

МИРТЕК®

изобретая будущее



УСПД
МИРТ-881

Руководство
администратора
МИРТ.411189.001Д5

03.2023



ЕАС

www.mirtekgroup.com

Аннотация

Данный документ представляет собой руководство администратора устройства сбора и передачи данных МИРТ-881 (далее по тексту – УСПД).

Руководство администратора предназначено для персонала, осуществляющего наладку (включая конфигурирование), эксплуатацию и техническое обслуживание УСПД и систем ИИС разработки ООО «МИРТЕК».

Перед началом работы с устройством администратор должен быть ознакомлен с данным документом.

Производитель оставляет за собой право выпускать обновления к указанному устройству, вносящие улучшения и дополнения, которые могут быть не отражены в настоящем Руководстве, без уведомления пользователей.

Наименование продукта УСПД МИРТ-881

Организация ООО «МИРТЕК»

Адрес г. Ставрополь, ул. Доваторцев, д.33а

E-mail info@mirtekgroup.ru

Дата 14.03.2023

Термины и сокращения:

COM-порт – последовательный коммуникационный порт персонального компьютера

RS-232 – Recommended Standard No.232 последовательный интерфейс

RS-485 – Recommended Standard No.485 последовательный интерфейс

Администратор – пользователь с определенным уровнем доступа, который позволяет осуществлять чтение собранных данных, чтение и запись всех параметров УСПД, в т. ч. редактирование параметров пользователей, чтение и редактирование настроек безопасности, чтение журнала безопасности

АСКУЭ – автоматизированная система контроля и учета электроэнергии

ГОСТ – государственный стандарт

Гость – пользователь с определенным уровнем доступа, который позволяет осуществлять чтение собранных данных, чтение всех параметров УСПД, кроме параметров пользователей

ВПО – встроенное программное обеспечение

ИБК – информационно-вычислительный комплекс

ИИС – информационно-измерительная система

КИИ – критическая информационная инфраструктура

Оператор – пользователь с определенным уровнем доступа, который позволяет осуществлять чтение собранных данных, чтение и запись всех параметров УСПД, кроме редактирования параметров пользователей

ОС – операционная система

ОСРВ – операционная система реального времени

ПК – персональный компьютер

ПО – программное обеспечение

ПУ – прибор учета

РА – руководство администратора

РП – руководство пользователя

РЭ – руководство по эксплуатации

УСПД – устройство сбора и передачи данных

Соглашения:

- наименования элементов интерфейса (кнопок в диалогах, пунктов меню, диалоговых окон, полей ввода и т. д.) выделены полужирным шрифтом, например: необходимо нажать кнопку **Считать**;
- значения, которые необходимо вводить в поля ввода, заключены в кавычки например: установите пользователю уровень доступа «Отключен»;
- цифры в круглых скобках в тексте перед наименованием рисунка, например: (1) (см. рисунок 5), означают порядковый номер шага на рисунке при выполнении того или иного действия;
- навигация в программе (краткая последовательность выбора пунктов меню и вкладок) обозначается символом →.
- контекстные переменные обрамляются символами <...>, например блок <Название журнала>.

Обратите повышенное внимание на инструкции, которые следуют за знаками:



важно



обязательно к исполнению

Содержание

1 Общие сведения	7
1.1 Назначение и область применения	7
1.2 Требования к пользователю	7
1.3 Сведения о программном обеспечении	7
1.3.1 Встроенное программное обеспечение	7
1.3.2 Системное программное обеспечение	8
1.3.3 Прикладное программное обеспечение	8
1.4 Процедуры поставки программного обеспечения	8
2 Порядок ввода УСПД в эксплуатацию	8
2.1 Общие сведения	8
2.2 Начало работы с УСПД	9
2.2.1 Подключение	9
2.3 Отображение информации об УСПД	11
2.4 Конфигурирование и просмотр данных	12
3 Обеспечение безопасности УСПД	14
3.1 Общие сведения	14
3.1.1 Действия УСПД при нарушении целостности ПО	16
3.2 Функции безопасности УСПД	16
3.3 Процедуры идентификации и аутентификации	20
3.4 Мероприятия по обеспечению безопасности	20
3.5 Работа с ПУ по протоколу СПОДЭС	21
3.5.1 Основные положения в части безопасности	21
3.5.2 События ПУ, принимаемые УСПД	23
4 Управление пользователями	25
4.1 Вкладка Управление пользователями	25
4.1.1 Добавление пользователя	26
4.1.2 Считывание списка пользователей	26
4.1.3 Редактирование пользователя	26
4.1.4 Запрещение подключения к УСПД	27
4.2 Вкладка Расширенные настройки безопасности	27
4.2.1 Чтение параметров безопасности	30
4.2.2 Добавление параметров безопасности	30
5 Сетевые настройки	30
5.1 Настройка сетевых интерфейсов	30

5.1.1 Чтение списка интерфейсов и сетевой конфигурации	31
5.1.2 Добавление IP-адреса	32
5.1.3 Изменение IP-адреса	32
5.1.4 Удаление IP-адреса	33
5.1.5 Добавление маршрута	33
5.1.6 Изменение маршрута	34
5.1.7 Удаление маршрута	34
5.2 Общие настройки	35
5.3 Состояние сетевых интерфейсов	36
5.4 SSL-сертификаты	36
5.4.1 Загрузка сертификата	37
5.4.2 Запись сертификата Веб-сервера	38
6 Обновление ПО и дополнительные настройки	38
6.1 Дополнительно	38
6.1.1 Загрузка конфигурационного файла МЭК 104	39
6.1.2 Изменение адреса ASDU mek 104	40
6.1.3 Обновление ВПО	40
6.1.4 Перезагрузка УСПД	40
6.1.5 Изменение флага в блоке Дополнительные параметры	41
6.1.6 Ограничение количества ПУ для опроса	41
7 Действие с конфигурацией	41
7.1 Вкладка действие с конфигурацией	41
7.1.1 Сохранение файла конфигурации	42
7.1.2 Загрузка файла конфигурации	42
8 Чтение и анализ журналов	43
8.1 Журналы УСПД	44
8.1.1 Чтение журнала УСПД	44
8.2 Журналы ПУ	46
8.2.1 Чтение журнала ПУ	47
8.3 Журнал безопасности	48
8.3.1 Чтение журнала безопасности	49
8.3.2 Проверка контрольных сумм системного ПО	50
9 Сведения об уязвимостях	51
10 Возможные проблемы и способы их решения	51
11 Применение в составе объекта критической инфраструктуры	52
Приложение А	53

1 Общие сведения

1.1 Назначение и область применения

Назначение УСПД – учет энергоресурсов, измерение времени, синхронизация времени в счетчиках энергоресурсов, а также сбор, накопление, хранение и передача накопленной информации на верхний уровень информационно-измерительных систем. УСПД обеспечивают защиту собранных данных. УСПД является изделием расширенной функциональности, предназначенным для построения на его основе многофункциональных автоматизированных систем коммерческого учета электроэнергии и мощности (АСКУЭ) с распределенной обработкой и хранением данных.

Область применения УСПД – энергообъекты розничного рынка электроэнергии и учет энергоресурсов в жилищно-коммунальном хозяйстве. УСПД устанавливается на подстанциях, в распределительных щитах промышленных предприятий, жилых и офисных зданий.

УСПД соответствует требованиям:

- класса II по ГОСТ 12.2.091 по способу защиты человека от поражения электрическим током;
- ГОСТ Р 51522.1-2011 (МЭК 61326-1:2005), ГОСТ 32134.1-2013, ГОСТ Р 52459.7-2009 в части помехоэмиссии и помехоустойчивости;
- класса III по ГОСТ IEC 60950-1-2014 по защите от поражения электрическим током;
- безопасности согласно ГОСТ IEC 61010-1-2014, ГОСТ IEC 62311-2013, ГОСТ IEC 62479-2013.

УСПД является средством измерения и зарегистрировано в Государственном реестре средств измерений: Устройства сбора и передачи данных «МИРТ-881» № 70453-18.

Дополнительные сведения об УСПД, его характеристиках, функциональных возможностях, подготовке к работе и порядке использования, приведены в документе «УСТРОЙСТВА СБОРА И ПЕРЕДАЧИ ДАННЫХ МИРТ-881. Руководство по эксплуатации» МИРТ.411189.001РЭ, опубликованном на официальном сайте ООО «МИРТЕК» – www.mirtekgroup.com.

1.2 Требования к пользователю

Для работы с УСПД требуются навыки работы с электротехническими устройствами, персональным компьютером на уровне опытного пользователя, соответствующий допуск по электробезопасности, а также знание данного руководства.

Администратор должен обладать необходимыми знаниями в предметной области для корректной работы с предоставляемой информацией.

1.3 Сведения о программном обеспечении

1.3.1 Встроенное программное обеспечение

УСПД поставляется со встроенным (микропроцессорным) программным обеспечением «MIRTEK.5001» разработки ООО МИРТЕК. ВПО «MIRTEK.5001» имеет свидетельство о государственной регистрации программы для ЭВМ №2021681042 от 15.12.2022 г., запись в реестре № 13018 от 5.03.2022 г.

