СЕРВЕР ДОСТУПА К ДАННЫМ (КОНТРОЛЛЕР)

TOPAZ IEC DAS MX681

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

ПЛСТ.421457.105 РЭ

Москва 2024

ОГЛАВЛЕНИЕ

1 ОПИСАНИЕ И РАБОТА 4
1.1 Назначение изделия 4
1.2 Модификации и условные обозначения 4
1.3 Технические характеристики 6
1.3.1 Конструкция 6
1.3.2 Рабочие условия эксплуатации 6
1.3.3 Безопасность и электромагнитная совместимость 7
1.3.4 Надежность 7
1.3.5 Питание 7
1.3.6 Характеристики контроллера 8
1.3.1 Синхронизация времени 8
1.3.2 Коммуникационные возможности 9
1.3.3 Каналы дискретного ввода-вывода 11
1.4 Комплектность 11
1.5 Устройство и работа 12
1.5.1 Работа кнопок и индикаторов 13
1.6 Конфигурирование устройства 13
1.6.1 Подключение к командной строке 13
1.6.2 Команды и утилиты для работы с устройством 15
1.7 Настройка функций безопасности 25
1.7.1 Конфигурирование порта управления 25
1.7.2 Подсистема регистрации событий безопасности. 25
1.7.3 Подсистема проверки целостности 27
1.7.4 Подсистема криптозащиты каналов связи 33
1.7.5 Подсистема аудита 33
1.8 Web-интерфейс 46
1.8.1 Подключение к web-интерфейсу 46
1.8.2 Работа с web-интерфейсом 48
2 МАРКИРОВКА И ПЛОМБИРОВАНИЕ 60
3 УПАКОВКА 61
4 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ 61
5 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ 61
6 УТИЛИЗАЦИЯ 62
7 ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ 62
7.1 Эксплуатационные ограничения и меры безопасности 62
7.2 Монтаж 62

7.2.1 Подготовка к монтажу 62
7.2.2 Установка на DIN-рейку 63
7.2.3 Внешние подключения 63
7.2.4 Шина T-BUS 63
7.2.5 Подключение питания 64
7.2.6 Подключение к сети Ethernet 66
7.2.7 Подключение к сетям последовательной передачи 67
7.2.8 Подключение каналов дискретного ввода-вывода 70
7.2.9 Подключение SIM-карт (при наличии GSM модема) 71
7.2.10 Установка антенны GPS/ГЛОНАСС 71
7.2.11 Подключение интерфейса человек-машина 72
ПРИЛОЖЕНИЕ А 73
ПРИЛОЖЕНИЕ Б 76

Настоящее руководство по эксплуатации (РЭ) предназначено для ознакомления со сведениями о конструкции, принципе действия, технических характеристиках сервера доступа к данным **TOPAZ IEC DAS MX681** (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 свободно программируемым контроллером, предназначенным для решения задач автоматизации, телемеханики и диспетчеризации.

Устройство используется для 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 IEC DAS MX681 A [B]/[C]/[D]/[E]/[F1- … -Fx] ([G1- … -Gx]-[H1- … -Hx]) I (J-K-L)		
Позиция	**Код**	**Описание**
Тип основного устройства		
A	ExxRyy	Общее количество портов устройства, где «xx» - суммарное количество портов Ethernet, «yy» - суммарное количество портов последовательной передачи данных
Дополнительные функции		
B	GSM	GSM модем на 2 mini-SIM-карты
	GSM-LTE	GSM/LTE модем на 2 mini-SIM-карты
	GSM(SC)	GSM модем с 2 встроенными SIM-chip
	GSM-LTE(SC)	GSM/LTE модем с 2 встроенными SIM-chip
C	PTS	Приемник сигналов точного времени (ГЛОНАСС/GPS)

TOPAZ IEC DAS MX681 A [B]/[C]/[D]/[E]/[F1- … -Fx] ([G1- … -Gx]-[H1- … -Hx]) I (J-K-L)		
Позиция	**Код**	**Описание**
D	DIOn	Универсальные каналы дискретного ввода-вывода, где «n» - количество каналов. Шаг наращивания – 4.
E	SSDm	SSD накопители, где «m» – суммарный объем ПЗУ накопителей SSD в Гб (Тб)
	SSDmT	
Панель оператора		
F1- … -Fx	nHDMI	Порт HDMI
	nUSB	Порты USB
	HMI7	Человеко-машинный интерфейс TOPAZ HMI7
	HMI15	Сенсорный монитор TOPAZ HMI15
Коммуникационные порты Ethernet		
G1- … -Gx	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
	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		
H1- … -Hx	nR	RS-485 клеммный вход
	nRS232	порты RS-232, клеммный вход или разъем DB9 (определяется заводом-изготовителем)
	nRS422	RS-422 клеммный вход
	nRS485Fo	RS-485 оптический ST-разъем
	nRS232Fo	RS-232 оптический ST-разъем
	«n» – количество портов последовательной передачи данных соответствующего типа, максимальное суммарное количество портов последовательной передачи данных – 16.	
Встроенный источник питания		
I	-	Два входа питания 24В DC
	HV	Встроенный источник питания 220В DC/AC
	2HV	Два независимых встроенных источника питания 220В DC/AC
Средства защиты сети		
J	-	Отсутствуют дополнительные средства защиты сети
	CSG	CybSec Gateway (Шлюз безопасности)
	IDS	CybSec IDS (Средство обнаружения вторжений)
Сертифицированная ОС		
K	-	Отсутствует сертифицированная ОС на базе Linux
	OC	Сертифицированная ОС на базе Linux
Дополнительное ПО		
L	-	Отсутствует дополнительное ПО
	01	TCC Dcrypt, в комплекте с лицензиями и сертификатами
	02	ИнфоТЕКС Vipnet, в комплекте с лицензиями и сертификатами
	03	Код Безопасности Континент АП, в комплекте с лицензиями и сертификатами
	04	НПП Гамма Кречет, в комплекте с лицензиями и сертификатами

TOPAZ IEC DAS MX681 A [B]/[C]/[D]/[E]/[F1- … -Fx] ([G1- … -Gx]-[H1- … -Hx]) I (J-K-L)		
Позиция	**Код**	**Описание**
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		

Пример записи обозначения устройства **TOPAZ IEC DAS MX681** при заказе:
с тремя Ethernet 1000 Мбит/с TX RJ-45, двумя портами RS-485, двумя входами питания 24 В:
«Сервер доступа к данным TOPAZ IEC DAS MX681 E3R2 (3GTx-2R)».

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 180x108,5x124 мм. Масса устройства не более 1 кг.

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

Габаритные размеры типовых модификаций контроллера приведены в таблице 2.

Таблица 2 – Габаритные размеры типовых модификаций устройства

Модификация	Габаритные размеры		
	Ширина, мм	Высота, мм	Глубина, мм
TOPAZ IEC DAS MX681 E3R2 (3GTx-2R)	45,0	99,0	114,5
TOPAZ IEC DAS MX681 E5R14 (3GTx-2Tx-14R)	112,5	99,0	114,5
TOPAZ IEC DAS MX681 E5R2 (3GTx-2FxM-2R)	67,5	99,0	118,0
TOPAZ IEC DAS MX681 E5R2 (3GTx-2Tx-2R)	67,5	99,0	114,5
TOPAZ IEC DAS MX681 E5R2 SSD512 (3GTx-2Tx-2R)	90,0	99,0	114,5
TOPAZ IEC DAS MX681 E5R6 (3GTx-2Tx-6R)	67,5	99,0	114,5
TOPAZ IEC DAS MX681 E5R6 SSD1T (3GTx-2FxM-6R)	90,0	99,0	118,0
TOPAZ IEC DAS MX681 E7R2 (3GTx-4Tx-2R)	90,0	99,0	114,5
TOPAZ IEC DAS MX681 E7R6 (3GTx-4Tx-6R)	90,0	99,0	114,5

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 3 – 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 4 – 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	0,04
Потребляемая мощность плат устройства, не более, Вт	12

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 ложного формирования команд ТУ, 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 5 – Характеристики контроллера

Наименование параметра	Значение
Операционная система	Linux
Слот для Flash-карты	microSD
Процессор	2 x ARM Cortex-A7
Частота, МГц	1200
Память ОЗУ, Гб	1 (DDR3L)
Память ПЗУ, Гб	8 (eMMC)
Поддержка языков программирования в соответствии со стандартом ГОСТ Р МЭК 61131-3	Да

1.3.1 Синхронизация времени

Характеристики синхронизации времени приведены в таблице ниже.

Таблица 6 – Характеристики синхронизации времени

Наименование параметра	Значение
Уход локальных часов без внешнего питания, с / сутки, не более	± 1
Уход локальных часов при отсутствии синхронизации по сигналам точного времени, с / сутки, не более	± 0,5
Точность синхронизации времени: - по протоколам ГОСТ Р МЭК 60870-5-101/104 - по протоколам NTP, SNTP - по протоколу PTP	 ±2 мс ±100 мкс ±1 мкс

1.3.1.1 Приемник сигналов точного времени

Наличие приемника сигналов точного времени указано в заказной кодировке устройства. Технические характеристики приемника сигналов точного времени ГЛОНАСС/GPS приведены в таблице ниже.

Таблица 7 – Технические характеристики приемника сигналов точного времени

Наименование параметра		Значение
Приемник ГЛОНАСС/GPS	каналы сопровождения	33
	каналы захвата	99
Тип генератора		TCXO
Разъем для антенны		SMA
Точность синхронизации времени по сигналам ГЛОНАСС/GPS		±200 нс

1.3.2 Коммуникационные возможности

1.3.2.1 Интерфейсы Ethernet

Количество и тип каналов Ethernet указаны в заказной кодировке устройства. Технические характеристики интерфейса Ethernet приведены в таблице ниже.

Таблица 8 – 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 9 – 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

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

<u>Примечание</u> Скорость передачи данных порта SFP соответствует скорости передачи данных SFP-модуля

Таблица 10 – 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 [1)]; 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 [1)]; PRP; HSR

Технологии	Описание
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)
Примечания: 1) Порты Ethernet на платах расширения (с двумя Ethernet) нельзя использовать в протоколе RSTP.	

1.3.2.2 Интерфейсы последовательной передачи данных

Количество и тип каналов последовательной передачи данных указаны в заказной кодировке устройства. Технические характеристики последовательных интерфейсов приведены в таблице ниже.

Таблица 11 – Технические характеристики последовательных интерфейсов

Наименование параметра	Значение
Протоколы передачи данных	ГОСТ Р МЭК 60870-5-101 (master/slave), ГОСТ Р МЭК 60870-5-103 (master), Modbus RTU/ASCII (slave), SPA-Bus (master)
Режим передачи	асинхронный последовательный двухсторонний полудуплексный
Скорость передачи	2400 – 115 200 бит/с (по заказу до 4 Мбит/с)
Интерфейс RS-485	
Тип разъема	клеммный вход
Контакты	+D (A), -D (B), G (GND)
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
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

1.3.2.3 Порты расширения

Наличие и тип портов расширения указаны в заказной кодировке устройства. Технические характеристики портов приведены в таблице ниже.

Таблица 12 – Технические характеристики портов расширения

Наименование параметра	Значение
Порт HDMI	
Тип разъема	Тип А

Наименование параметра	Значение
Порт USB	
Тип разъема	USB
Поддержка спецификации	USB 2.0

1.3.2.4 GSM модем

Наличие и тип модема указаны в заказной кодировке устройства. Технические характеристики GSM модема приведены в таблице ниже.

Таблица 13 – Технические характеристики модема

Наименование параметра		Значение
Количество SIM-карт		2
Формат SIM-карты		mini-SIM или SIM-chip
Разъем 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 модем		
Поддерживаемые стандарты передачи данных		CSD, GPRS, EDGE, UMTS, HSDPA, HSUPA
Количество антенн		1
GSM/LTE модем		
Поддерживаемые стандарты передачи данных		CSD, GPRS, EDGE, UMTS, HSPDA, HSUPA, HSPA+, DC-HSPA+, LTE
Количество антенн		до 2 (поддержка MIMO)

1.3.3 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 14 – Технические характеристики каналов дискретного ввода-вывода

Наименование параметра	Значение
Режим работы	дискретный ввод; дискретный вывод
Напряжение встроенного источника питания, В	от 10,2 до 13,8
Максимальный ток встроенного источника питания, мА	200
Ток потребления на каждом канале, мА	3
Сопротивление токоограничивающего резистора, кОм	4

1.4 Комплектность

Комплект поставки указывается в индивидуальном паспорте устройства.

В стандартный комплект поставки входят:

1) устройство TOPAZ IEC DAS MX681;
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

После подачи питания производится инициализация устройства. В случае успешной инициализации, индикатор готовности **RDY** светится зеленым цветом (при старте свет стабильный, в процессе работы мигает зеленым цветом с частотой 1 Гц). В случае любой аварийной ситуации в процессе работы устройства, свечение индикатора готовности непрерывное или отсутствует.

