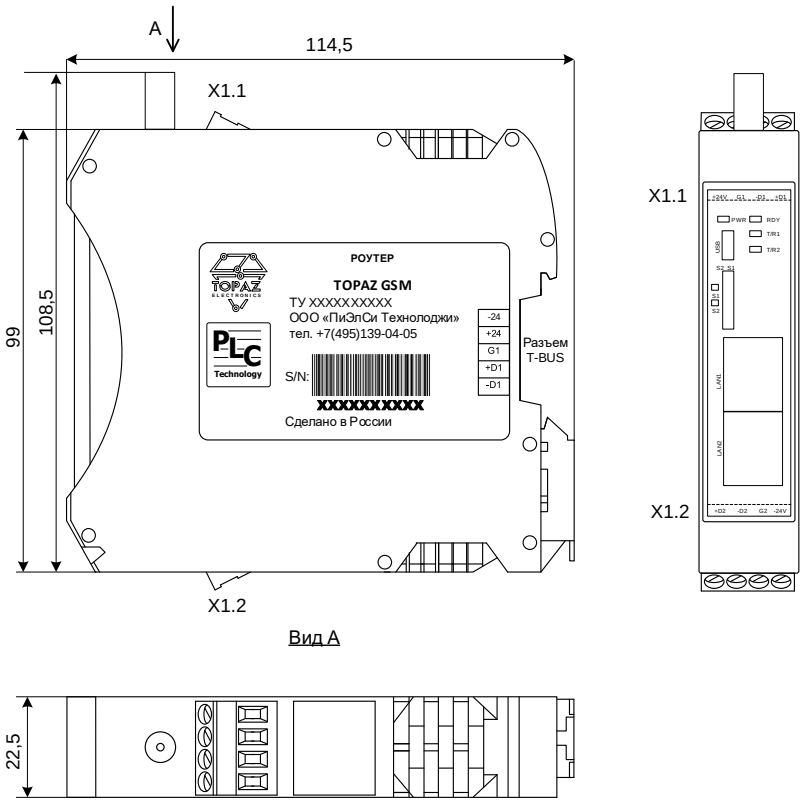


Рисунок А.5 – Габаритные размеры роутера TOPAZ GSM-LTE-2Tx-2R-2LV

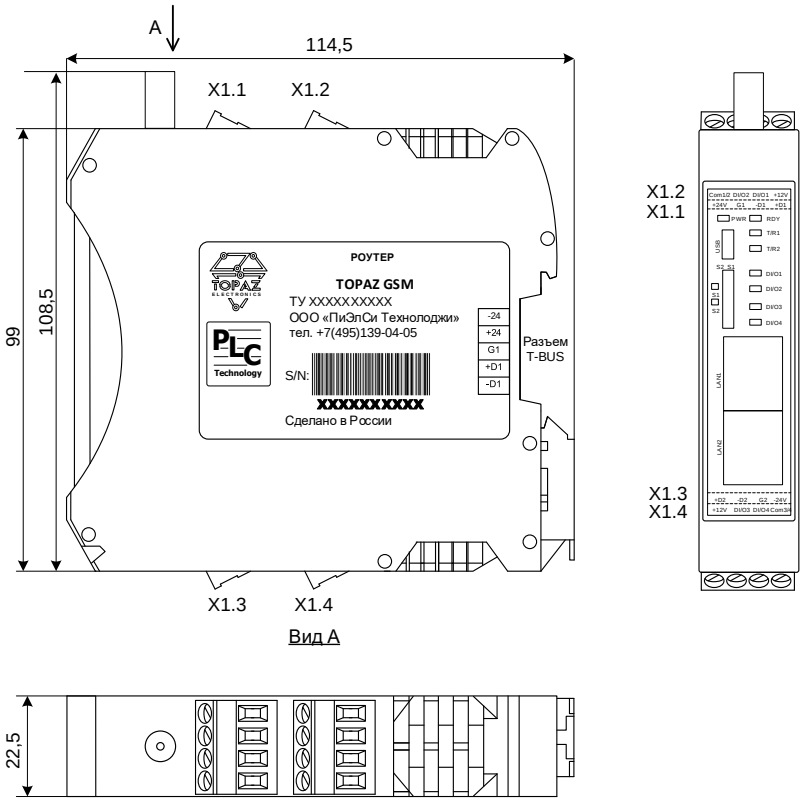


Рисунок А.6 – Габаритные размеры роутера TOPAZ GSM-LTE-2Tx-2R-DIO4-2LV

Таблица А.1 – Обозначения клемм и портов

Обозначение*	Описание
Питание напряжением постоянного тока	
+24 (+24V)	Вход питания (+24 В)
-24 (-24V)	Вход питания (-24 В)
Питание напряжением переменного тока	
~ 220 В	Клеммы питания 220 В
Заземление	
⏚	клемма заземления
Интерфейс конфигурирования	
USB	USB порт для подключения через консоль
Интерфейс RS-485	
Gn	GND
+Dn	data+
–Dn	data-
Интерфейс RS-232	
Gn	GND
Txn	TD
Rxn	RD
Интерфейс RS-422	
+TXn	TD(B)+
-TXn	TD(A)-
+RXn	RD(B)+
-RXn	RD(A)-
Интерфейс Ethernet	
LANn	Порт Ethernet
Универсальные каналы ввода-вывода	
DIO1, DIO2	Каналы дискретного ввода 1 и 2 (группа 1)
COM1/2	Общий провод (группа 1)
+12V	Выход источника напряжения 12 В (группа 1)
DIO3, DIO4	Каналы дискретного ввода 3 и 4 (группа 2)
COM3/4	Общий провод (группа 2)
+12V	Выход источника напряжения 12 В (группа 2)
* n – номер входа/порта	

Таблица А.2 – Обозначения кнопок и индикаторов

Обозначение*	Описание
Кнопки (в наличии RS и RB)	
RS	Перезагрузка устройства
RB	Активация загрузчика с SD карты, при одновременном нажатии с кнопкой RS
Кнопки (в наличии RB)	
RB	Активация загрузчика с SD-карты
Индикаторы	
PWR	Наличие питания
RDY	Состояние готовности устройства
T/Rn	Передача информации по интерфейсу связи RS-485
DI/On	Состояния канала дискретного ввода/вывода
S1	Передача данных по каналу GSM1
S2	Передача данных по каналу GSM2
HDD	Работа с накопителем данных
* n – номер входа/порта	

ПРИЛОЖЕНИЕ Б

Утилита PuTTY – одна из распространенных бесплатных программ, не требующая установки. В данном разделе приведено описание подключения к устройству с помощью данной утилиты.

Сайт разработчика:
http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html.
Ссылка непосредственно исполняемый файл программы:
https://the.earth.li/~sgtatham/putty/latest/x86/putty.exe.

Подключение через серийный порт

После запуска программы PuTTY откроется окно настройки, где во вкладке **Session** необходимо выбрать тип соединения **Serial** и его основные параметры (номер виртуального порта будет отличаться от приведенного в примере в зависимости от вашей системы):