Сведения о встроенном программном обеспечении приведены в таблице 1.

Таблица 1 – Встроенное программное обеспечение

№	Наименование аппаратного обеспечения	Программное обеспечение
1	Сборка процессорная i.MX 6ULL (Myzr) модель MY-IMX6-CB140-6Y2C-512M-16G	«MIRTEK.5001» версии 2.0
2	Модуль GSM EG91 EX (Quectel)	EG91EXGAR08A05M1G

Встроенное программное обеспечение УСПД по своей структуре делится на метрологически значимую (измерительную) и незначимую части. Контрольная сумма метрологически значимой части 0xc62a остается неизменной, контрольная сумма метрологически незначимой (не измерительной) части может изменяться при обновлении ВПО.

1.3.2 Системное программное обеспечение

Системное ПО выполнено на базе операционной системы Linux (бесплатное программное обеспечение с открытым исходным кодом):

- ядро 4.9.88 (лицензия GNU GPL 2);
- корневая файловая система buildroot-2017.02.9 (лицензия GNU GPL 2).

ВПО УСПД функционирует на базе SQL-сервера PostgreSQL 9.5.10.

Системное ПО устанавливается и конфигурируется на предприятии-изготовителе и не подлежит изменению на объекте эксплуатации.

1.3.3 Прикладное программное обеспечение

Конфигурирование УСПД выполняется про помощи прикладного программного обеспечения **MeterTools** версия 4.2. **MeterTools** является собственной разработкой ООО «МИРТЕК» и имеет свидетельство о государственной регистрации программы для ЭВМ № 2014612562 от 28.02.2014 г.

1.4 Процедуры поставки программного обеспечения

ВПО УСПД, поставляется комплектно с УСПД МИРТ-881, неразрывно связано с ним, и на момент поставки имеет актуальную версию. ВПО поставляется в соответствии с заключенными договорами на поставку УСПД МИРТ-881 и имеет гарантийный срок соответствующий УСПД.

ПО **MeterTools**, необходимое для конфигурирования УСПД, распространяется бесплатно в электронном виде на сайте www.mirtekgroup.com.

Подробная информация о ПО **Meter Tools** опубликована на официальном сайте ООО «МИРТЕК» – www.mirtekgroup.com.

2 Порядок ввода УСПД в эксплуатацию

2.1 Общие сведения

Порядок ввода УСПД в эксплуатацию состоит из следующих этапов:

- приемка;
- монтаж;
- подготовка к работе;
- начало работы с УСПД;
- конфигурация УСПД.

Сведения, необходимые для приемки, монтажа и подготовке к работе УСПД приведены в документе РЭ.

2.2 Начало работы с УСПД

2.2.1 Подключение

Для выполнения конфигурирования УСПД необходимо подключить УСПД к ПК с помощью преобразователя RS-485 – USB или использовать Ethernet кабель.

Подать питание на УСПД в соответствии с требованиями РЭ.

Запустить ПО **MeterTools** и произвести подключение к УСПД, используя задействованный канал связи (RS232, RS485, Ethernet).

Порядок работы с программным обеспечением **MeterTools** для УСПД приведен в документе «УСПД МИРТ-881. Руководство пользователя», опубликованном на официальном сайте ООО «МИРТЕК» – www.mirtekgroup.com.

Для правильного подключения УСПД необходимы сведения об возможности использования интерфейсов и параметрах подключения.

2.2.1.1 Цифровые интерфейсы

Количество и характеристики интерфейсов УСПД представлены в таблице 2.

Таблица 2 – Количество и характеристики интерфейсов УСПД

Тип интерфейса	Кол-во	Скорость обмена	Подключения
RS485 МИРТ-881-D6.1 МИРТ-881-WD3	4 2	9600 бит/с	ПУ, каналообразующие устройства, ПО верхнего уровня, Конфигуратор
RS232	1	115200 бит/с	ПО верхнего уровня, Конфигуратор
Ethernet МИРТ-881-D6.1 МИРТ-881-WD3	1 2	100 Мбит/с	ПУ, ПО верхнего уровня, Конфигуратор
USB	2	Спецификация 2.0	

2.2.1.2 Параметры подключения

Параметры подключения УСПД для каналов RS232, RS485 приведены в таблице 3 и на рисунках 1, 2.

Таблица 3 – Параметры подключения УСПД для каналов RS232, RS485

Канал	RS232	RS485
Параметры канала	СОМ-порт – порт, назначенный адаптеру	
	Скорость, бод – 115200	Скорость, бод – 9600
	Биты данных – 8	
	Четность – нет	
Параметры опроса	Стоповые биты – 1	
	Ожидание ответа, мс – 5000	
	Задержка перед, мс – 0	
	Количество перезапросов – 1	
Подключение	Автоматическое	
Параметры подключения	УСПД	
	Логин – «admin» (по умолчанию)	
	Пароль – «0» (по умолчанию)	