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:

- прием информации по цифровым каналам связи;
- автоматическое накопление, хранение и передача информации по цифровым каналам связи;
- ведение системного времени и его автоматическая коррекция/синхронизация по сигналам точного времени.
- самодиагностика и тестирование работоспособности первичных преобразователей (датчиков);
- ведение журнала событий.
- синхронизации собственных часов от внешней сети по протоколам PTP, NTP и SNTP;
- синхронизации времени подконтрольных устройств;
- регистрация событий безопасности;
- идентификация, аутентификация пользователей;
- разделение прав пользователей;
- межсетевого экранирования;
- отправки событий безопасности в централизованные системы мониторинга;
- контроля целостности.

В зависимости от типа установленных плат, устройство также может выполнять функции:

- контроля состояния дискретных входов (телесигнализация);
- управления дискретными выходами (телеуправление);
- передачи данных по GPRS сети;
- синхронизации собственных часов с помощью сигналов спутниковых навигационных систем (ГЛОНАСС/GPS).
- осуществлять передачу данных с использованием СКЗИ

В режиме «информационного шторма» устройство поддерживает одновременное соединение с 50 внешними устройствами по протоколу МЭК 61850.

В «Журнале событий» устройства автоматически фиксируются время и даты наступления следующих событий:

- ввода расчетных коэффициентов измерительных каналов;
- попыток несанкционированного доступа;
- фактов изменения данных;

- перезапусков устройства;
- фактов корректировки времени с обязательной фиксацией времени до и после коррекции или величины коррекции времени, на которую было скорректировано устройство;
- результатов самодиагностики;
- отключения питания.

1.5.1 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

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

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 15 – 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**

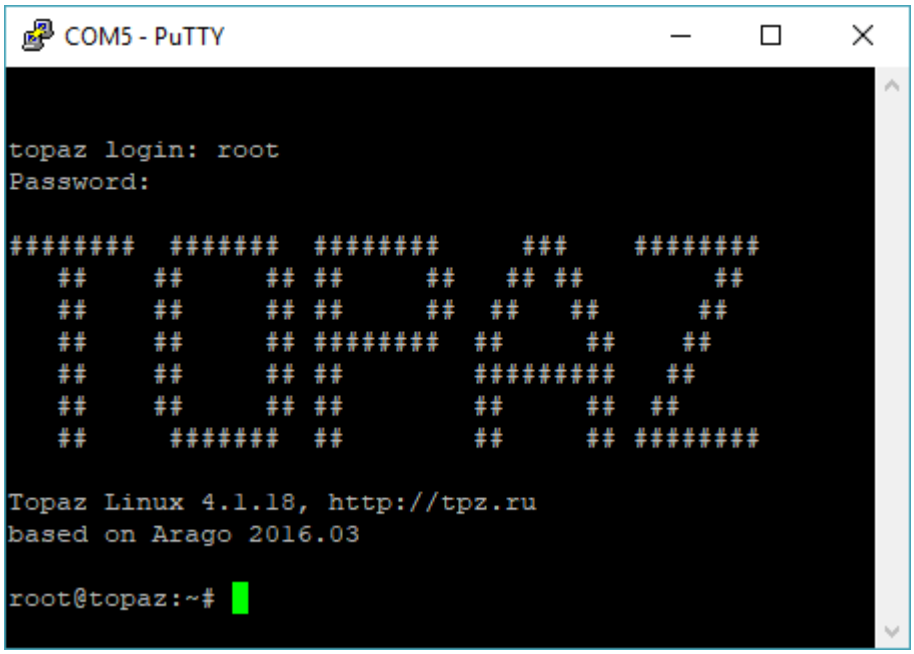


Рисунок 1 – Экран приветствия командной строки

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.

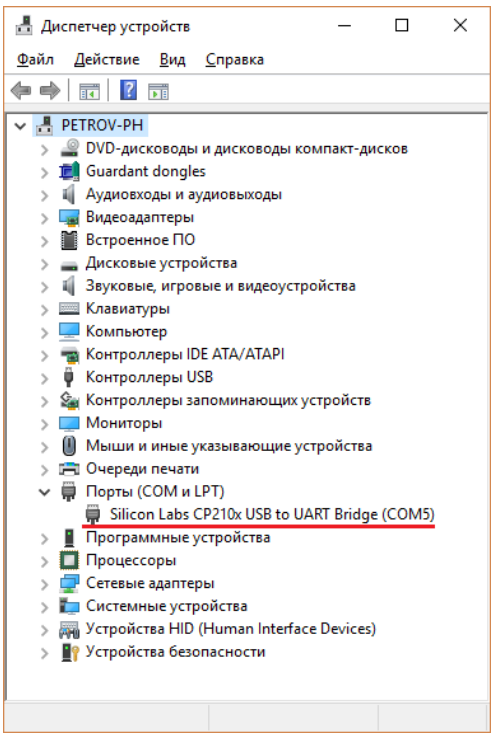


Рисунок 2 – Отображение устройства в диспетчере устройств Windows

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 16 – 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 устройства к персональному компьютеру через Ethernet используются следующие настройки LAN:

порт LAN#1 192.168.3.127

порт LAN#2 192.168.4.127

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 17 – 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».

```
Сброс к заводским настройкам / Factory reset / Sbros k zavodskim nastroykam
Уверены? / Are you sure? [y/n]:
```

Рисунок 3– 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 18 – 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

Опция	Описание
	допустимых опций ifconfig, вносимые изменения будут выполняться для всех инициализированных интерфейсов.

Таблица 19– 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 20 – 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 21 – 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 22 – 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 23 – 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 24 – 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.

Команда	Аргументы	Описание
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)
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 25 – 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 4

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 5

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 26 – 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 27 – 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 28 – 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 29 – 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 6 – Список запущенных сервисов

1.6.2.14.1 Синтаксис

```
service [<сервис> <команда>]
```

Таблица 30 – 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
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 п. 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 игнориро
вать 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 файло в 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-aes
ni.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; d
angling : 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, TCC Diamond VPN, OpenVPN, IPSec, PPTP VPN.

Настройка СКЗИ Infotecs ViPNet VPN, TCC Diamond 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 31 – 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 32 – 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 33 – 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*.

Опция	Описание
-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.

Опция	Описание
-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 34 – 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
-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.

Опция	Описание
-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.
-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 35 – 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 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

Опция	Описание
	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.
-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

Опция	Описание
	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.
-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

Опция	Описание
	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)
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

Опция	Описание
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".
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 **35**):

- **-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 выполните следующие действия:

- подключите компьютер с помощью Ethernet-кабеля к разъему Ethernet устройства;

- откройте интернет-браузер;
- наберите в адресной строке интернет-браузера адрес устройства (по умолчанию **192.168.3.127** для порта LAN1).

При отсутствии неполадок, в окне интернет-браузера появится запрос авторизации (рисунок 6). Введите логин и пароль (по умолчанию: логин – **admin**, пароль – **admin**) и нажмите кнопку «ВОЙТИ» или клавишу «Enter».

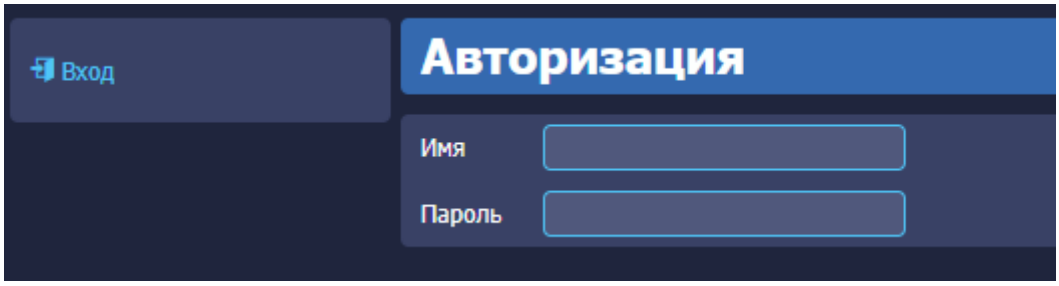


Рисунок 7 – Окно авторизации для доступа к web-интерфейсу

<u>Примечание</u> Компьютер и устройство должны находиться в одной подсети (адрес подсети устройства по умолчанию **255.255.255.0**). Адрес компьютера в подсети должен отличаться от адреса устройства, например **192.168.3.2**.

После корректно ввода логина и пароля открывается доступ к основному интерфейсу управления устройством (рисунок 5).

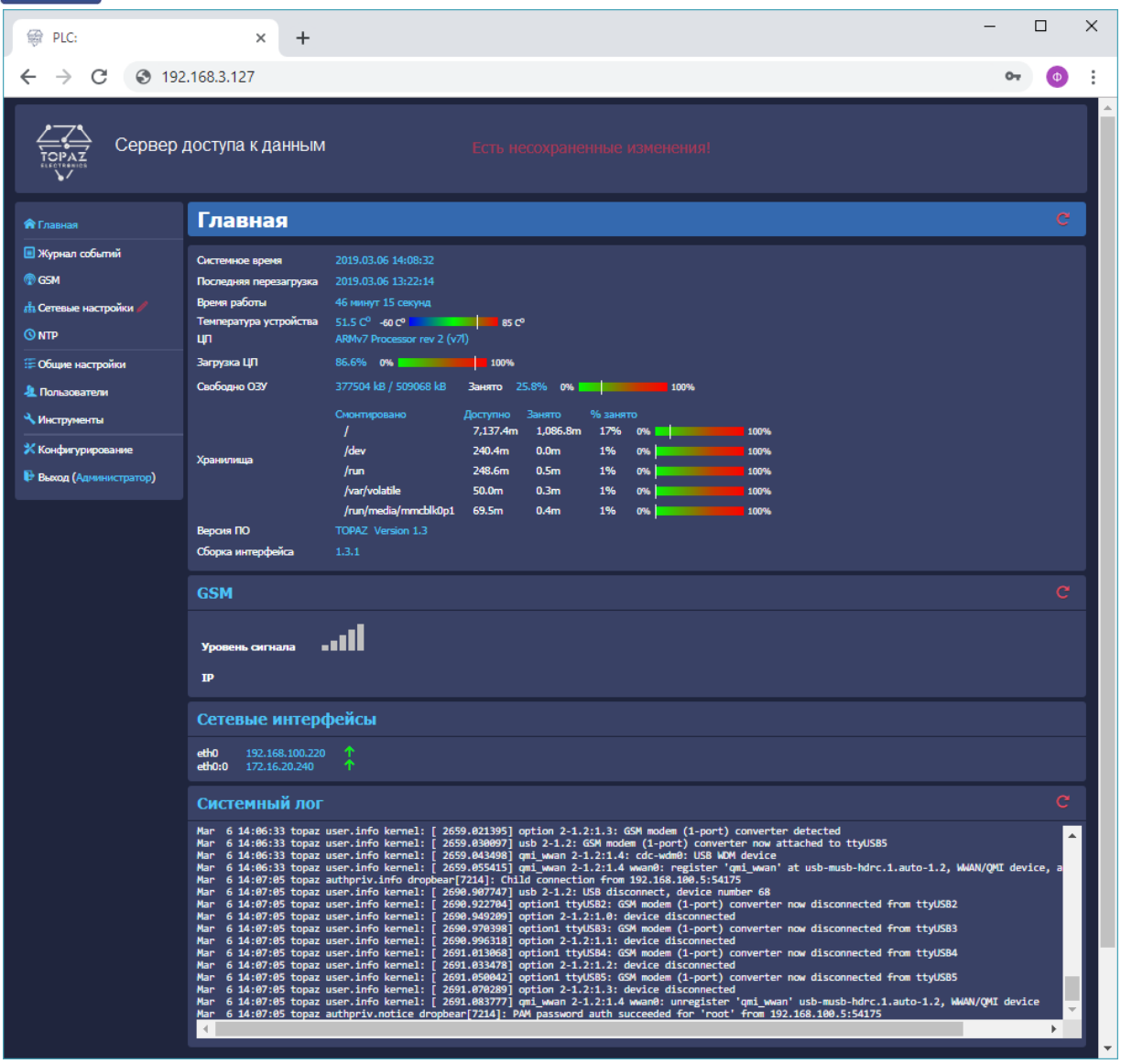


Рисунок 8 – Основное окно web-интерфейса (раздел «Главная»)

1.8.2 Работа с web-интерфейсом

Навигация по разделам web-интерфейса осуществляется через главное меню, расположенное в левой части окна web-браузера.

При переходе в раздел, происходит загрузка текущих данных и параметров данного раздела. В правом верхнем углу каждой области раздела расположена кнопка . Нажатие на данную иконку производит обновление текущих данных соответствующей области.

Для того, чтобы редактируемые изменения настроек текущего раздела вступили в силу, необходимо нажать кнопку Сохранить. Для того, что бы отменить текущие несохраненные изменения, следует нажать кнопку Вернуть прежние. При наличии несохраненных настроек, в верхней части экрана загорится надпись: «Есть несохраненные изменения!», а напротив раздела с измененными, но не сохраненными, настройками будет отображена иконка .

При работе со списками для добавления нового элемента списка следует нажать на кнопку . Для удаления элемента списка следует нажать кнопку напротив интересующего элемента списка.