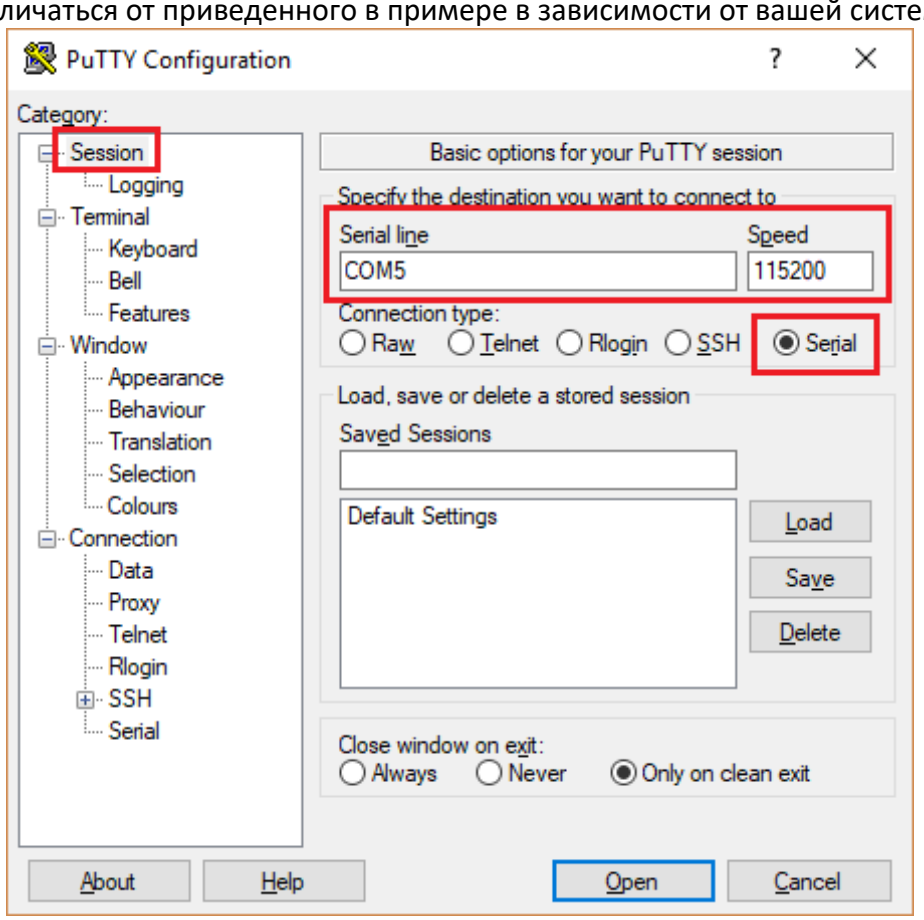


Рисунок Б.1 – Задаваемые настройки раздела Session (сессия)

В настройках соединения (**Connection**) – выбрать последовательный порт (**Serial**) и установить параметры соединения согласно таблице **12**:

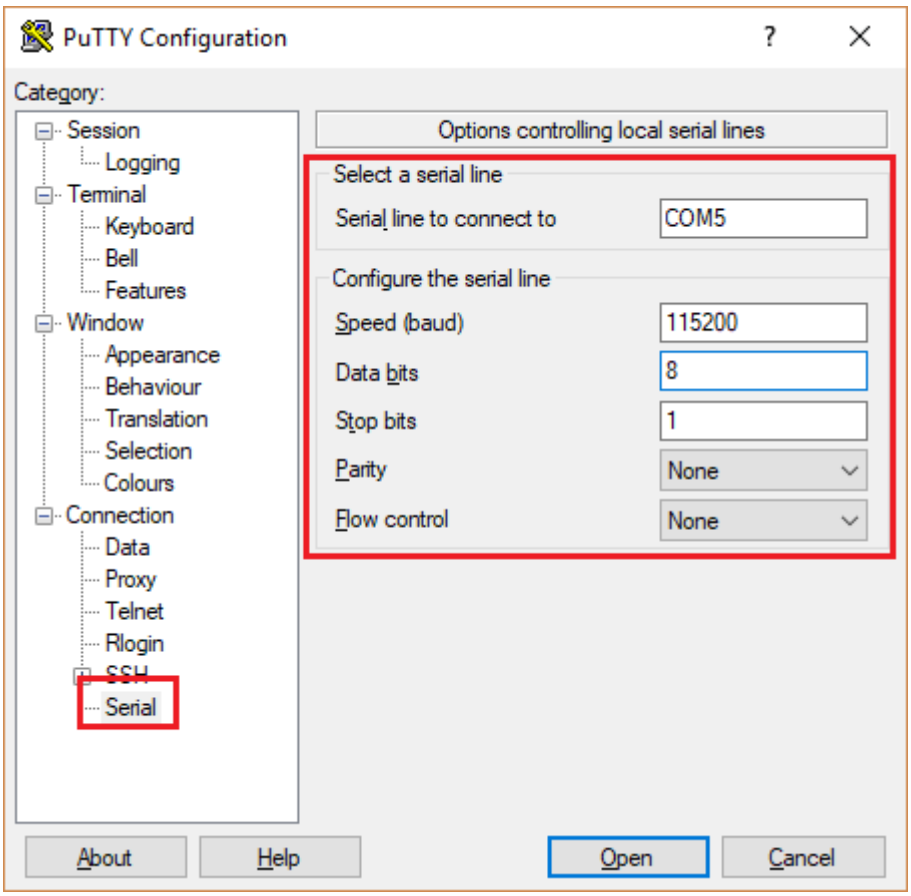


Рисунок Б.2 – Задаваемые настройки раздела Serial (серийный порт)

После настройки параметров последовательного порта, необходимо нажать кнопку «Открыть» (Open) для установки соединения и вызова окна консоли.

Подключение через Ethernet порт

Для подключения к устройству по протоколу SSH, во вкладке **Session** необходимо выбрать тип соединения **SSH** и его основные параметры:

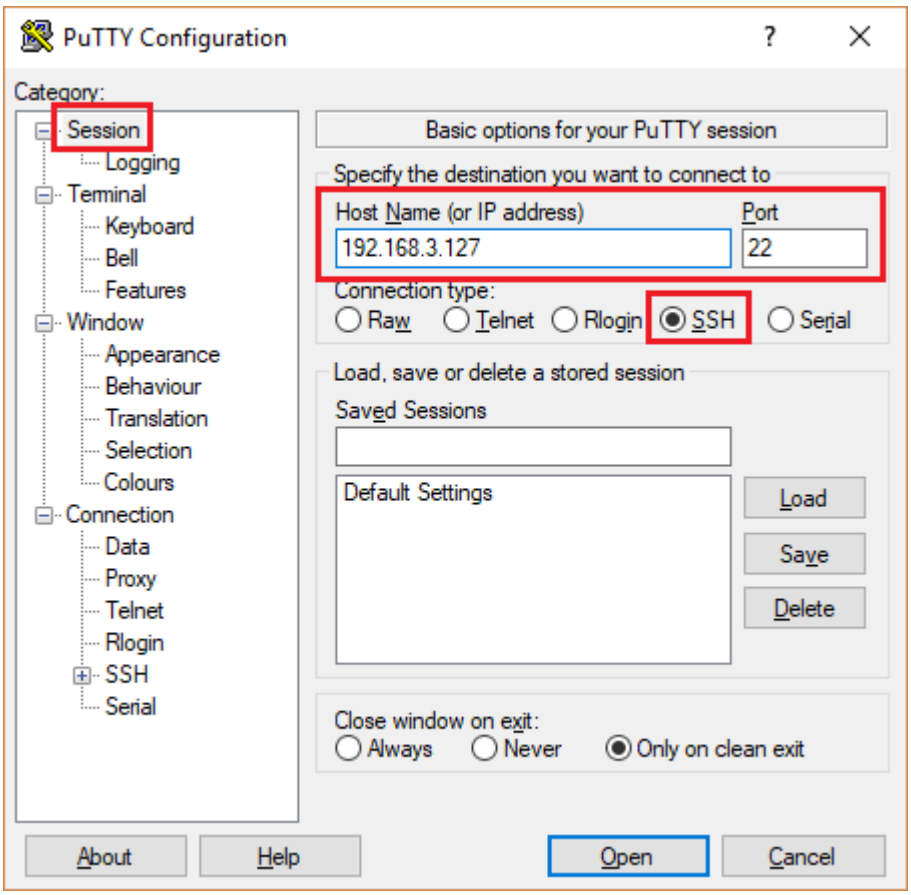


Рисунок Б.3 – Задаваемые настройки раздела Session (сессия)

После настройки параметров последовательного порта, необходимо нажать кнопку «Открыть» (Open) для установки соединения и вызова окна консоли.