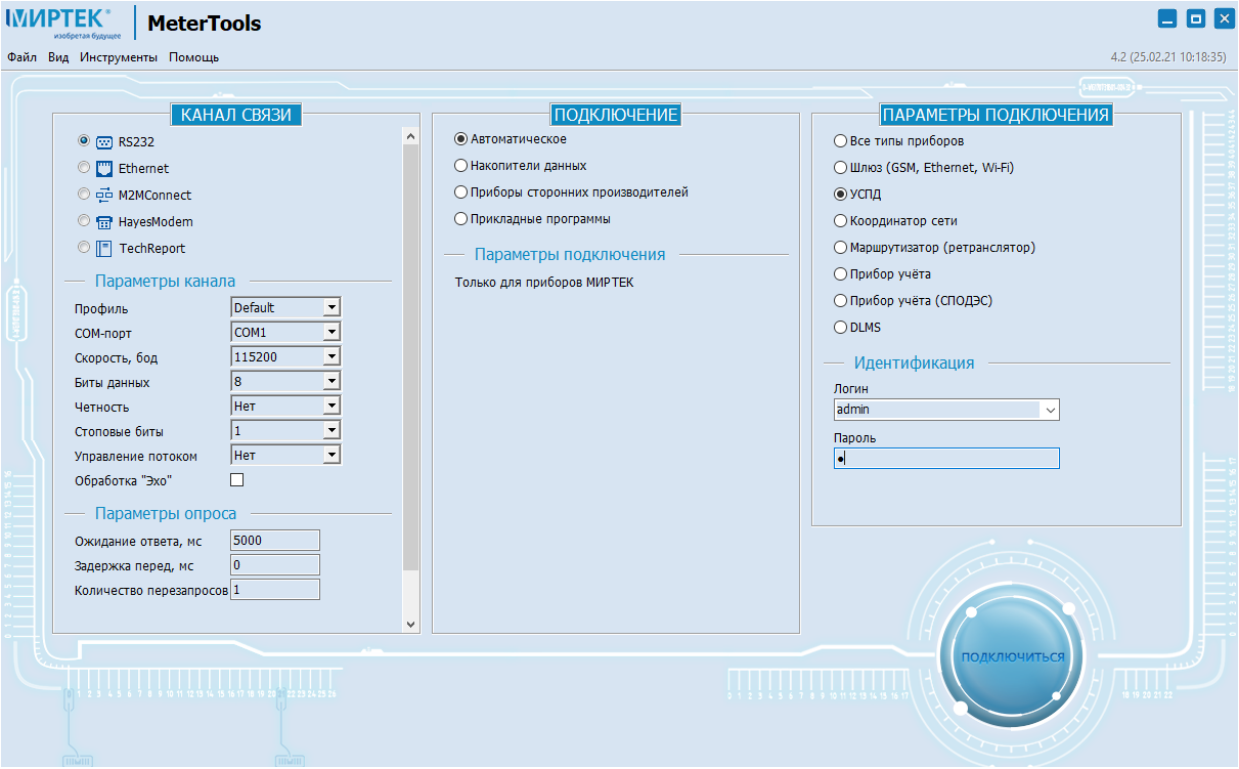


Рисунок 1 – Подключение по каналу RS232

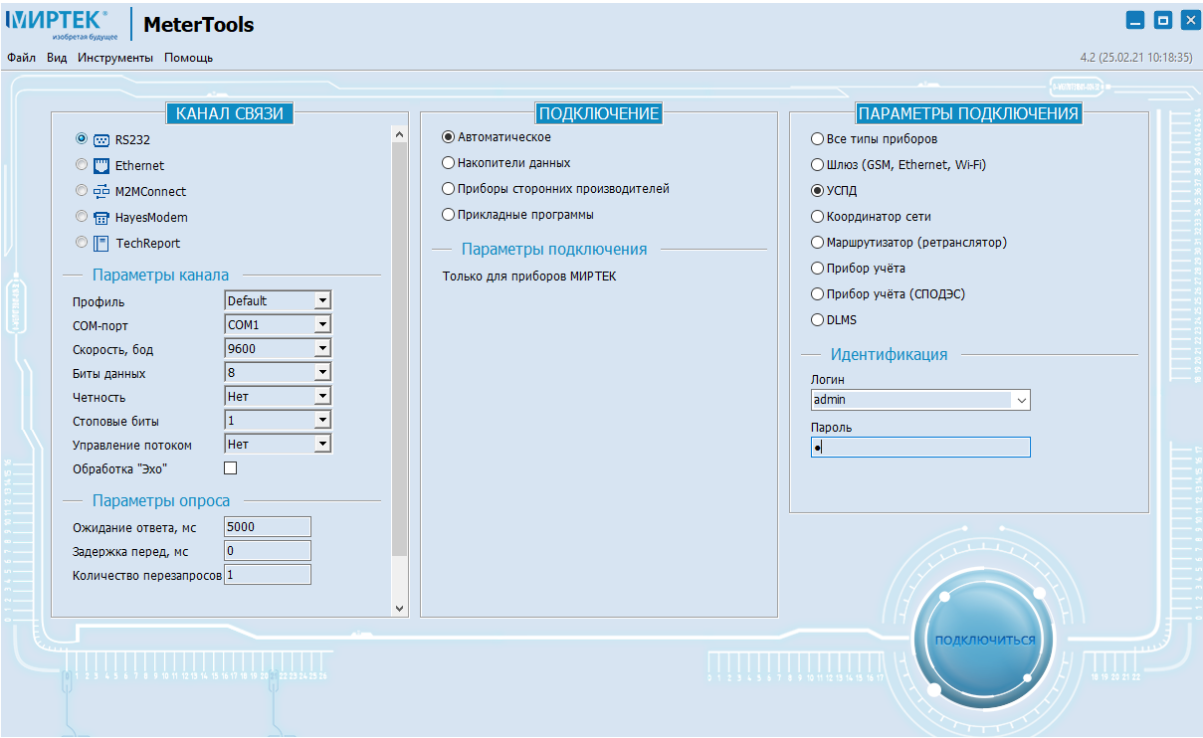


Рисунок 2 – Подключение по каналу RS485

Параметры подключения к УСПД по каналу связи Ethernet приведены в таблице 4 и на рисунке 3.

Таблица 4 – Параметры подключения УСПД для канала Ethernet

Канал	Ethernet
Параметры канала	IP-адрес – 192.168.2.59 (192.168.250.35) (по умолчанию) Порт подключения – 44445 Тип подключения – TCP

Канал	Ethernet
Параметры опроса	Ожидание ответа, мс – 5000 Задержка перед, мс – 0 Количество перезапросов – 1
Подключение	Автоматическое
Параметры подключения	УСПД Логин – «admin» (по умолчанию) Пароль – «0» (по умолчанию)

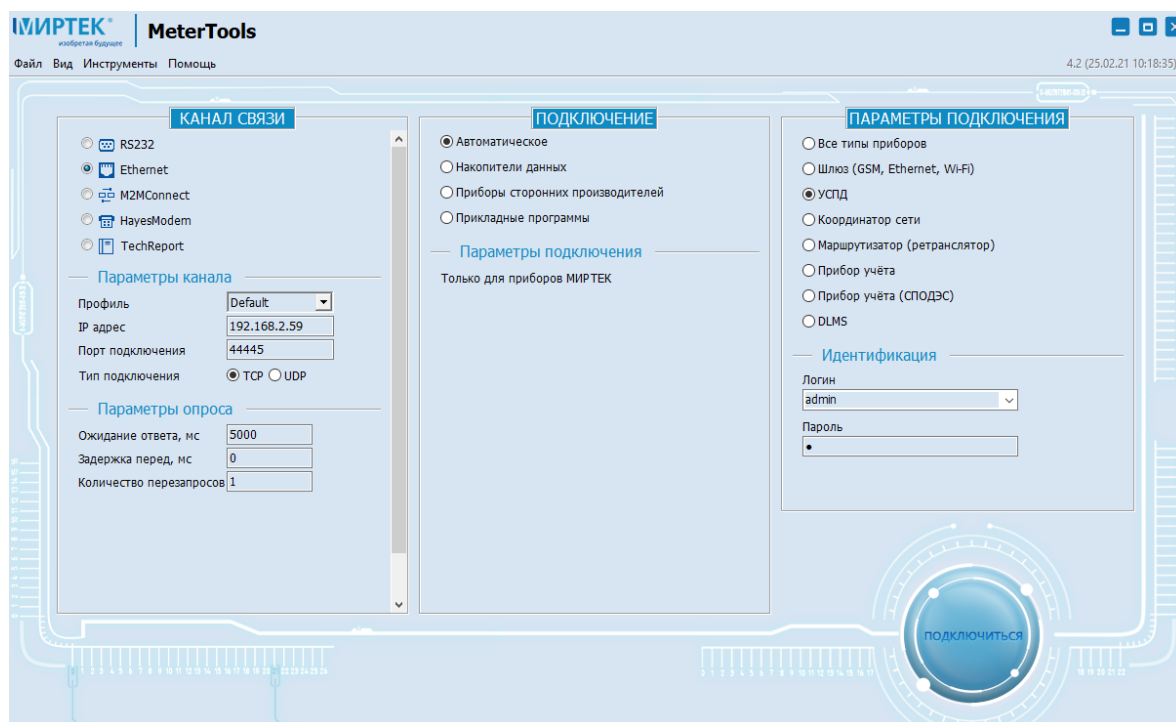


Рисунок 3 – Подключение по каналу Ethernet

2.3 Отображение информации об УСПД

После успешного подключения к УСПД выводится блок для считывания и просмотра общих сведений об устройстве, основных параметров и их значений.

Путь к данному блоку в навигационном меню: Информация → Общая



В блоке Информация → Общая надлежит проверять контрольные суммы ВПО после загрузки/обновления ВПО УСПД.



Заводские пароли УСПД после завершения настройки должны принудительно изменяться эксплуатационным персоналом. Если при подключении к УСПД был использован предустановленный пароль администратора, выводится сообщение: **Выполнена авторизация с предустановленным паролем администратора. Необходимо изменить пароль** (см. рисунок 4).

Поля:

- Заводской №.
- Дата производства.
- Завод изготовитель.
- Описание типа – модификация УСПД.

Сведения о метрологически значимой части ПО:

- Номер версии – идентификационный номер ПО.

- **Алгоритм вычисления** – алгоритм, используемый при вычислении контрольной суммы метрологически значимой части ПО.
- **Цифровой идентификатор ПО** – номер версии и контрольная сумма.

Прочие сведения:

- **Основная часть ПО** – номер версии и контрольная сумма.
- **Время прибора** – время собственных часов УСПД.
- **Время ПК** – время часов ПК.
- **Расхождение** – разбег времени между часами УСПД и ПК.
- **Время работы** – время работы УСПД после включения питания.
- **Время бездействия** – время бездействия УСПД.
- **Время работы после синхронизации** – время работы УСПД после синхронизации времени.
- **Идентификатор базы данных.**
- **Идентификатор профиля модема.**
- **Логин пользователя.**
- **Роль** – роль пользователя.
- **Статус авторизации.**

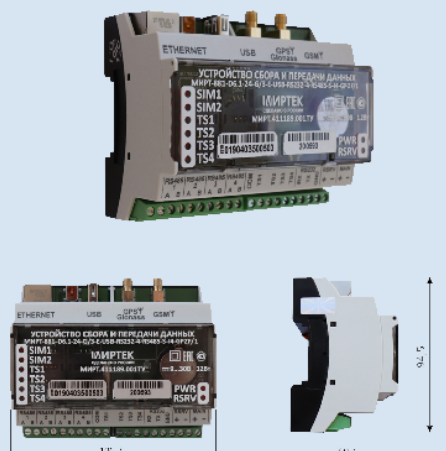
Кнопки:

- **Считать** – в зависимости от положения в интерфейсе и действий пользователя: чтение списка устройств, подключенных к УСПД (2) (см. рисунок 4), или чтение основных параметров УСПД (1).

Информация → Общая

Считать **2**

Устройство
успд



Основная часть ПО	Версия 2.0 (0x3F3F)
Время прибора	05.10.2022 17:01:11
Время ПК	05.10.2022 17:01:10
Расхождение	01 сек.
Время работы	04 ч. 16 мин. 01 сек.
Время бездействия	03 ч. 44 мин. 12 сек.
Время работы после синхронизации	Не производилась
Идентификатор базы данных	65994752
Идентификатор профиля модема	8049
Логин пользователя	admin
Роль	Администратор
Статус Авторизации	Пользователь авторизован

Заводской №	0190401900423
Дата производства	24.07.2019
Завод изготовитель	ООО "МИРТЕК", г.Таганрог
Описание типа	МИРТ-881-D6-24-G/1-E-2*USB-RS232-4
Метрологически значимая часть ПО	
Идентификационное наименование ПО	МИРТ-8806
Номер версии (ид. номер) ПО	1.0
Алгоритм вычисления	CRC
Цифровой идентификатор ПО	Версия 1.0 (0xC62A)

1 Считать **Выполнена авторизация с предустановленным паролем администратора. Необходимо изменить пароль.**

Рисунок 4 – Блок Информация – Общая

2.4 Конфигурирование и просмотр данных

Порядок работы с программным обеспечением **MeterTools** для УСПД приведен в РП. Краткое описание назначения пунктов меню приведено в таблице 5.