1.8.2.1 Раздел «Главная»

В данном разделе выводится общая информация об устройстве (рисунок 5).

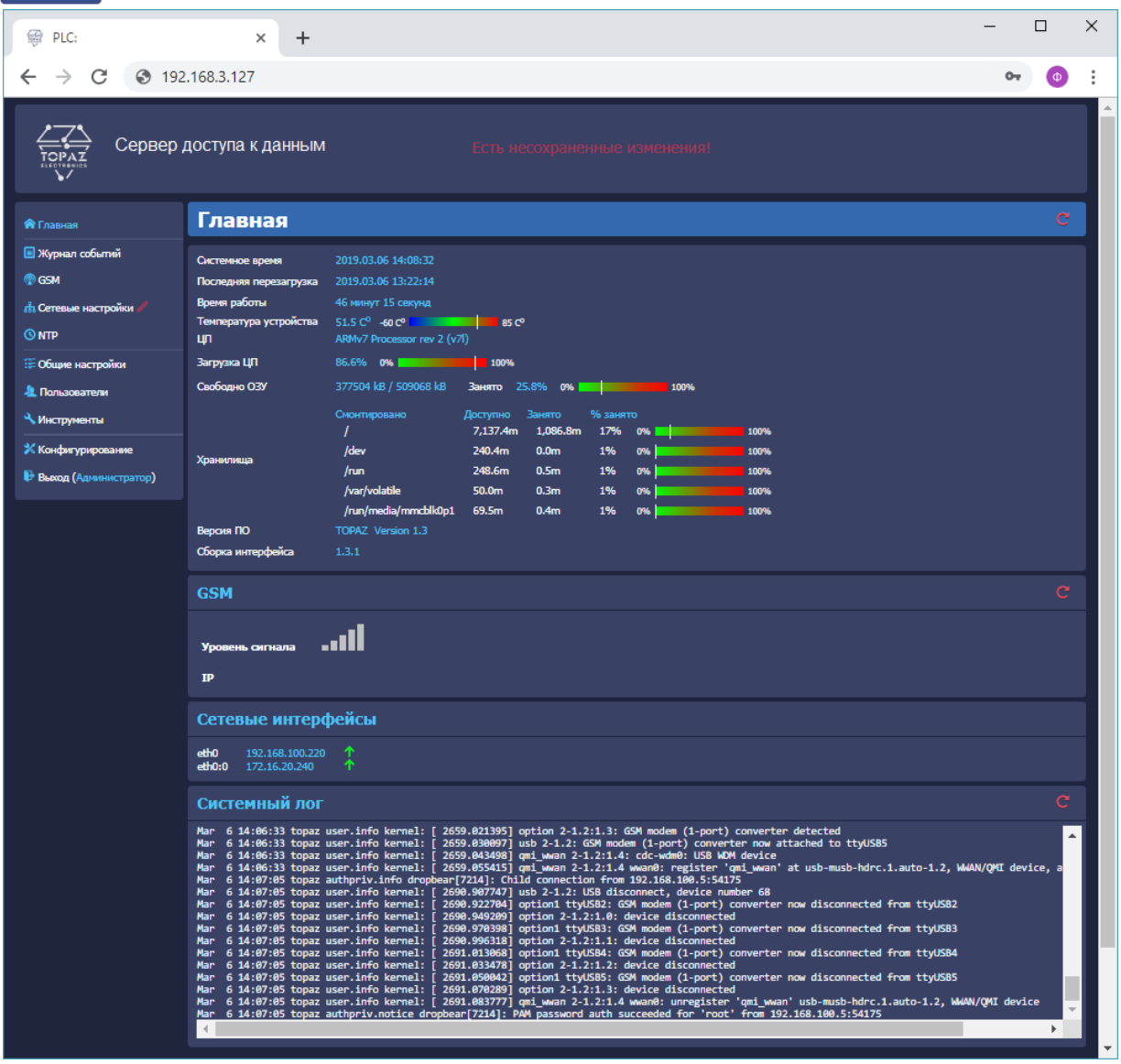


Рисунок 9 – Основное окно web-интерфейса (раздел «Главная»)

Таблица 36 – Поля раздела «Главная»

Название	Описание
Системное время	Текущие дата и время устройства согласно UTC
Последняя перезагрузка	Дата и время последней перезагрузки согласно UTC
Время работы	Время работы устройства (дней)
Температура устройства	Температура внутри корпуса устройства
ЦП	Модель центрального процессора (ЦП) устройства
Загрузка ЦП	Уровень загрузки ЦП
Свободное ОЗУ	Количество свободной оперативной памяти
Хранилища	Уровень загрузки физических и виртуальных хранилищ.
Версия ПО	Версия программного обеспечения устройства
Сборка интерфейса	Версия web-интерфейса
GSM	Уровень сигнала GSM модема и IP-адрес сим карты, выдаваемый оператором сотовой сети (при наличии GSM модема в модификации)

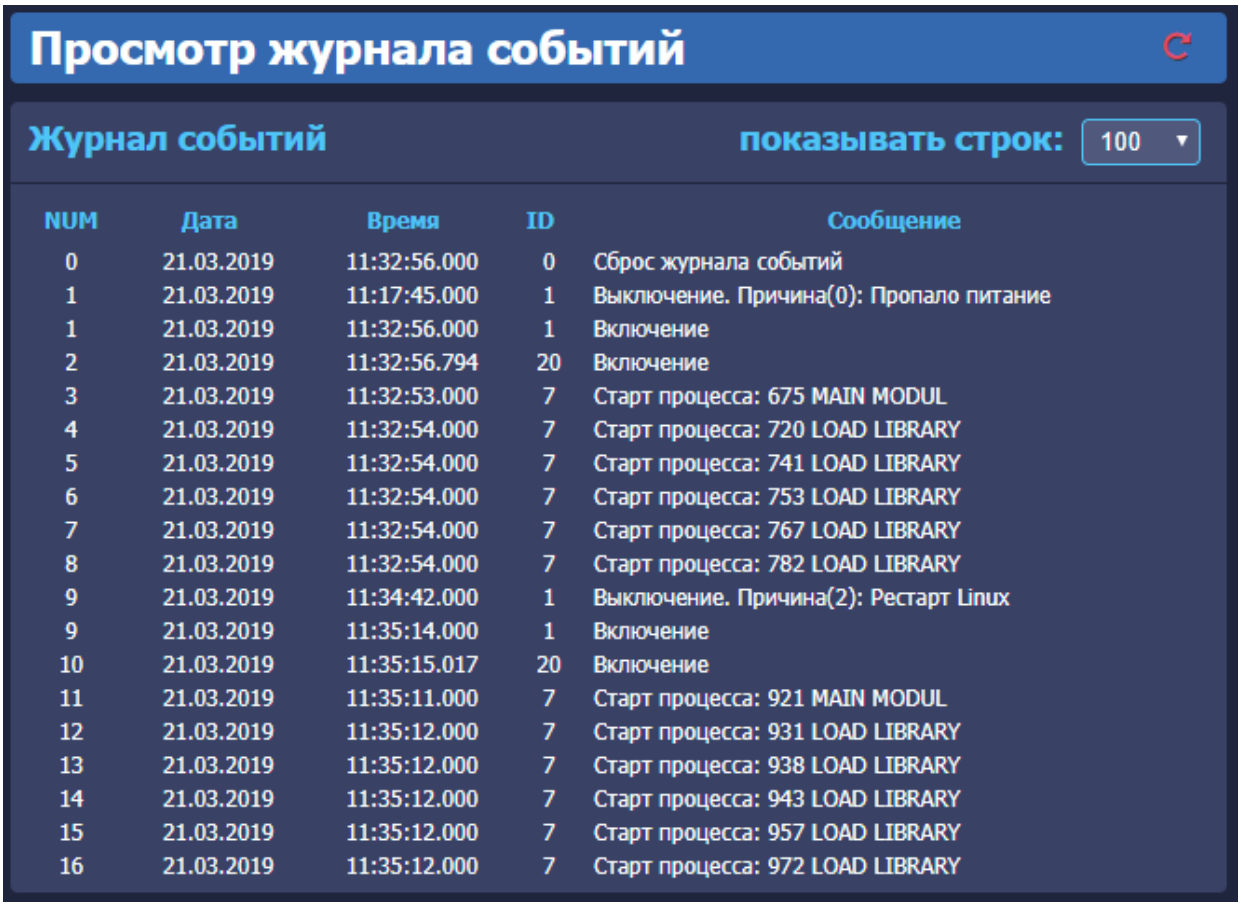
Название	Описание
Сетевые интерфейсы	Таблица интерфейсов Ethernet устройства (название, IP-адрес, текущее состояние). Количество интерфейсов может отличаться от количества портов устройства, в зависимости от выбранных настроек.
Статус GPS	Состояние работы ГЛОНАСС/GPS приемника (при наличии в модификации)
Системный лог	Лог событий устройства.

1.8.2.2 Раздел «Журнал событий»

В данном разделе отображен журнал событий устройства. В поле «показывать строк» можно задать количество событий на странице.

Таблица 37 – Поля раздела «Журнал событий»

Название	Описание
NUM	Номер события
Дата	Дата события
Время	Время события
ID	Идентификатор (тип) события.
Сообщение	Описание события



NUM	Дата	Время	ID	Сообщение
0	21.03.2019	11:32:56.000	0	Сброс журнала событий
1	21.03.2019	11:17:45.000	1	Выключение. Причина(0): Пропало питание
1	21.03.2019	11:32:56.000	1	Включение
2	21.03.2019	11:32:56.794	20	Включение
3	21.03.2019	11:32:53.000	7	Старт процесса: 675 MAIN MODUL
4	21.03.2019	11:32:54.000	7	Старт процесса: 720 LOAD LIBRARY
5	21.03.2019	11:32:54.000	7	Старт процесса: 741 LOAD LIBRARY
6	21.03.2019	11:32:54.000	7	Старт процесса: 753 LOAD LIBRARY
7	21.03.2019	11:32:54.000	7	Старт процесса: 767 LOAD LIBRARY
8	21.03.2019	11:32:54.000	7	Старт процесса: 782 LOAD LIBRARY
9	21.03.2019	11:34:42.000	1	Выключение. Причина(2): Рестарт Linux
9	21.03.2019	11:35:14.000	1	Включение
10	21.03.2019	11:35:15.017	20	Включение
11	21.03.2019	11:35:11.000	7	Старт процесса: 921 MAIN MODUL
12	21.03.2019	11:35:12.000	7	Старт процесса: 931 LOAD LIBRARY
13	21.03.2019	11:35:12.000	7	Старт процесса: 938 LOAD LIBRARY
14	21.03.2019	11:35:12.000	7	Старт процесса: 943 LOAD LIBRARY
15	21.03.2019	11:35:12.000	7	Старт процесса: 957 LOAD LIBRARY
16	21.03.2019	11:35:12.000	7	Старт процесса: 972 LOAD LIBRARY

Рисунок 10 – раздел «Журнал событий»

1.8.2.3 Раздел «SPY:Менеджер»

В данном разделе задаются параметры менеджера восстановления процессов.

Для включения мониторинга состояния сервиса iec-control включите опцию «Мониторить iec-controls». При включенной опции сервис iec-control будет восстановлен автоматически в случае, если произойдет его сбой. Параметр «Период» задает частоту опроса состояния iec-controls.

Кнопкой можно добавить менеджер RS485-Ethernet бриджа. Кнопкой можно добавить менеджер пользовательского процесса linux.

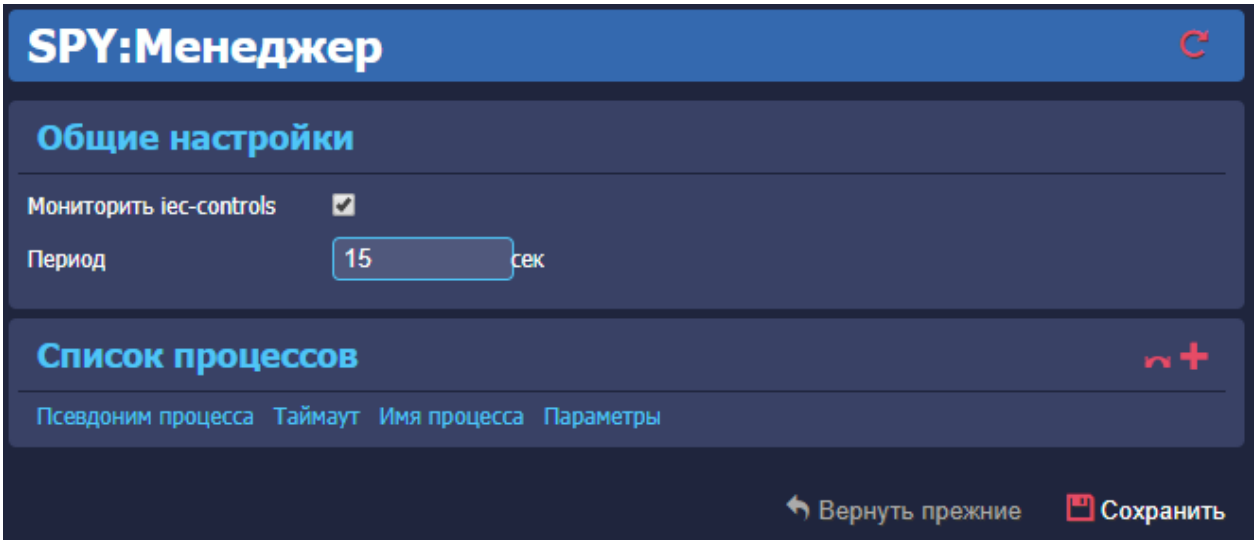


Рисунок 11 – Раздел «SPY:Менеджер»

1.8.2.4 Раздел «GSM»

Данный раздел предназначен для настройки мобильного Интернета на устройстве при наличии в модификации функции GSM-модема. Параметры SIM-карт задаются независимо.