Пункты, выделенные жирным шрифтом, предназначены для администратора.

Таблица 5 – Назначение пунктов меню

Название пункта	Описание
Информация	
Общая	Считывание и просмотр общих сведений об устройстве, основных параметров и их значений.
Абонентская	Считывание и запись в память УСПД абонентской информации, а также просмотр заводской информации.
Статус опроса	Контроль сбора данных со счетчиков, а именно просмотр текущей информации о количестве подключенных приборов, типах, протоколах, заводских и сетевых адресах, времени успешного обращения к приборам учета и пр.
Оповещения	Просмотр информации о возникших ошибках при работе с УСПД.
Настройки	
Дата и время	Просмотр текущего времени УСПД, текущего времени подключенного ПК, изменения часового пояса, настройка синхронизации приборов учета, выполнение коррекции времени, указание сервера точного времени, установление (снятие) запрета опроса при недоступности источника точного времени.
Параметры опроса	Настройка объема и периодичности опроса приборов учета.
Таблица счетчиков	Добавление ПУ в реестр УСПД.
Дополнительно	Дополнительные настройки, в т. ч. загрузка (выгрузка) конфигурационного файла УСПД, обновление встроенного ПО и т. п.
Глубина хранения данных	Настройка глубины хранения данных, собранных с приборов учета.
Настройка каналов	Контроль состояния, а также включение (отключение) портов каналов связи.
Управление нагрузкой	Настройка считывания состояния, параметров отключения (включения) реле нагрузки, подключенного ПУ.
GSM	Настройки конфигурации APN, выбор приоритетной SIM-карты, настройки для проверки работоспособности GSM, а также считывание уровня сигнала (RSSI) и выбора активного слота SIM-карты.
Управление пользователями	Создание пользователей с назначением им определенной роли, внесение изменений в параметры пользователей, в т. ч. изменение роли и пароля пользователя. Дополнительные настройки параметров безопасности для всех пользователей.
Телемеханика	Контроль состояния дискретных входов УСПД, управление дискретными выходами (телеуправление) как самого УСПД, так и подключенных к нему внешних устройств.
Действие с конфигурацией	Сохранение и загрузка параметров конфигурации.
Сетевые настройки	Настройка и контроль состояния сетевых интерфейсов.
Координаторы	Настройка работы с координаторами МИРТ-145 (RF 433), МИРТ-554 ZigBee (RF2400) и СЭК ZigBee.

Название пункта	Описание
Конфигурация M2M	Настройка конфигурации M2M сервера.
Показания	
Мгновенные значения	Считывание и просмотр мгновенных значений измерений параметров электрической сети, зафиксированных на момент сбора данных с приборов учета.
Текущие	Считывание и просмотр текущих показаний энергии, в т. ч. с разбивкой по тарифам и типам энергии.
Месячные срезы	Считывание и просмотр показаний по месячному срезу, в т. ч. с разбивкой по тарифам.
Дневные срезы	Считывание и просмотр показаний на начало суток (суточные срезы), в т. ч. с разбивкой по тарифам.
Часовые срезы	Считывание и просмотр показаний на начало часа (часовые срезы), в т. ч. с разбивкой по тарифам.
Профили энергии	Считывание и просмотр информации о профиле энергии.
Профили мощности	Считывание и просмотр информации о профиле мощности.
Журналы	
Журналы УСПД	Считывание и просмотр журналов для контроля работы УСПД.
Журналы ПУ	Считывание и просмотр журналов, содержащих информацию о приборах учета, подключенных к УСПД. Подробнее см. п. 8.2.
Журнал безопасности	Считывание и просмотр журнала безопасности УСПД.
Тарифное расписание	
Конструктор	Создание и сохранение тарифного расписания в УСПД, а также запись расписания в устройства, подключенные к УСПД.
Действия с ПУ	
Изменение пароля	Установка основного и дополнительного паролей в память устройств, подключенных к УСПД.
Конфигурация	Настройка конфигурации месячного среза, коэффициентов трансформации и запись их в память устройств, подключенных к УСПД.
Индикация	Настройка и запись в память устройств, подключенных к УСПД, режимов индикации.
Параметры качества сети	Просмотр и установка границ контроля параметров качества сети в память устройств, подключенных к УСПД.

3 Обеспечение безопасности УСПД

3.1 Общие сведения

УСПД обеспечивает ограничение доступа к данным, изменяемым и неизменяемым параметрам конфигурации, а также передачу аутентификационной информации по сети в закрытом виде.

На конструктивном и программно-информационном уровнях в УСПД предусмотрен ряд мер защиты.

В аппаратной части доступ к разъемам, функциональным модулям и пр. ограничен системой механических и электронных пломб.

В операционную систему Linux встроен межсетевой экран iptables. С помощью межсетевого экрана выполняется защита ВПО и данных УСПД от внешних вторжений.

Все сетевые пакеты проходят проверку в настраиваемом фильтре iptables. В результате проверки выполняется действие, указанное в параметрах настройки iptables. Например, пакет передается ВПО УСПД или удаляется/отклоняется.

При настройке фильтра в цепочке Input, которая обрабатывает входящие подключения, устанавливаются правила, на соответствие которым проверяются входящие пакеты.

На программном уровне выполняется следующий комплекс мер защиты:

- установка паролей при параметрировании, а также замена заводских паролей на пароли пользователей в соответствии с требованиями политики безопасности предприятия;
- разграничение полномочий пользователей различных уровней;
- шифрование передаваемых данных в соответствии со спецификацией используемого протокола обмена;
- защита данных при подключении УСПД к публичным или закрытым сетям связи, в том числе с использованием защищенного канала VPN с шифрованием;
- исключение возможности корректировки данных по протоколу;
- дистанционное обновление встроенного ПО только по каналу, защищенному шифрованием или с помощью механизма доверенного удаленного обновления прошивки.

УСПД регистрирует следующие события безопасности в журнале событий:

- дата и время вскрытия корпуса либо шкафа учета, если УСПД установлено в шкафу;
- дата и время последнего перепрограммирования (параметрирования);
- дата и время сеанса связи со счетчиком, приведшего к изменению параметров конфигурации или режимов функционирования счетчика, в том числе управление нагрузкой;
- дата и время фиксации события аппаратного или программного сбоя;
- дата и время инициализации счетчика, последнего сброса измеряемых значений электрической энергии (мощности), число сбросов с метками времени с момента выпуска счетчика;
- дата и время попытки доступа с неуспешной аутентификацией, в том числе с нарушением правил управления доступом;
- дата и время модификации встроенного ПО.

Запись событий безопасности выполняется постоянно без возможности удаления или изменения записей журнала.

Подробнее см. пп. 8.1, 8.3.

УСПД используется преимущественно в составе систем АСКУЭ и интегрировано в следующие информационные вычислительные комплексы (ИВК):

- ПО «RadioAcces»;
- ПО «Пирамида-Сети»;
- ПО «Пирамида 2.0»;
- ПО «Альфа-Центр».

На программном уровне встроенное программное обеспечение УСПД защищено от несанкционированного и нештатного вмешательства в работу со стороны прикладного ПО:

- Взаимодействие УСПД с прикладным ПО осуществляется в соответствии с уровнем доступа пользователя, см. п. 4.1.1;

- Выполняется хэширование паролей;
- Обеспечивается возможность передачи шифрованных паролей;
- Обеспечивается возможность шифрования данных;
- Взаимодействие с прикладным ПО выполняется только по разрешенным протоколам обмена.

Таким образом гарантируется выполнение только определенного набора команд в соответствии с протоколом и запрет на выполнение команд вне уровня доступа, предоставленного для работы прикладного ПО.

3.1.1 Действия УСПД при нарушении целостности ПО

Проверка целостности ПО выполняется в процессе самодиагностики после включения/перезагрузки УСПД, а затем ежедневно.

События начала проверки целостности ПО, контрольные суммы компонентов системного ПО, завершения проверки целостности ПО сохраняются в журнале безопасности УСПД.

При обнаружении нарушения целостности ПО УСПД выполняет следующие действия:

1. Событие нарушения целостности ПО записывается в журнал безопасности.
2. Выполняется перезагрузка УСПД.
3. ВПО переходит в безопасный режим работы:
 - полностью отключается опрос ПУ и других устройств;
 - для работы по интерфейсам используется только протокол конфигуратора (mirt1);
 - в конфигураторе блокируется весь функционал за исключением просмотра заводской информации и журнала безопасности.



При нарушении целостности программного обеспечения и состава параметров УСПД ограниченно работоспособно. В данном случае восстановление УСПД должно быть выполнено на предприятии-изготовителе.

3.2 Функции безопасности УСПД

1. Обеспечивается идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору и паролю условно-постоянного действия, соответствующего требованиям сложности, при использовании прикладного (специализированного) программного обеспечения для конфигурации. При этом фиксируется событие и статус подключения (успешно/неуспешно) см. п. 4.1.
2. Обеспечивается ограничение количества неудачных попыток входа за установленный период времени. Количество неудачных попыток аутентификации – не более трех, см. п. 4.2.
3. Обеспечивается блокирование на заданный интервал времени доступа с устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неудачных попыток входа, см. п. 4.2.
4. При превышении заданного количества неудачных попыток аутентификации пользователя выполняется блокировка доступа к устройству на предустановленный период времени, см. п. 4.2.
5. При превышении заданного количества неудачных попыток аутентификации пользователя функции безопасности фиксируют событие блокировки в журнале событий безопасности, см. п. 8.3.

6. Счетчик неуспешных попыток аутентификации обнуляется после успешной аутентификации пользователя, см. п. 4.2.
7. Функции безопасности блокируют открытый сеанс (сессию) доступа по истечению заданного интервала времени с завершением сеанса (сессии) и с блокированием доступа к ресурсам устройства, см. п. 4.2.
8. Функции безопасности допускают наличие параллельных (одновременных) сеансов (сессий). Функционал обеспечивает конфигурируемую блокировку одновременного выполнения критических функций: смена ПО, смена времени, конфигурационную настройку, см. Руководство по эксплуатации п. 1.4.
9. При работе с паролями обеспечивается следующий функционал:
 - пароли не хранятся в открытом виде, см. п. 3.1;
 - заводские пароли можно изменить, см. п. 3.1;
 - исключается возможность повторного применения ранее использованных паролей (не менее 4 паролей), см. п. 4.2.
10. В УСПД реализована ролевая модель доступа, делегирующая следующие функциональные возможности только для администратора:
 - управление (назначение/изменение) паролями, см. п. 4.1.;
 - чтения событий в журнале событий безопасности, см. п. 8.3;
 - обновление системного программного обеспечения и внесения изменений в параметры конфигурационной настройки безопасности.
11. Завершение сеанса субъекта производится самим субъектом или автоматически, при превышении допустимого интервала времени бездействия авторизованного пользователя, выключении, перезагрузке устройства, см. п. 4.2.
12. Аутентификационная информация не передается по сети в открытом виде, за исключением режима соединения «Считыватель», см. п. 4.2.
13. Отдельный встроенный журнал событий безопасности УСПД размещен в отдельном выделенном сегменте энергонезависимой памяти. Обеспечивается запись событий в объеме не менее 500 записей, см. пп. 8.3, 4.2.
14. Запись событий безопасности выполняется постоянно без возможности удаления, изменения записей событий безопасности, см. п. 3.1.
15. Все записи журнала событий безопасности, см. п. 8.3.1, содержат:
 - идентификатор субъекта, который был инициатором события, либо процесса, подлежащего регистрации (в случаях, когда возможно зафиксировать роль пользователя);
 - дата и время события;
 - тип события;
 - источник события / идентификатор (серийный номер) съемного носителя информации);
 - протокол подключения;
 - порт подключения;
 - результат события / процесса: успешный, неуспешный.
16. Данные событий безопасности имеют уникальный номер. Присвоение уникальных номеров производится по сквозному принципу, см. п. 8.3.1.
17. Записи журнала событий безопасности сохраняются при любых штатных операциях с УСПД, операция сброса к заводским настройкам не предусмотрена.

18. Имеется функция цикличной перезаписи самых старых записей журнала событий новыми записями с соответствующим сбросом сквозной нумерации уникальных номеров записей, см. п. 8.3.1.
19. Данные событий безопасности в виде записей журнала событий безопасности сортируются по номерам и датам создания, см. п. 8.
20. В журнале событий безопасности, см. п. 8.3, регистрируются следующие типы событий:
 - загрузка (останов), сбой, перезагрузка программного обеспечения;
 - проверка контрольных сумм файлов программного обеспечения и конфигурации;
 - подключение к интерфейсам управления;
 - запрос на параллельный сеанс доступа к УСПД;
 - использование механизма аутентификации;
 - превышение количества неудачных попыток аутентификации;
 - обновление (модификация встроенного) программного обеспечения;
 - изменение конфигурации (параметров настройки);
 - включение и выключение портов связи;
 - вскрытие шкафа с УСПД;
 - дата и время вскрытия корпуса;
 - дата и время последнего перепрограммирования (параметрирования);
 - дата и время фиксации данных об аппаратном или программном сбое;
 - дата и время попытки несанкционированного нарушения целостности программного обеспечения и параметров;
 - дата и время сеанса связи с устройством, приведшего к изменению параметров конфигурации, режимов функционирования (в том числе введение полного и (или) частичного ограничения (возобновления) режима потребления электрической энергии (управление нагрузкой);
 - изменение текущих значений времени и даты при синхронизации времени в журнале событий времени до и после коррекции или величины коррекции времени, на которую было скорректировано значение;
 - создание, редактирование, отключение пользователей, изменение паролей и криптографических ключей;
 - использование съемных носителей информации.
21. Передача новых записей журнала событий безопасности на верхний уровень не реже 1 раза в сутки (новых событий, возникших в течение 24 часов с момента последней передачи).
22. Передача записей журнала событий безопасности ПУ в УСПД осуществляется, в том числе, по протоколу СПОДЭС. Регистрируются события, передаваемые по протоколу СПОДЭС, в том числе события безопасности. Полный перечень событий ПУ приведен в п. 3.5.2.
23. Функции безопасности включают ролевую политику безопасности, см. приложение А.
24. Правами и привилегиями по доступу к функциям безопасности наделен только администратор в соответствии с политикой безопасности УСПД, см. приложение А.
25. Для выполнения любого действия в рамках функционала назначенной роли пользователь должен быть успешно аутентифицирован, см. п. 2.2.1.
26. Доверенная загрузка обеспечивает:

- блокирование попыток несанкционированной загрузки нештатной операционной системы/встроенного программного обеспечения;
 - контроль целостности компонентов программного обеспечения устройства.
27. Обеспечивается контроль использования съемных носителей информации на интерфейсах устройства путем фиксации соответствующего события в журнале событий безопасности, см. п. 8.3.
28. Система самодиагностики непрерывно (1 раз в сутки) и при старте выполняет проверку целостности исполняемой программы и данных. Устройство блокирует выходные воздействия и формирует соответствующую сигнализацию при обнаружении системой самодиагностики нарушения целостности исполняемой программы или данных. Результаты отрицательных проверок целостности исполняемой программы или данных фиксируются в журнале событий безопасности, см. п. 8.3.
29. Разрешено восстановление конфигурации путем загрузки резервных копий конфигурации, см. п. 7.
30. Обновление ВПО по интерфейсу выполняется в прикладном ПО MeterTools, входящего в комплект поставки, см. п. 6.1.
31. После обновления ВПО УСПД роли и пароли пользователей сохраняются.
32. УСПД обеспечивает хранение аутентификационной информации (пароля и ключа), требуемой для установления соединения с ПУ (см. п. 3.5.1) с правами доступа:
- публичный клиент (самый низкий уровень доступа);
 - считывание данных (возможна аутентификация и шифрование данных, изменение настроек и данных невозможно, кроме операции «сдвиг времени»);
 - конфигурирование счетчика (полный доступ к настройкам, чтение данных).
33. УСПД обеспечивает изменение в ПУ аутентификационной информации (пароля и ключа) по протоколу СПОДЭС в режиме «Конфигуратор» (см. п. 3.5.1).
34. В УСПД допускается применение одной и той же аутентификационной информации (пароля и ключа) для установления соединения с ПУ.
35. Обеспечение защиты данных от несанкционированного доступа как при подключении УСПД к публичным сетям, так и закрытым сетям связи, в том числе с использованием защищенного канала VPN с шифрованием (см. п. 6.1).
36. Корректировка данных по протоколу передачи данных невозможна: в протоколе не предусмотрены команды для изменения собранных данных, показаний, событий.
37. УСПД обеспечивает защиту от атак типа отказ в доступе (DDoS).
38. Дистанционное обновление ВПО вне защищенного канала с шифрованием невозможно (см. п. 6.1).
39. События вскрытия шкафа инициативно передаются через УСПД в ИВК и ОИК ЦУС, см. п. 4.2.
40. Организация сквозного канала связи обеспечивается только после успешной авторизации с устройством, доступ к которому обеспечивается по «прозрачному каналу».
41. УСПД принимает команды от внешнего модуля телеуправления при условии успешной авторизации с типом соединения «конфигуратор».
42. Реализован спорадический режим передачи инициативных сообщений.

43. Поддержка защищенных протоколов передачи данных (https и др.) для встроеного Web-сервера.
44. Заводской (серийный) номер УСПД не перепрограммируется и доступен для считывания по интерфейсам.
45. Количество ПУ с функцией полного или частичного ограничения режим потребления не должно превышать 750 ПУ, см. п. 4.2.
46. Заводские пароли УСПД после завершения настройки принудительно изменяются эксплуатационным персоналом (см. п. 2.3).

3.3 Процедуры идентификации и аутентификации

Целью идентификации и аутентификации при доступе пользователя к УСПД является опознание пользователя и необходимая уверенность, что это именно тот пользователь, за которого он себя выдает.