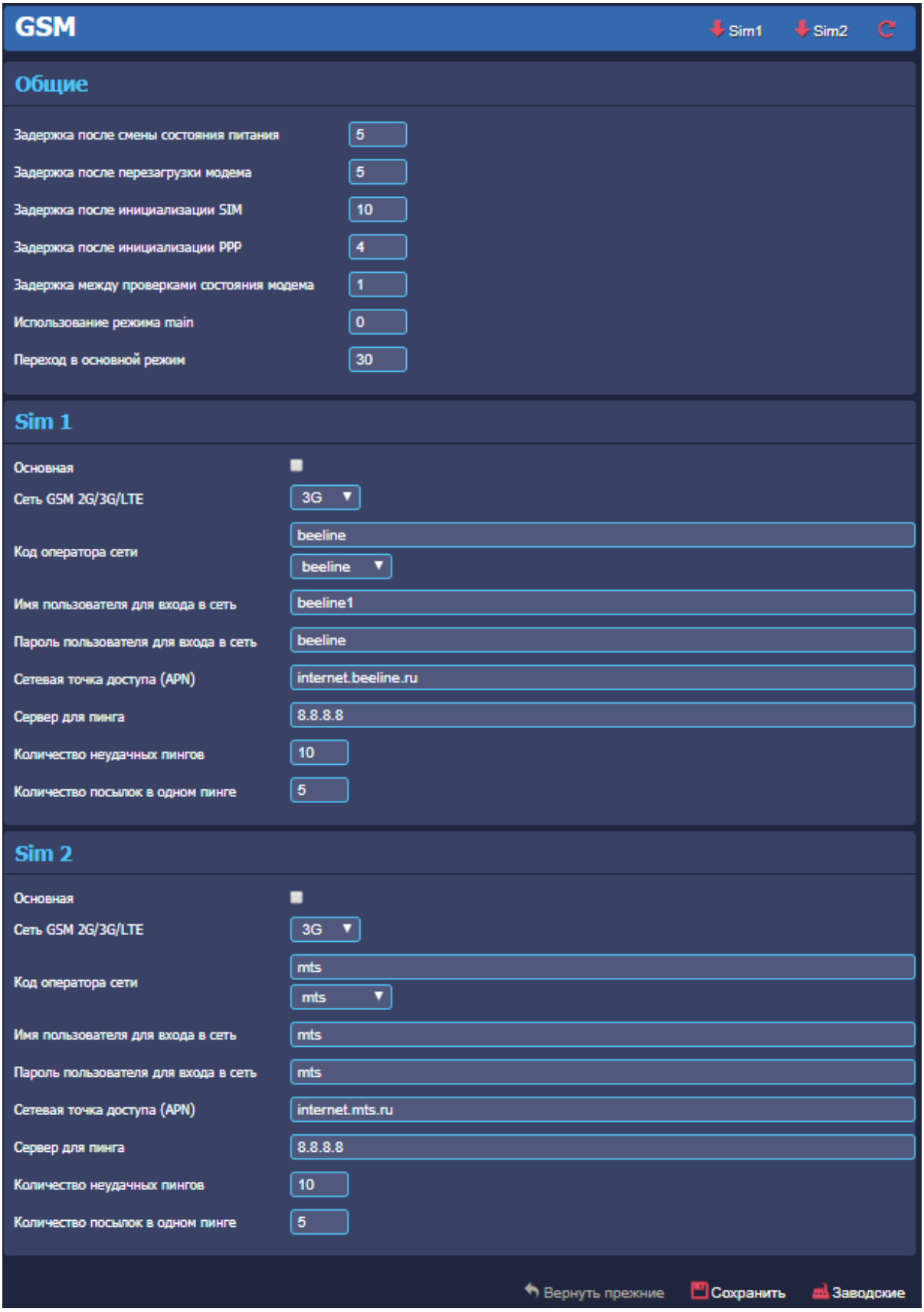


Рисунок 12 – Раздел «GSM»

Таблица 38 – Параметры SIM-карты

Поле	Описание
Общие параметры	
Задержка после смены состояния питания	Задержка (сек) на подключение к сетям GSM после включения устройства.
Задержка после перезагрузки модема	Задержка (сек) на подключение к сетям GSM после перезагрузки устройства.
Задержка после инициализации SIM	Задержка (сек) после инициализации SIM-карт устройства.
Задержка после инициализации PPP	Задержка (сек) после инициализации PPP.
Задержка между проверками состояния модема	Задержка (сек) между проверками состояния работы модема.
Использование режима main	Режим переключения Sim карт. 0 (по умолчанию)
Переход в основной режим	Задержка (сек)на переход в основной режим при восстановлении связи с основной Sim картой после потери связи.
Параметры Sim 1 (Sim 2)	
Основная	Является ли данная Sim-карта основной.
Сеть GSM 2G/3G/LTE	Выбор приоритетного режима работы с сотовыми сетями: LTE – работа в сети LTE; 2G – работа в сети 2G; 3G – работа в сети 3G.
Код оператора сети	Код оператора мобильной сети. Выбирается из списка или задается вручную.
Имя пользователя для входа в сеть	Имя пользователя для доступа в сотовую сеть провайдера
Пароль пользователя для входа в сеть	Пароль для доступа в сотовую сеть провайдера
Сетевая точка доступа (APN)	Имя сотовой сети (APN). Необходимо, если у SIM-карты корпоративный тариф или выделенная сотовая сеть внутри провайдера
Сервер для пинга	IP-адрес удаленного хоста для проверки работы соединения
Количество неудачных пингов	Количество неудачных ICMP запросов, приводящее к перезагрузке устройства.
Количество посылок в одном пинге	Количество ICMP пакетов отправляемых при проверке доступности IP-адреса удаленного хоста.

1.8.2.5 Раздел «GPS/ГЛОНАСС»

В данном разделе отображено состояние работы GPS/ГЛОНАСС приемника.

Таблица 39 – Описание полей раздела «GPS/ГЛОНАСС»

Настройка	Описание
Статус GPS	Состояние работы GPS/ГЛОНАСС приемника.
Статус антенны	Наличие подключенной антенны.
Активных спутников	Количество активных спутников GPS/ГЛОНАСС.
Статистика по спутникам	Детальная статистика по активным спутникам.

1.8.2.6 Раздел «Сетевые настройки»

В данном разделе можно задать параметры Ethernet, а также посмотреть текущее состояние активных интерфейсов Ethernet.

В таблице «Изменение параметров» приведены параметры существующих интерфейсов Ethernet. Добавление нового интерфейса выполняется кнопкой . Удаление существующего интерфейса осуществляется кнопкой . Нажатием кнопки можно добавить альтернативный адрес интерфейса.

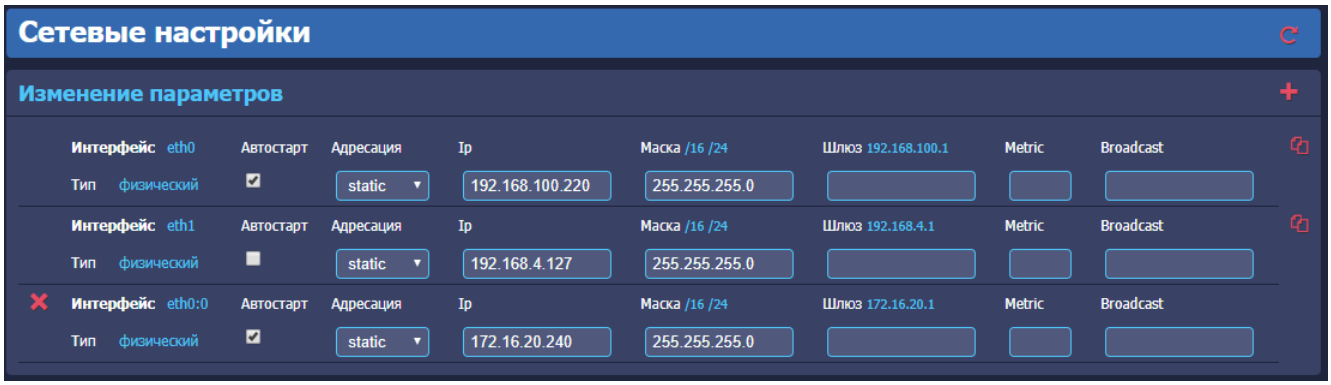


Рисунок 13 – Пример параметров интерфейсов Ethernet

Основные параметры интерфейсов Ethernet приведены в таблице ниже.

Таблица 40 – Основные параметры интерфейсов Ethernet

Название	Описание
Общие параметры	
Интерфейс	Имя интерфейса, задаваемое автоматически при добавлении.
Тип	Тип интерфейса, задаваемый при создании интерфейса. Физические интерфейсы привязаны к физическим портам Ethernet и их нельзя создавать или удалять.
Автостарт	Автоматический старт интерфейса при включении устройства
Адресация	Метод адресации: **static** (статический) – метод адресации интерфейсов по умолчанию. рекомендованный метод адресации, при котором интерфейсу задается статически выделенный IPv4 адрес. **manual** (вручную) –метод, используемый для описания интерфейсов, для которых нет настроек, применяемых по умолчанию. При данном методе, интерфейс настраивается вручную командами **up** и **down**, или сценариями из каталогов */etc/network/if–*.d.* **dhcp** (DHCP-клиент) – метод, используемый для получения адреса через DHCP. Данный метод не рекомендован к использованию, так как при нем устройство имеет динамический IP-адрес
Параметры адресации метода static	
IP	IP-адрес устройства
Маска	Маска подсети
Шлюз	Шлюз интерфейса
Metric	Метрика шлюза, используемая для маршрута по умолчанию
Broadcast	Широковещательный адрес, используемый для передачи широковещательных пакетов в сети
Параметры адресации метода dhcp	
Metric	Метрика шлюза, используемая для маршрутов.

Название	Описание
Время аренды в часах	Запрашиваемое время аренды в часах.
Время аренды в секундах	Запрашиваемое время аренды в секундах.

При добавлении нового интерфейса необходимо задать его типа и параметры, после чего нажать кнопку «Записать». Пример окна добавления нового интерфейса приведен ниже.

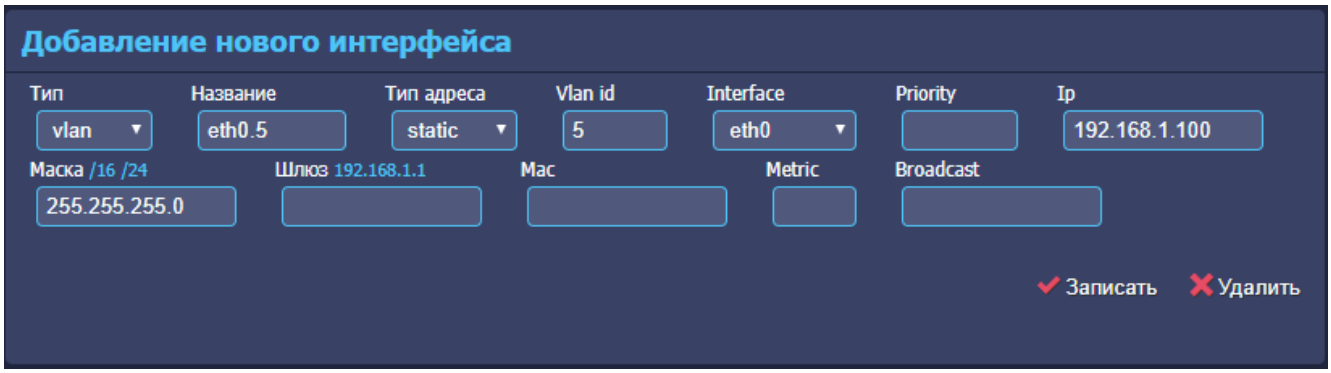


Рисунок 14 – Окно добавления нового интерфейса

Параметры интерфейсов приведены в таблице ниже.