Процедуры идентификация и аутентификация включают:

1. Подготовка, формирование и регистрация информации о пользователе, присвоение ему идентификатора доступа и регистрация в перечне пользователей с присвоенным идентификатором.
2. Хранение и поддержание актуального состояния идентификационной и аутентификационной информации.
3. Идентификацию пользователя, запросившего доступ к УСПД перед сессией работы с УСПД.
4. Аутентификацию пользователя, включающую проверку его подлинности и принадлежности ему предъявленного идентификатора и аутентификационной информации.

Идентификации и аутентификации пользователя осуществляется только в рамках УСПД, в котором хранится информации о данном пользователе.

Идентификации и аутентификации пользователя при доступе к УСПД осуществляется в рамках одного процесса.

Для идентификации и аутентификации пользователя для доступа к УСПД может использоваться прикладное ПО, например **MeterTools** версия 4.2.

При процедуре идентификации и аутентификации используются дополнительные меры защиты: контроль попыток авторизации, требования к сложности паролей.

При доступе к УСПД пользователь выполняет запрос доступа и предоставляет идентификационную и аутентификационную информацию.

В прикладном ПО выполняется присвоение пользователю идентификатора доступа и аутентификационной информации, а также фиксируется связь идентификатора и аутентификационной информации с конкретным пользователем.

ВПО УСПД опознает пользователя и проверяет принадлежность пользователю идентификатора доступа и аутентификационной информации, введенных в прикладном ПО.

Пользователи, ПО и ВПО должны обеспечивать безопасность используемой идентификационной и аутентификационной информации.

3.4 Мероприятия по обеспечению безопасности

Одной из основных задач администратора УСПД является обеспечение безопасности устройства.

Защита УСПД, включая встроенное программное обеспечение УСПД, выполняется с использованием следующих организационных и технических мер:

- осуществление ввода УСПД в эксплуатацию и эксплуатация УСПД в соответствии с требованиями эксплуатационной документации;
- обеспечение физической сохранности УСПД, исключение возможности доступа к ним посторонних лиц;
- разрешение прохождения входящих пакетов только по портам, используемым УСПД;
- контроль правильной настройки и эксплуатации УСПД администратором;
- изменения заводского пароля администратора при вводе УСПД в эксплуатацию;
- запрет внесения изменений в критические настройки УСПД без согласования с администратором;
- предотвращение несанкционированного доступа к логинам и паролям администраторов и пользователей в рамках принятых регламентов;
- выдача логина и пароля с уровнем доступа «Оператор» для доступа из стороннего прикладного ПО;
- сверка контрольной суммы метрологически значимой части ВПО, которая выводится в ПО **MeterTools** (меню Информация), с контрольной суммой, приведенной в формуляре для проверки целостности метрологически значимой части ВПО;
- анализ трафика на предмет угроз при подключении к внешним информационным системам;
- анализ журналов регистрации событий безопасности;
- проведение расследования, анализ и ликвидация негативных последствий при выявлении критических событий безопасности;
- своевременная установка актуальных обновлений ВПО и конфигурационного ПО.



При возникновении аварийной ситуации, вызванной несанкционированным вмешательством в работу УСПД, ошибками в эксплуатации УСПД и пр. следует остановить работу УСПД, выполнить анализ возникновения ошибки, предпринять действия по ее устранению. При необходимости, передать информацию об ошибке разработчикам и/или системным администраторам.

3.5 Работа с ПУ по протоколу СПОДЭС

3.5.1 Основные положения в части безопасности

Подробное описание работы с ПУ в части безопасности приведено в документе «ПРИБОРЫ УЧЕТА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ Требования к информационной модели обмена данными (версия 3)» СТО 34.01-5.1-006-2021 от 01.07.2022.

В настоящем разделе приведены основные требования к обмену с ПУ в части безопасности.

Особенностью протокола СПОДЭС является трехстадийный процесс обмена:

1. Создание информационной модели сервера. В качестве сервера выступает ПУ. Каждому типу ПУ соответствует своя информационная модель. Информационная модель определяет набор измеряемых величин, формат, единицы измерения и

размерность измеряемых величин. Информационная модель может быть считана с одного из ПУ данного типа и использоваться затем для всех ПУ данного типа.

2. Установление соединения между клиентом и сервером. В качестве клиента выступает УСПД (хост). Инициатором соединения выступает клиент. Сервер должен поддерживать 4 типа соединений, отличающихся правами доступа к объектам:

- Публичный клиент – минимальный доступ на чтение, запись и выполнение методов запрещены;
- Считыватель показаний – доступ для всех объектов на чтение разрешён, разрешена запись только пароля низкого уровня, разрешен метод для коррекции времени на ± 900 секунд для объекта «Часы»;
- Конфигуратор – полный доступ ко всем объектам;
- Инициативный – выдача PUSH сообщений.

3. Обмен данными между клиентом и сервером. Обмен данными может осуществляться по различным коммуникационным каналам в зашифрованном, либо незашифрованном виде.

Сведения о защите информации и сервисам прикладного уровня для различных типов соединений приведены в таблице 6.

Таблица 6 – Типы соединений с ПУ

Параметр	Публичный клиент	Считыватель показаний	Конфигуратор	Инициативный
Защита информации	Не применяется	Аутентификация	Аутентификация и/или шифрование	Не применяется
Сервисы прикладного уровня	Чтение Чтение блоком	Чтение Чтение блоком Селективная выборка Выполнить действие	Чтение Чтение блоком Селективная выборка Выполнить действие Запись Запись блоком	Уведомление о данных
Уровень преобразования	Самый низкий	Низкий	Высокий	Самый низкий

Выполнение действия осуществляется типами соединений ПУ в соответствии установленным уровнем преобразования. Так, для типа «Считыватель показаний» не осуществляются действия по управлению реле отключения нагрузки, смене тарифного расписания.

Уровни преобразования:

Самый низкий уровень – доступ к ПУ осуществляется без процедуры аутентификации доступа. Самый низкий уровень безопасности используется для соединения типа «Публичный клиент».

Низкий уровень – доступ к ПУ осуществляется через процедуру аутентификации доступа, основанную на явной передаче пароля. Соединение с ПУ устанавливается только в случае верного пароля. Низкий уровень безопасности используется для соединения типа «Считыватель показаний». Использование низкого уровня безопасности связано с риском перехвата пароля и выполнения несанкционированных операции с ПУ. Поэтому, данный уровень безопасности рекомендуется использовать только для чтения данных.

Высокий уровень безопасности – доступ к прибору учета осуществляется через процедуру аутентификации доступа, основанную на алгоритме, при котором пароль не передается. Перехватить пароль не представляется возможным. Поэтому данный уровень безопасности должен использоваться для соединения типа «Конфигуратор», где разрешены операции записи.

В механизме аутентификации **высокий уровень безопасности** используется несколько ключей: Одноадресный ключ шифрование длиной 16 байт; Ключ аутентификации длиной 16 байт; Мастер ключ длиной 16 байт, МК.

В список обязательных сервисов, поддерживаемых клиентом и приложением, входят следующие сервисы:

- Запрос на установление соединения
- Ответ на запрос установления соединения
- Запрос данных
- Установка данных
- Запрос события
- Команда выполнения
- Ответ на запрос данных
- Ответ на команду установки
- Ответ на команду выполнения
- Запрос данных с шифрованием
- Установка данных с шифрованием
- Запрос события с шифрованием
- Команда выполнения с шифрованием
- Ответ на запрос данных с шифрованием
- Ответ на команду установки с шифрованием
- Ответ на команду выполнения с шифрованием



Подключение к ПУ в режиме конфигурирования без шифрования запрещено.

3.5.2 События ПУ, принимаемые УСПД

УСПД принимает, регистрирует и обеспечивает хранение и передачу на верхний уровень следующих событий ПУ:

0.0.99.98.0.255 – События, связанные с напряжением

1. Фаза А – пропадание напряжения
2. Фаза А – восстановление напряжения
3. Фаза В – пропадание напряжения
4. Фаза В – восстановление напряжения
5. Фаза С – пропадание напряжения
6. Фаза С – восстановление напряжения
7. Превышение коэффициента несимметрии последовательности – начало
8. Превышение коэффициента несимметрии последовательности – окончание
9. Фаза А – перенапряжение начало ДопИнфо: sec, min, hour, day, mon, year наступления события
10. Фаза А – перенапряжение окончание ДопИнфо[4] == 0x01
11. Фаза В – перенапряжение начало ДопИнфо: sec, min, hour, day, mon, year наступления события

12. Фаза В – перенапряжение окончание ДопИнфо[4] == 0x02
13. Фаза С – перенапряжение начало ДопИнфо: sec, min, hour, day, mon, year наступления события
14. Фаза С – перенапряжение окончание ДопИнфо[4] == 0x03
15. Фаза А – провал начало ДопИнфо: sec, min, hour, day, mon, year наступления события
16. Фаза А – провал окончание ДопИнфо[4] == 0x01
17. Фаза В – провал начало ДопИнфо: sec, min, hour, day, mon, year наступления события
18. Фаза В – провал окончание ДопИнфо[4] == 0x02
19. Фаза С – провал начало ДопИнфо: sec, min, hour, day, mon, year наступления события
20. Фаза С – провал окончание ДопИнфо[4] == 0x03
21. Неправильная последовательность фаз начало
22. Неправильная последовательность фаз окончание

0.0.99.98.1.255 События, связанные с током

1. Фаза А – экспорт начало ДопИнфо[0] == 0x01
2. Фаза А – экспорт окончание ДопИнфо[0] == 0x01
3. Фаза В – экспорт начало ДопИнфо[0] == 0x02
4. Фаза В – экспорт окончание ДопИнфо[0] == 0x02
5. Фаза С – экспорт начало ДопИнфо[0] == 0x03
6. Фаза С – экспорт окончание ДопИнфо[0] == 0x03
7. Фаза А – наличие тока при отсутствии напряжения начало
8. Фаза В – наличие тока при отсутствии напряжения начало
9. Фаза С – наличие тока при отсутствии напряжения начало
10. Фаза А – превышение максимального тока начало ДопИнфо: sec, min, hour, day, mon, year наступления события
11. Фаза А – превышение максимального тока окончание ДопИнфо[4] == 0x01
12. Фаза В – превышение максимального тока начало ДопИнфо: sec, min, hour, day, mon, year наступления события
13. Фаза В – превышение максимального тока окончание ДопИнфо[4] == 0x02
14. Фаза С – превышение максимального тока начало ДопИнфо: sec, min, hour, day, mon, year наступления события
15. Фаза С – превышение максимального тока окончание ДопИнфо[4] == 0x03

0.0.99.98.2.255 События, связанные с вкл.\выкл. счетчика, коммутации реле нагрузки

1. Выключение питания
2. Включение питания
3. Выключение абонента дистанционное
4. Включение абонента дистанционное
5. Получение разрешения на включение абоненту
6. Включение реле нагрузки абонентом
7. Выключение локальное по превышению лимита мощности
8. Выключение локальное по превышению напряжения

0.0.99.98.3.255 События программирования параметров счетчика

1. Установка времени

2. Изменение параметров перехода на летнее время
3. Изменение даты активации ТР
4. Активация ТР
5. Изменение расчетного дня/часа (РДЧ)
6. Изменение коэффициента трансформации по току
7. Изменение коэффициента трансформации по напряжению
8. Изменение периода захвата профиля 1
9. Коррекция времени

0.0.99.98.4.255 События внешних воздействий

1. Магнитное поле – начало
2. Магнитное поле – окончание
3. Срабатывание электронной пломбы крышки клеммников
4. Срабатывание электронной пломбы корпуса

0.0.99.98.6.255 События контроля доступа

1. Попытка несанкционированного доступа (интерфейс)

0.0.99.98.7.255 Журнал самодиагностики

1. Часы реального времени — ошибка
2. Блок памяти — ошибка

0.0.99.98.8.255 Превышение реактивной мощности (тангенса сети)

1. Превышение установленного порога – начало
2. Превышение установленного порога – окончание

4 Управление пользователями

Настройки → Управление пользователями

Форма **Управление пользователями** содержит вкладки **Управление пользователями** и **Расширенные настройки безопасности**.

УСПД обеспечивает возможность установки следующих типов уровня доступа:

- **Администратор** – данный уровень доступа позволяет осуществлять чтение собранных данных, чтение и запись всех параметров УСПД, в т. ч. редактирование параметров пользователей, чтение и редактирование настроек безопасности, чтение журнала безопасности.
- **Оператор** – данный уровень доступа позволяет осуществлять чтение собранных данных, чтение и запись всех параметров УСПД, кроме редактирования параметров пользователей.
- **Гость** – данный уровень доступа позволяет осуществлять чтение собранных данных, чтение всех параметров УСПД, кроме параметров пользователей.



Вся информация о зарегистрированных пользователях, включая имена, роли и пароли сохраняется после обновления ПО.

4.1 Вкладка **Управление пользователями**

Настройки → Управление пользователями → Управление пользователями

Вкладка **Управление пользователями** предназначена для считывания списка пользователей, добавления новых пользователей с указанием для каждого пользователя уровня доступа к данным, редактирование пользователя.



По умолчанию в УСПД внесен пользователь, имеющий логин «admin», пароль «0», уровнем доступа **Администратор**.



Удаление пользователя невозможно. Для запрета на подключение к УСПД установите пользователю уровень доступа «Отключен», см. п. 4.1.4.

Поля вкладки:

- **Логин** – имя пользователя;
- **Пароль** – пароль пользователя;
- **Описание** – комментарий;
- **Роль** – уровень доступа, запрет на подключение пользователя.

Кнопки:

- **Сохранить** – сохранение нового пользователя.
- **Считать** – считывание списка пользователей из УСПД.
- **Отмена** – отмена процесса считывания.
- **Записать** – запись в память УСПД данных пользователя, выбранного в списке.

4.1.1 Добавление пользователя

Для добавления нового пользователя:

3. Заполните поля в соответствии с описанием (1) (см. рисунок 5).
4. Нажмите кнопку **Сохранить** (2).

№	Логин	Роль	Пароль	Описание

Рисунок 5 – Добавление пользователя

4.1.2 Считывание списка пользователей

Для считывания списка пользователей:

1. Нажмите кнопку **Считать**.

Для остановки считывания:

1. Нажмите кнопку **Отмена**.

4.1.3 Редактирование пользователя

Для изменения уровня доступа, пароля и/или описания пользователя:

1. Считайте список пользователей, см. п. 4.1.2.
2. Выберите целевое поле в строке пользователя.
3. Отредактируйте значение поля в соответствии с описанием.
4. Нажмите кнопку **Записать** в строке пользователя (1) (см. рисунок 6).

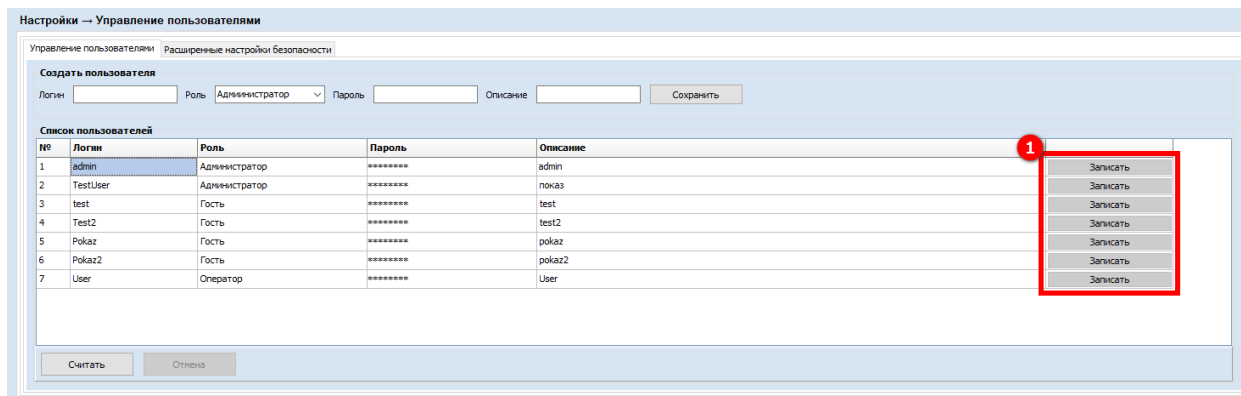


Рисунок 6 – Запись пользователя в память УСПД

4.1.4 Запрещение подключения к УСПД

Для запрещения подключения пользователя к УСПД:

1. Считайте список пользователей, см. п. 4.1.2.
2. Выберите поле **Роль** в строке пользователя.
3. Установите значение поля «Отключен» (см. рисунок 7).
4. Нажмите кнопку **Записать** (1) в строке пользователя (см. рисунок 6).

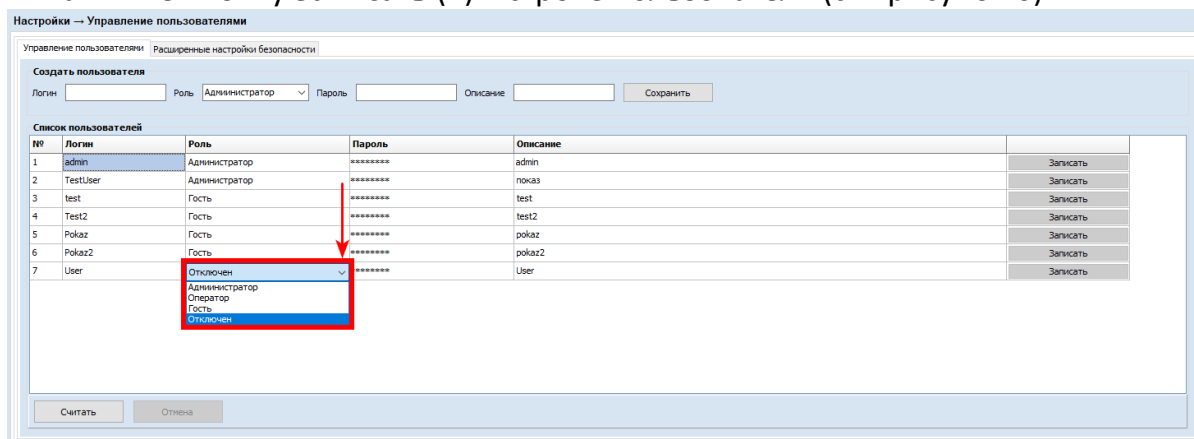


Рисунок 7 – Запрет на подключение к УСПД

4.2 Вкладка *Расширенные настройки безопасности*

Настройки → Управление пользователями → Расширенные настройки безопасности

На вкладке **Расширенные настройки безопасности** указываются дополнительные настройки параметров безопасности для всех пользователей. Например, параметры контроля авторизации, требования к паролям. А также выполняется контроль записи журнала безопасности. Подробнее о журнале безопасности см. п. 8.3.