Таблица 41 – Параметры интерфейсов Ethernet

Название	Описание
Тип	Тип интерфейса: **bridge** – мост; **vlan** – виртуальная сеть (VLAN); **prp** – резервирование по протоколу PRP; **hsr** – резервирование по протоколу HSR; **bond** – агрегирование каналов Ethernet; **rstp** – RSTP; **vrrp** – VRRP.
Параметры bridge	
Slave 1 … Slave n	Интерфейсы, объединенные в данный мост
bridge_stp	Задействовать ли stp для данного моста
Параметры vlan	
Vlan id	VLAN ID - идентификатор/номер виртуальной сети. У каждой VLAN должен быть уникальный идентификатор
Interface	Интерфейс данной VLAN
Priority	Приоритет VLAN при тегировании (0-7)
Mac	MAC-адрес (уникальный идентификатор) VLAN
Параметры prp	
Slave 1	Интерфейс 1 пары PRP
Slave 2	Интерфейс 2 пары PRP
Параметры hsr	
Slave 1	Интерфейс 1 кольца HSR
Slave 2	Интерфейс 2 кольца HSR
Параметры bond	
Slave 1 … Slave n	Интерфейсы, объединенные в единый канал

Название	Описание
Тип	Режим агрегирования: **balance-rr** – последовательная передача пакетов с **Slave 1** по **Slave n**; **active-backup** – активен один интерфейс, если активный интерфейс вышел из строя (link down), другой интерфейс заменяет активный; **balance-xor** – передача распределяется между интерфейсами на основе формулы «(**MAC_источника** XOR **MAC_получателя**) % **число_интерфейсов**». Один интерфейс работает с определенным получателем. Режим обеспечивает балансировку нагрузки и отказоустойчивость. **broadcast** – все пакеты передаются параллельно по всем интерфейсам; **802.3ad** – Link Agregation; **balance-tlb** – входящие пакеты принимаются только активным сетевым интерфейсом, исходящий трафик распределен в зависимости от текущей загрузки интерфейсов; **balance-alb** – входящий и исходящий трафик распределен в зависимости от текущей загрузки интерфейсов.
Miimon	Частота наблюдения (MII link). Данное значение определяет как часто будет проверяться состояние соединения на каждом из интерфейсов.
Down delay	Время ожидания, прежде чем отключить slave в случае отказа соединения. Данная опция влияет на **Miimon**.
Up delay	Время ожидания, прежде чем включить slave после восстановления соединения. Данная опция влияет на **Miimon**.
Параметры rstp	
Slave 1 … Slave n	Интерфейсы, объединенные в RSTP
Параметры vrrp	
ID	ID для виртуального устройства (VRID). Значение 0-255
Проверка (сек)	Частота, с которой устройством отправляется сообщения о свой активности.
Приоритет	Приоритет (Priority). Устройство с наибольшим приоритетом будет выбрано в качестве master и станет держателем virtual ip (адрес по которому с устройством будут связываться другие устройства в сети).

В поле «Текущее состояние устройства» отображены параметры и статистика работы активных интерфейсов , в примере ниже “eth0” – **LAN1**, “eth1” – **LAN2**, “lo” – **localhost**.

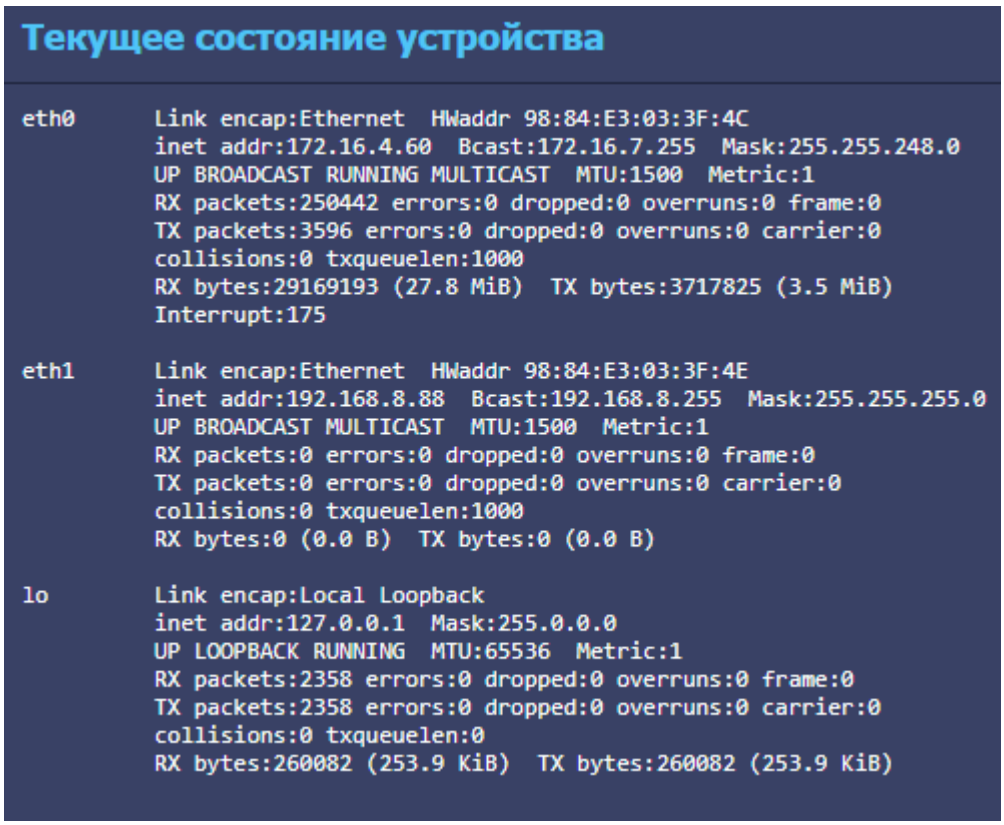


Рисунок 15 – Пример текущего состояния интерфейсов Ethernet

1.8.2.7 Раздел «NTP»

В данном разделе приведены настройки и статистика синхронизации по протоколу NTP.

Таблица 42 – Настройки NTP

Столбец	Описание
peer	Наличие соседнего сервера.
ip/url	Адрес NTP сервера к которому осуществляются запросы синхронизации.
prefer	Является ли данный сервер предпочитаемым.
burst	Посылать 8 пакетов вместо одного.
iburst	Ускорить начальный процесс синхронизации.
nomodify	Запретить удаленную настройку.
notrap	отправлять сообщение об исключении внешним серверам.
ignore	Запретить любые сообщения с указанного адреса.
minpoll	Минимальное время опроса сервера.
maxpoll	Максимальное время опроса сервера.
stratum	Stratum уровень устройства. Для устройств, синхронизирующих собственные часы непосредственно от систем ГЛОНАСС/GPS, данное значение, как правило, задается равным 1.
refid	Вышестоящий сервер.

В таблице «Синхронизация» области «Статистика» отображен список серверов точного времени, находящихся в одной сети с устройством.

Таблица 43 – Описание таблицы «Синхронизация»

Столбец	Описание
remote	IP-адрес удаленного сервера (из списка в конфигурационном файле) Перед IP-адресом сервера может стоять префикс, обозначающий следующее: ***** (звездочка) — устройство синхронизируется от данного источника; **+** (плюс) — сервер доступен в качестве источника синхронизации; **-** (минус) — использовать данный сервер в качестве источника синхронизации не рекомендуется; **#** (решетка) — выбран для синхронизации, но есть 6 лучших кандидатов; **X** (крестик) — сервер недоступен; **.** (точка) — исключен из списка кандидатов из-за большого расстояния; **пробел** — слишком большой уровень, цикл или ошибка. Для локального сервера точного времени (приемник ГЛОНАСС/GPS данного устройства) вместо IP-адреса отображается текст «**LOCAL(0)**». В случае, когда приемник ГЛОНАСС/GPS данного устройства является источником синхронизации, он отображается как ***LOCAL(0)**. Внутренний приемник ГЛОНАСС/GPS по умолчанию имеет Stratum 0.
refid	Reference ID сервера
st	Stratum сервера.
t	Тип пира (u- unicast, m- multicast)
when	Время последней синхронизации
poll	Время в секундах, за которое сервис NTP синхронизируется с пиром
reach	Доступность сервера – восьмеричное представление массива из 8 бит, отражающего результаты последних восьми попыток соединения с сервером. Значение 377 означает, что последние восемь запросов были успешны.
delay	Время задержки ответа от сервера
offset	Разница времени между локальным сервером и сервером синхронизации. Положительное значение означает, что локальные часы опережают часы удаленного сервера, отрицательное —отстают.
jitter	Дисперсия - мера статистических отклонений от значения смещения (поле offset) по нескольким успешным парам запрос-ответ. Меньшее значение дисперсии предпочтительнее, поскольку позволяет точнее синхронизировать время.

В поле **Статистика по клиентам** отображена статистика синхронизации по протоколу NTP клиентов, подключенных к устройству за последние 20 минут.

1.8.2.8 Раздел «Общие настройки»

В данном разделе находятся общие настройки устройства. В нем можно задать источник синхронизации времени (NTP или RTU327) и часовой пояс.

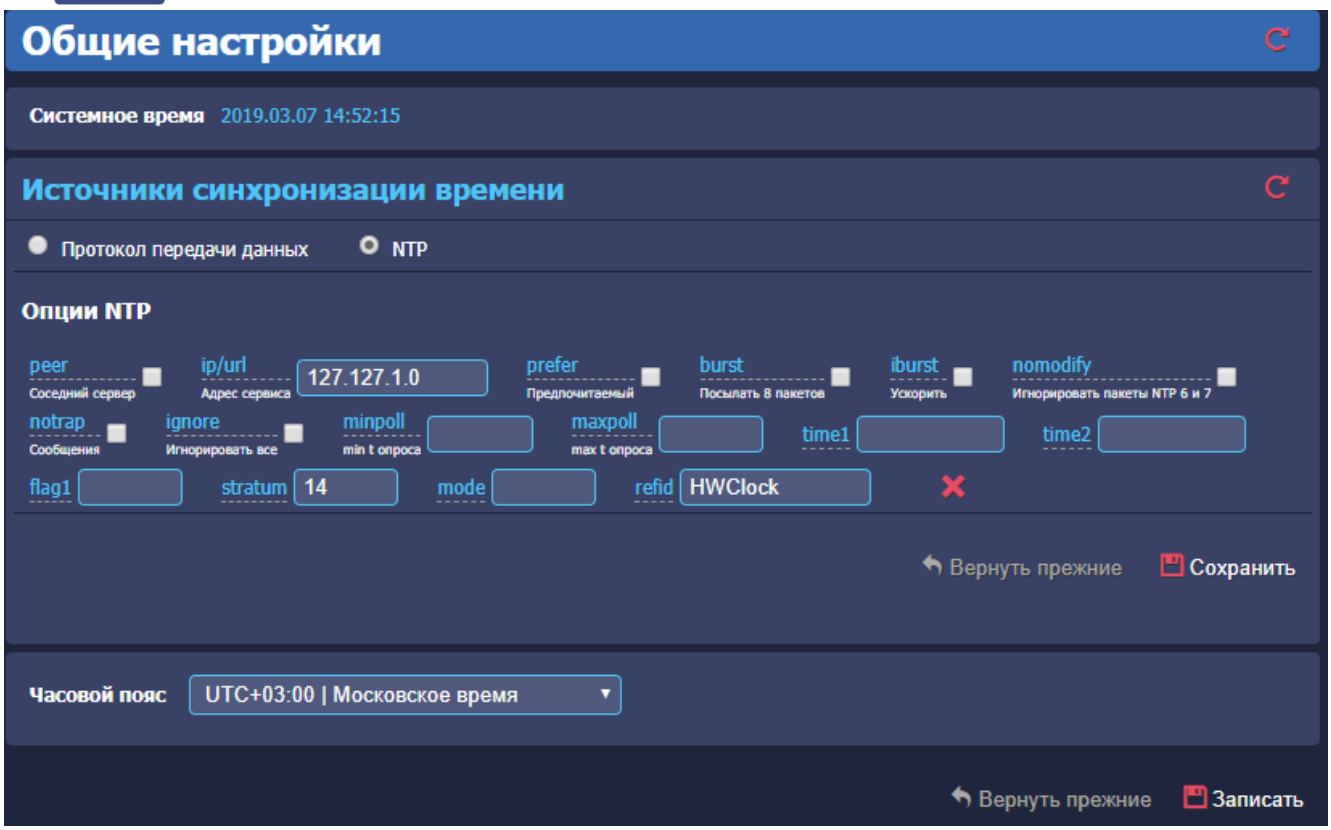


Рисунок 16 – Внешний вид раздела «Общие настройки»

1.8.2.9 Раздел «Пользователи»

Удалить пользователя (действие доступно только для администраторов) можно с помощью кнопки . Чтобы изменить пароль пользователя следует нажать кнопку .

Таблица 44 – Описание таблицы «Список активных пользователей»

Столбец	Описание
№	Порядковый номер
Логин	Имя пользователя
Роль	Права учетной записи: **Администратор** – пользователь может изменять параметры устройства, добавлять, удалять и задавать пароль учетных записей; **Менеджер** – пользователь может изменять только параметры устройства; **Оператор** – пользователь может просматривать параметры устройства без возможности редактирования.

По умолчанию в устройстве зарегистрирован пользователь **admin** (пароль **admin**, роль администратор).

1.8.2.10 Раздел «Инструменты»

<u>Перезагрузка</u>

Для перезагрузки устройства нажмите кнопку Перезагрузить устройство.

<u>Статусы служб</u>

В данном поле отображен статус запущенных служб.

Ping host

Утилита для проверки соединения с удаленным узлом.

Чтобы проверить соединение:

- Введите IP-адрес удаленного узла в поле **Хост**;
- Введите лимит лога;
- Нажмите кнопку **Start**, и в поле **Лог** будет отображен результат проверки.

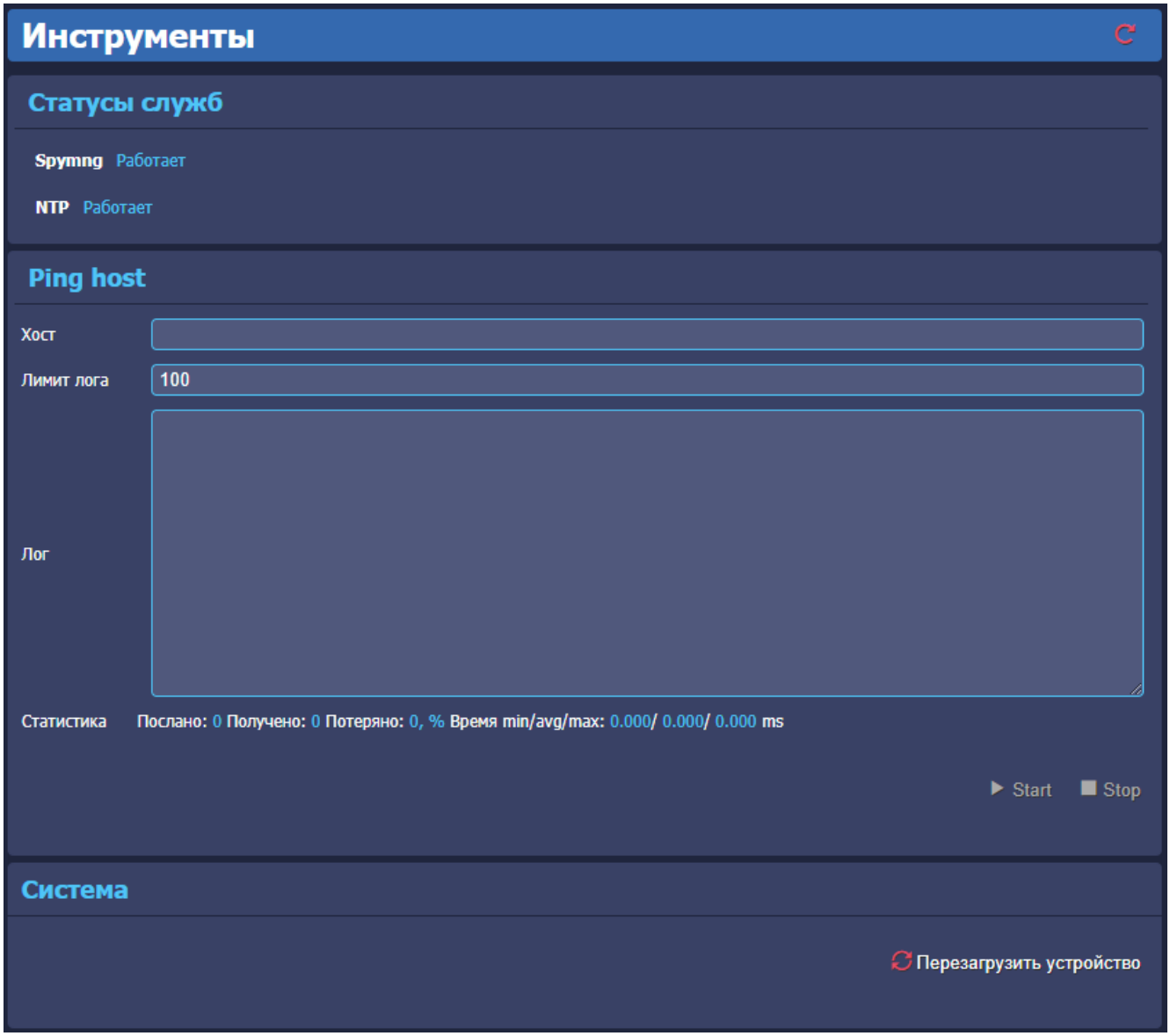


Рисунок 17 – Внешний вид раздела «Инструменты»

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}С;
- значение относительной влажности воздуха: 30-80 %.

Предельные климатические факторы хранения:

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

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

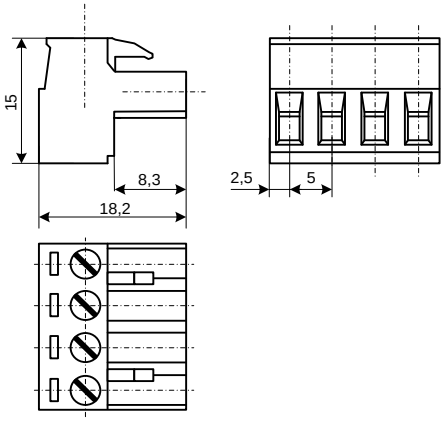


Рисунок 19 – Габаритные размеры разъема MSTBT 2,5/4-ST

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».

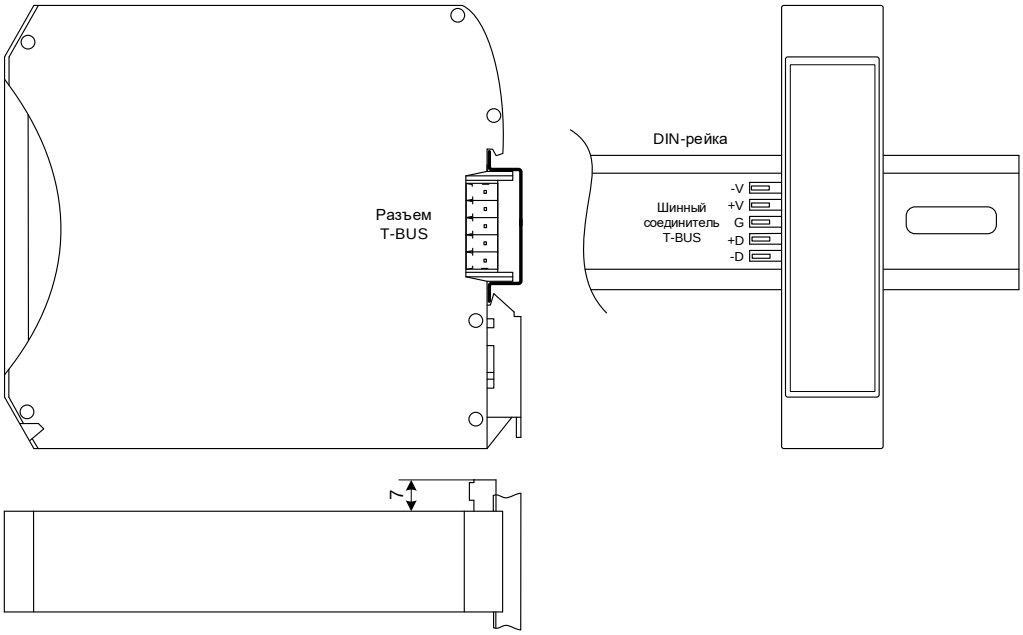


Рисунок 20 – Размещение устройства на DIN-рейке с шиной T-BUS

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

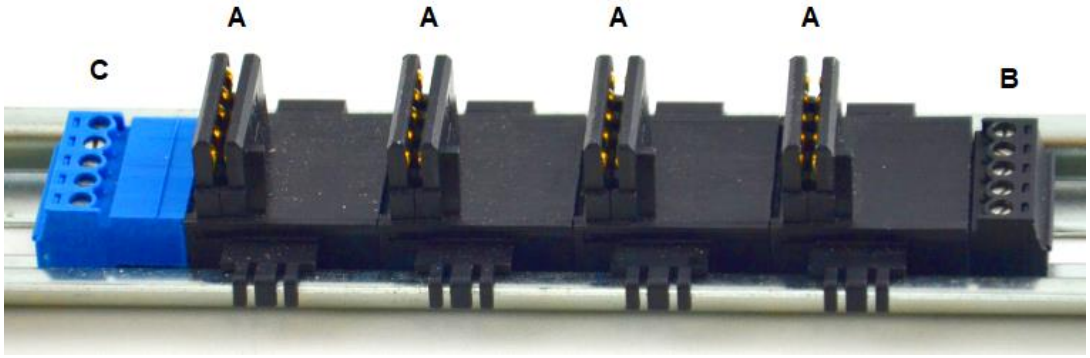


Рисунок 21 – Внешний вид шины T-BUS

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.

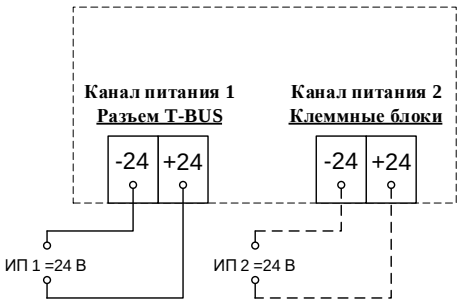


Рисунок 22 – Схема подключения питания каналов 24В

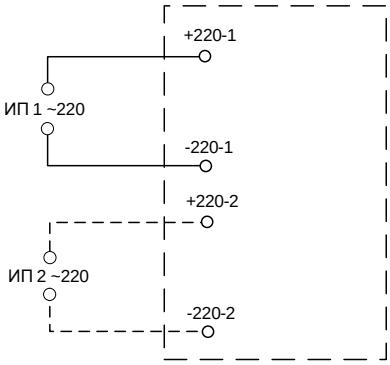


Рисунок 23 – Схема подключения питания каналов 220В

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).

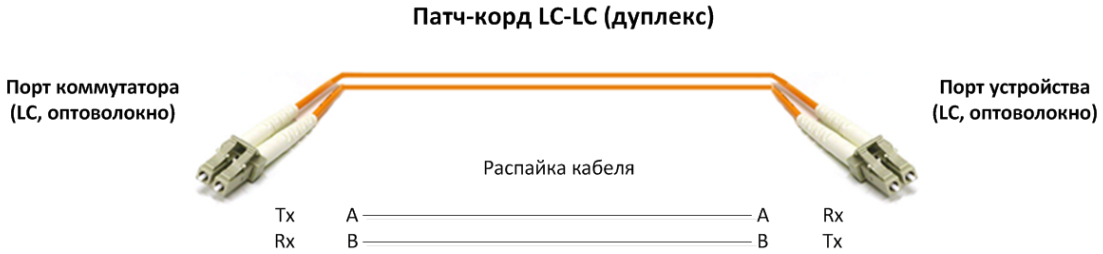


Рисунок 24 – Схема подключения оптоволоконного кабеля

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

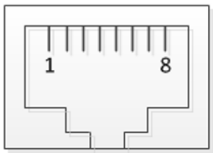
7.2.6.2 Подключение Ethernet-портов 10/100 BaseT(X)

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 45 – 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

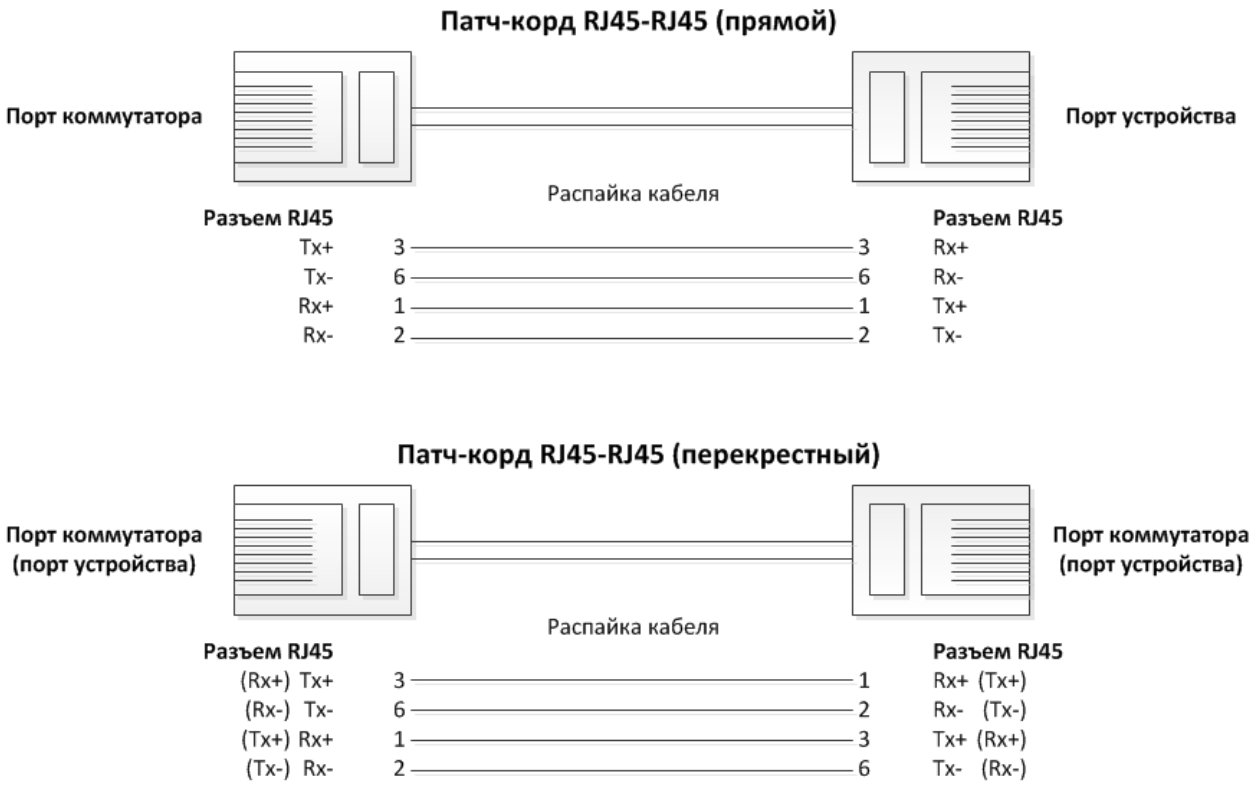


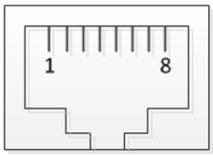
Рисунок 25 – Схема соответствия контактов

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 46 – 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 22. Назначение контактов клеммных блоков RS-485 приведено на рисунке 23. Клеммы подключения к интерфейсу RS-485-1 контроллерной платы устройства дублированы на шине T-BUS.

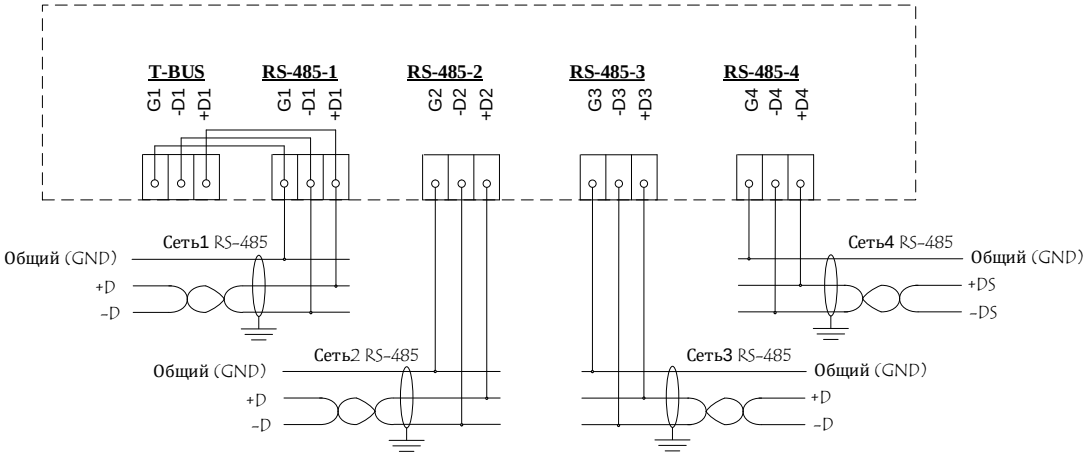


Рисунок 26 – Схема подключения устройства к сетям RS-485

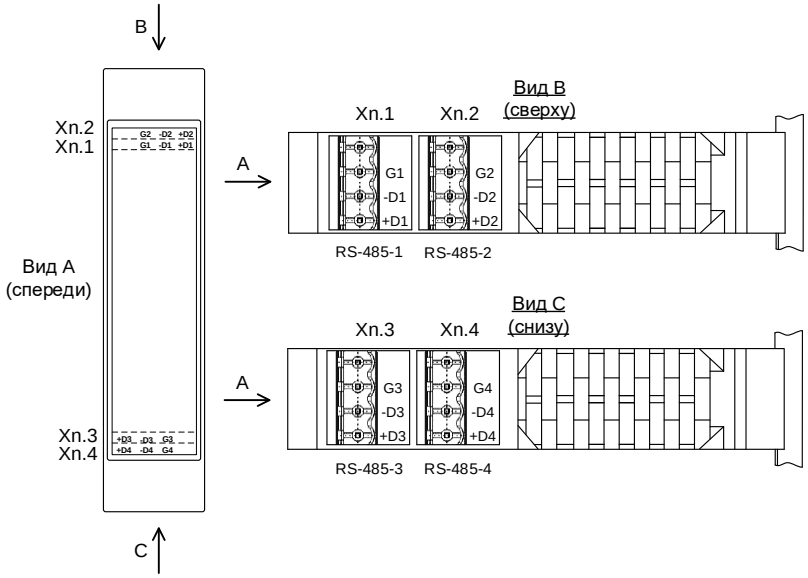


Рисунок 27 – Назначение контактов клеммных блоков RS-485

7.2.7.2 Подключение к сетям RS-422

Схема подключения к сети RS-422 приведена на рисунке 24. Назначение контактов клеммных блоков RS-422 приведено на рисунке 25. Сопротивление согласующего резистора (R_T) 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 24.

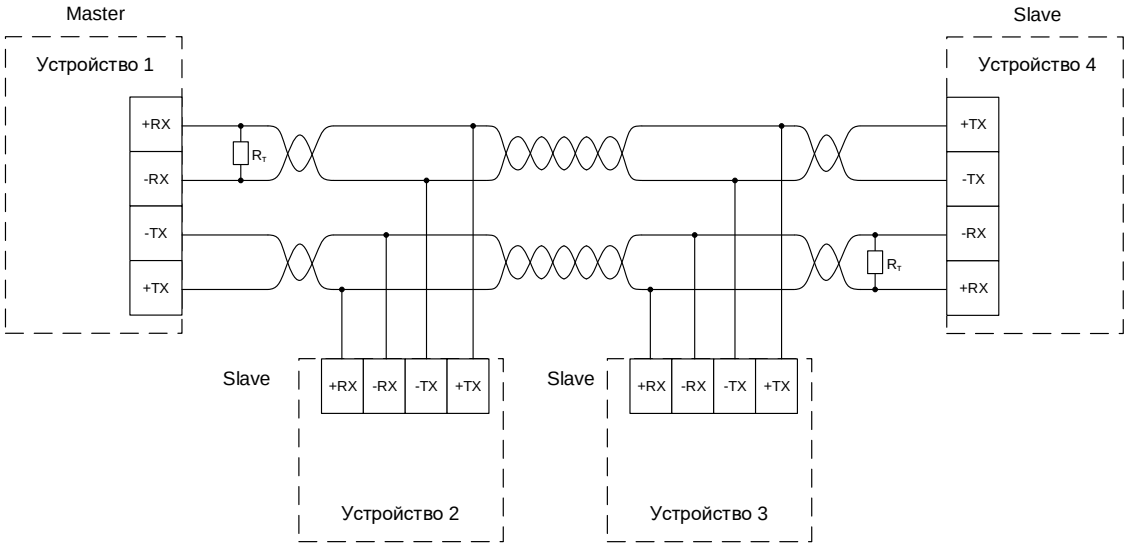


Рисунок 28 – Схема подключения устройств к сети RS-422

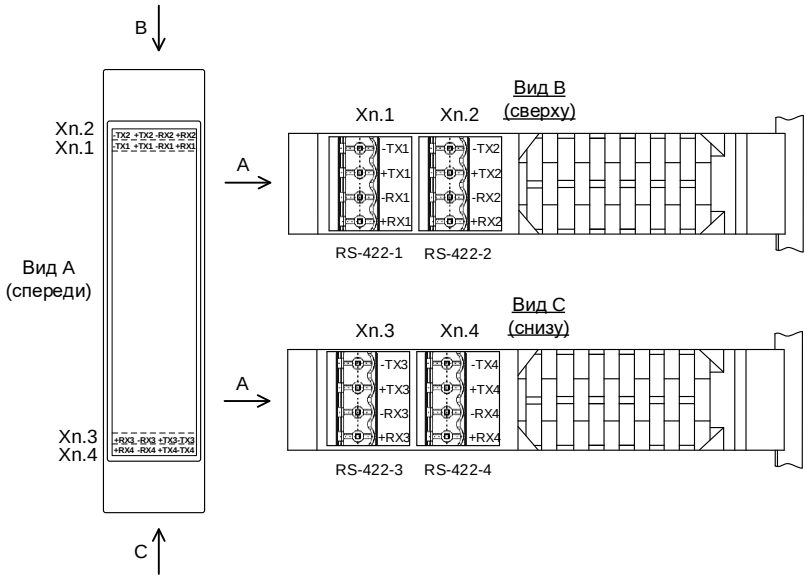
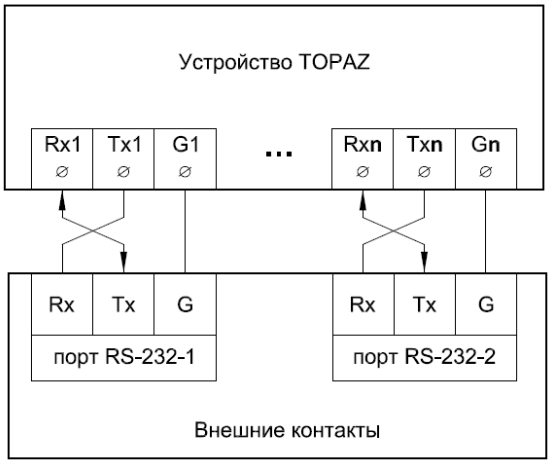


Рисунок 29 – Назначение контактов клеммных блоков RS-422

7.2.7.3 Подключение к сетям RS-232

Подключение по интерфейсу RS-232 может осуществляться как через клеммы, расположенные на верхней и нижней панелях устройства так и через вилку DB9, расположенную на передней панели.

Назначение клемм указано на корпусе устройства. На рисунке 26 представлена схема подключение клемм RS-232 устройства TOPAZ к другим устройствам.



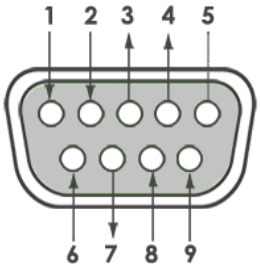
n – номер порта RS-232. Количество портов RS-232 определяется заказным обозначением устройства

Рисунок 30 – Схема подключение клемм RS-232

Назначение контактов вилки DB9 представлено в таблице 47.

Таблица 47 – 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

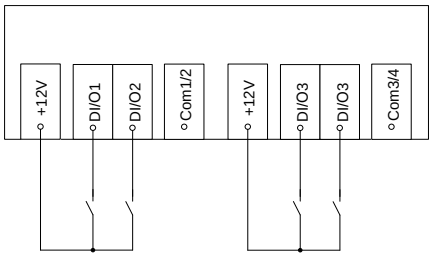


Рисунок 31 – Подключения каналов дискретного ввода с питанием от внутреннего источника питания.

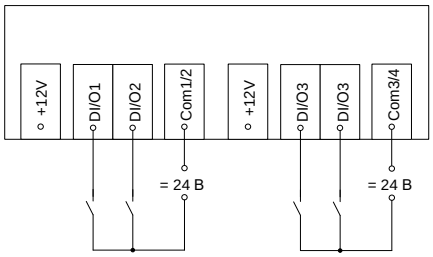


Рисунок 32 – Подключения каналов дискретного ввода с питанием от внешнего источника питания.

7.2.8.2 Режим дискретного вывода

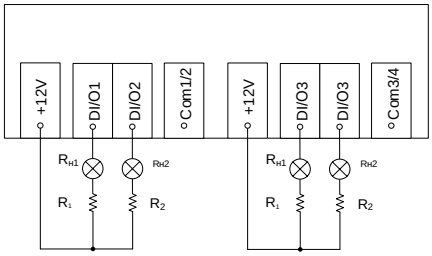


Рисунок 33 – Подключения каналов дискретного вывода с питанием от внутреннего источника питания.

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)

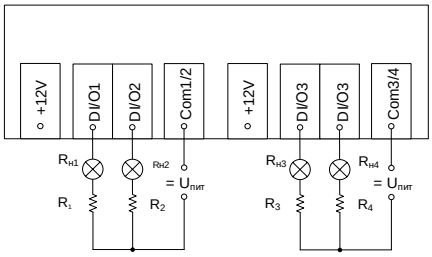


Рисунок 34 – Подключения каналов дискретного вывода с питанием от внешнего источника питания.

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 (при наличии GSM модема)

Для обеспечения возможности подключения устройства к сети Интернет через сотовую связь понадобится SIM-карта формата mini-SIM. До установки ее 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.

7.2.11 Подключение интерфейса человек-машина

Подключение сенсорного монитора **TOPAZ HMI15** осуществляется посредством двух кабелей: кабеля передачи видео данных **HDMI - DVI-D** и кабеля передачи данных сенсорного экрана **USB**, как показано на рисунке ниже.

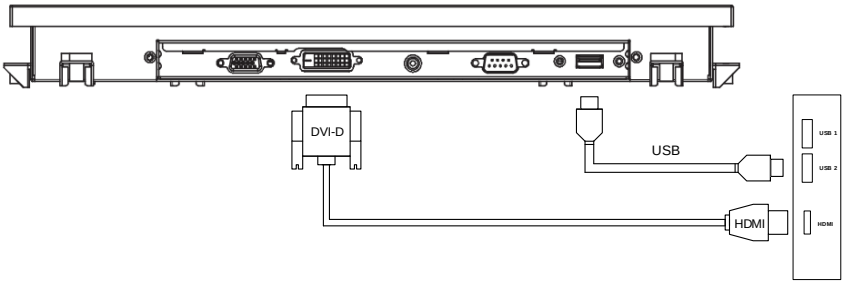


Рисунок 35 – Подключение каналов ввода/вывода монитора

Подключение других сенсорных мониторов, а также кнопочной панели TOPAZ HMI7 производится по схеме аналогичной схеме подключения сенсорного монитора HMI15.

ПРИЛОЖЕНИЕ А

Рисунок А.1 – Внешний вид устройства TOPAZ IEC DAS MX681 E6R6 2GSM (2GTx-4Tx-POE-6R)

Рисунок А.2 – Внешний вид устройства TOPAZ IEC DAS MX681 E3R2 (3GTx-2R)

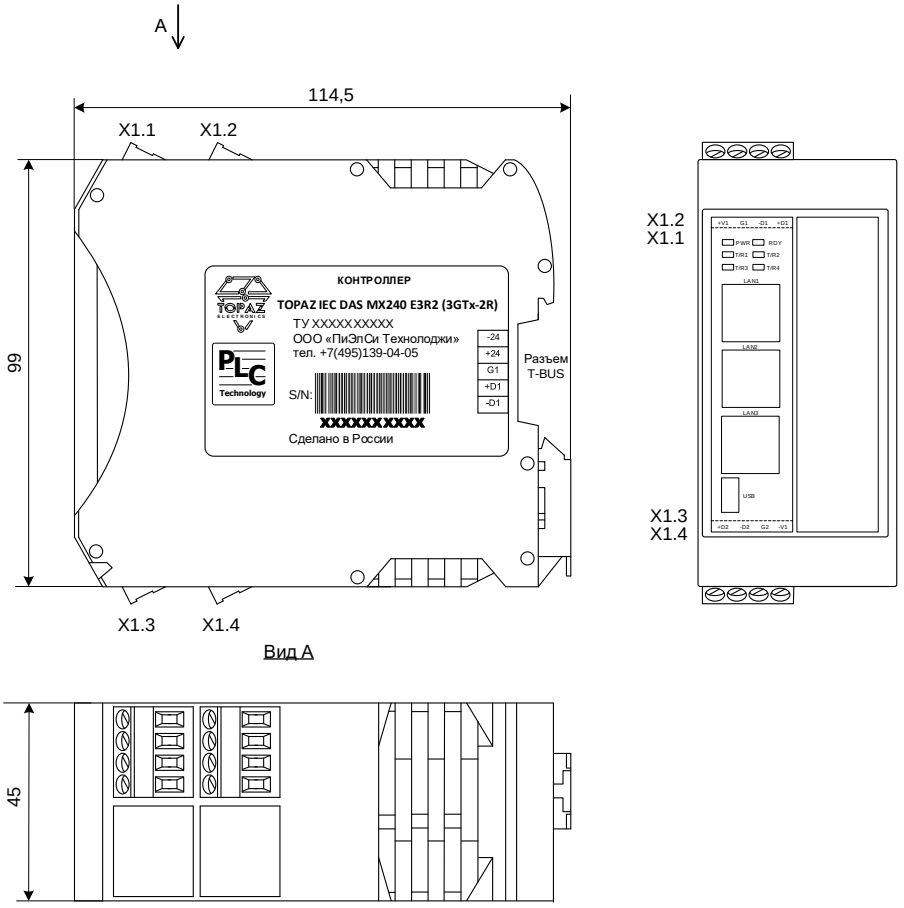


Рисунок А.3 – Габаритные размеры устройства TOPAZ IEC DAS MX681 E3R2 (3GTx-2R)

Таблица А.1 – Обозначения клемм и портов

Обозначение*	Описание
Питание напряжением постоянного тока	
+24 (+Vn)	Клеммы питания 24 В
-24 (-Vn)	
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)-

Обозначение*	Описание
+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
DIO3, DIO4	Каналы дискретного ввода 3 и 4 (группа 2)
COM3/4	Общий провод (группа 2)
+12V	Выход источника напряжения 12 В
* 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
PPS	Наличие синхронизации GPS/ГЛОНАСС
* 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):

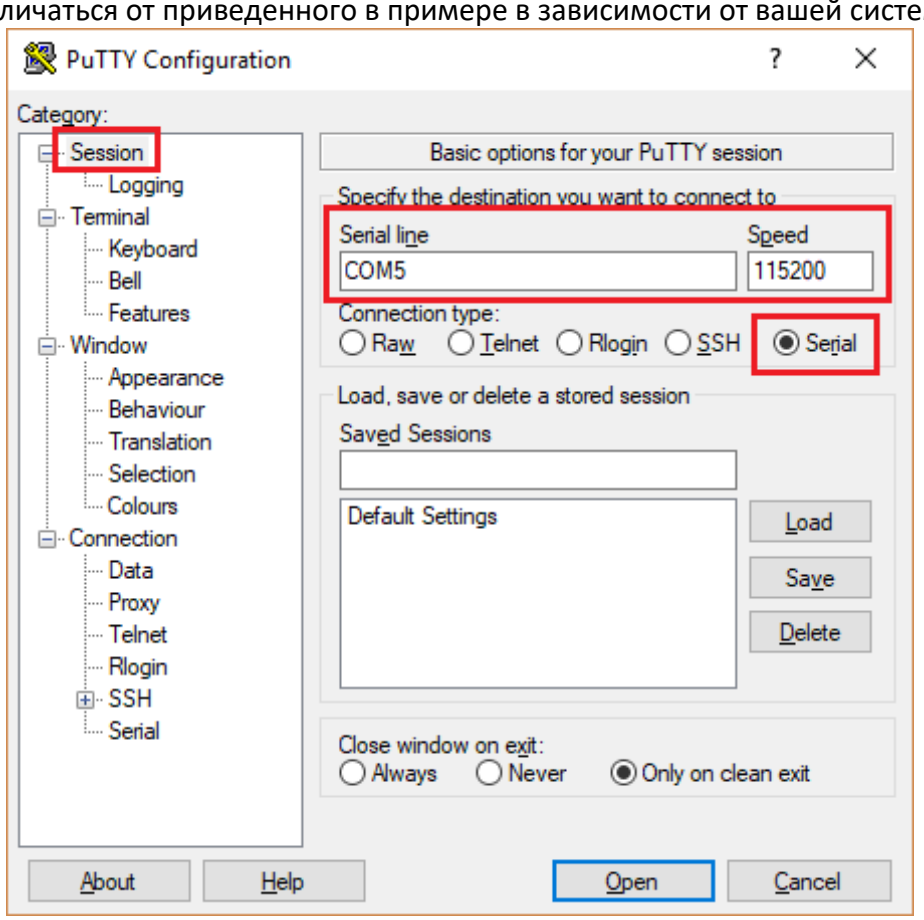


Рисунок Б.1 – Задаваемые настройки раздела Session (сессия)

В настройках соединения (**Connection**) – выбрать последовательный порт (**Serial**) и установить параметры соединения согласно таблице 16:

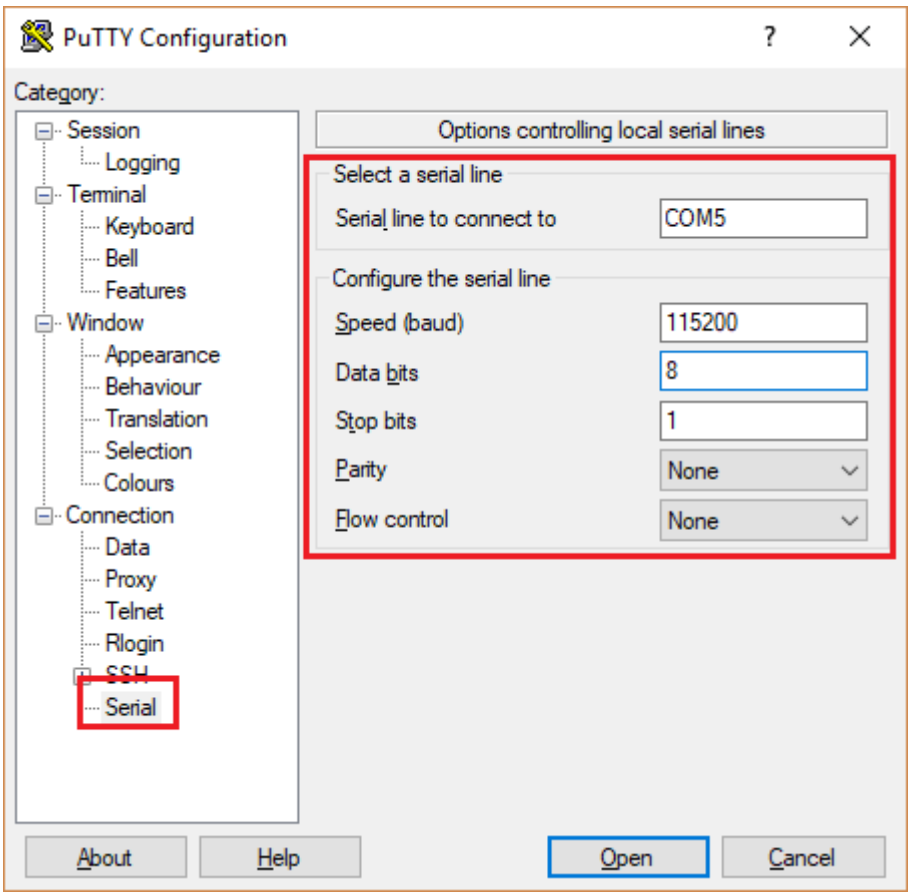


Рисунок Б.2 – Задаваемые настройки раздела Serial (серийный порт)

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

<u>Подключение через Ethernet порт</u>

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

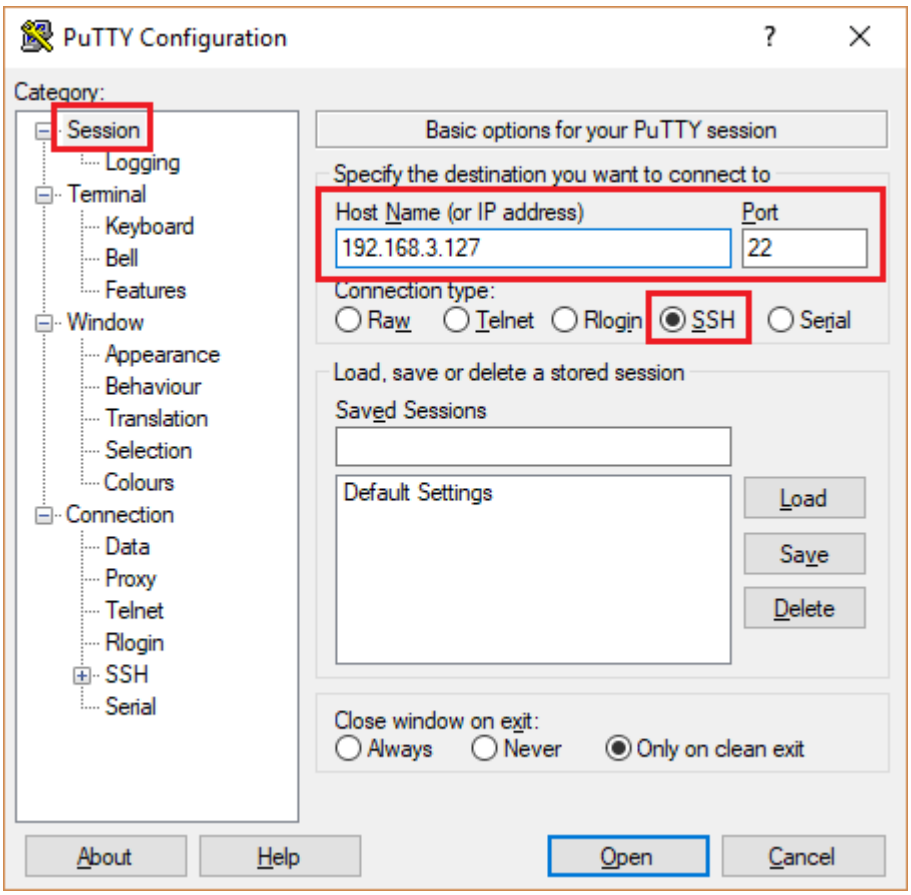


Рисунок Б.3 – Задаваемые настройки раздела Session (сессия)

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