Для работы с настройками безопасности считайте значение поля **Включить расширенные настройки безопасности**, установите флаг в поле, если он не установлен, нажмите кнопку **Записать**.

Настройки → Управление пользователями

Управление пользователями | Расширенные настройки безопасности

1 ☒ Включить расширенные настройки безопасности

Подключение

☐ Разрешить только подключение с шифрованием

☐ Запретить прямой доступ к портам без авторизации

Журнал безопасности

☐ Вести отдельный журнал безопасности

Глубина хранения журнала, записей

Контроль авторизации

☐ Включить контроль авторизации

Количество попыток

Задержка между попытками, сек

Задержка после превышения количества попыток, сек

Период неактивности пользователя до автоматического отключения, сек

Поведение при параллельном запросе авторизации

Требования к паролям

☐ Включить контроль паролей

☐ Запрет повторного использования пароля

Количество хранимых паролей

Минимальная длина пароля

Рисунок 8 – Расширенные настройки безопасности

Кнопки:

- **Считать** – считывание информации в выбранном блоке формы.
- **Записать** – запись информации в выбранном блоке формы.

Поля формы:

- **Включить расширенные настройки безопасности** – если флаг в поле установлен, применяются расширенные настройки безопасности (см. рисунок 8).

Блок **Подключение**:

- **Разрешить только подключение с шифрованием** – если флаг в поле установлен, подключение выполняется только по каналу с шифрованием.
- **Запретить прямой доступ к портам без авторизации** – если флаг в поле установлен, доступ к портам УСПД возможен только после авторизации пользователя.

Подключение

☐ Разрешить только подключение с шифрованием

☒ Запретить прямой доступ к портам без авторизации

Рисунок 9 – Блок Подключение

Блок **Журнал безопасности**:

- **Вести отдельный журнал безопасности** – если флаг в поле установлен, ведется запись событий в журнал безопасности (см. рисунок 10).
- **Глубина хранения журнала, записей** – максимальное количество записей в журнале безопасности.

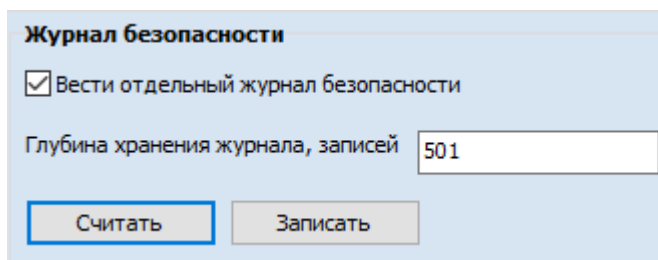


Рисунок 10 – Блок Журнал безопасности

Блок Контроль авторизации:

- **Включить контроль авторизации** – если флаг в поле установлен, можно ввести дополнительные параметры авторизации (см. рисунок 11).
- **Количество попыток** – максимальное количество попыток авторизации. Усложняет автоматический подбор пароля. После успешной аутентификации пользователя счетчик количества попыток обнуляется.
- **Задержка между попытками, сек** – время между неуспешными попытками авторизации. Указывается в секундах.
- **Задержка после превышения количества попыток, сек** – время, после которого можно повторить попытку авторизации (после превышения допустимого количества попыток авторизации). Указывается в секундах.
- **Период неактивности пользователя до автоматического отключения, сек** – время, через которое произойдет автоматическое закрытие сессии пользователя при его неактивности. Указывается в секундах.

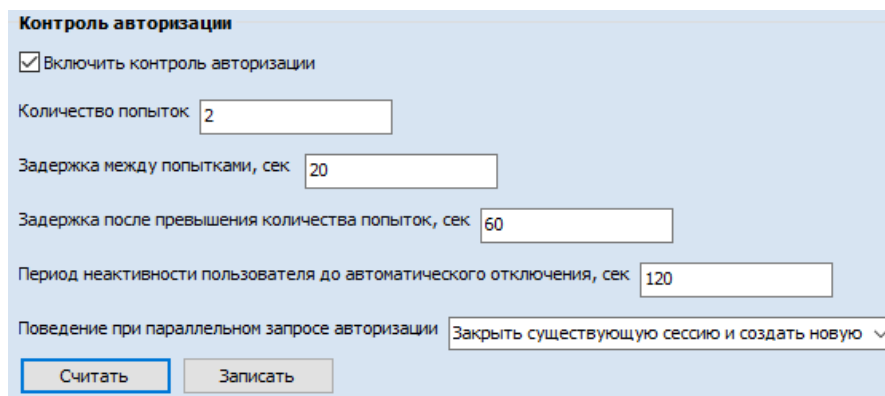


Рисунок 11 – Блок Контроль авторизации

Блок Требования к паролям:

- **Включить контроль паролей** – если флаг в поле установлен, будут проверяться ограничения при установке или изменении пароля (см. рисунок 12).
- **Запрет повторного использования пароля** – если флаг в поле установлен, повторное использование пароля запрещено.
- **Количество хранимых паролей** – максимальное количество хранимых паролей.
- **Минимальная длина пароля** – минимальное количество символов в пароле.

- **Сложность пароля** – если флаги в полях предлагаемых символов установлены, выполняется проверка соответствия символов пароля выбранным требованиям.

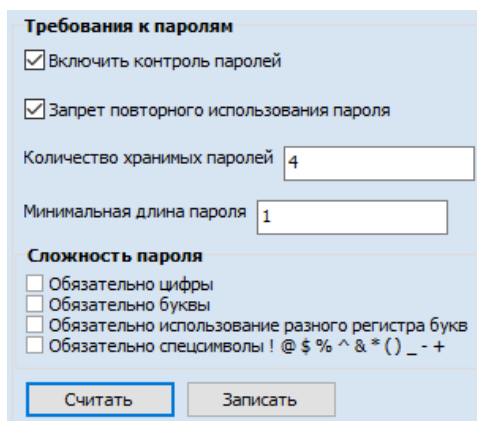


Рисунок 12 – Блок Требования к паролям

Блок **Мониторинг вскрытия шкафа УСПД**:

- **Мониторинг вскрытия шкафа УСПД** – если флаг в поле установлен, будут проверяться ограничения при установке или изменении пароля (см. рисунок 12).
- **Выбор порта телесигнализации** – выберите порт телесигнализации в выпадающем списке. Для выбора порта необходимо ознакомиться с проектным заданием на монтаж УСПД.

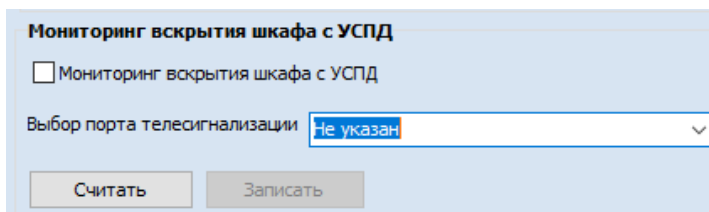


Рисунок 13 – Блок Мониторинг вскрытия шкафа УСПД

4.2.1 Чтение параметров безопасности

Для чтения параметров настроек безопасности:

1. Нажмите кнопку **Считать** в целевом блоке.

4.2.2 Добавление параметров безопасности

Для добавления параметров настроек безопасности:

1. Установите флаг в первом поле целевого блока.
2. Отредактируйте поля блока в соответствии с описанием.
3. Нажмите кнопку **Записать** в целевом блоке.

5 Сетевые настройки

Настройки → Сетевые настройки

Форма содержит вкладки **Настройки сетевых интерфейсов**, **Состояния сетевых интерфейсов**, **Общие настройки**, которые предназначены для просмотра, настройки и контроля состояния сетевых интерфейсов.

5.1 Настройка сетевых интерфейсов

Настройки → Сетевые настройки → Настройка сетевых интерфейсов

Форма **Настройка сетевых интерфейсов** предназначена для ввода параметров настройки сетевых интерфейсов.

Следующие поля блока могут быть изменены только для администратором:



- **Разрешить доступ суперпользователя по SSH**
- **Разрешить обновление с USB-устройства**
- **Разрешить загрузку файлов только при подключении с шифрованием**

Поля:

- Поле выбора порта Ethernet;
- **Флаг DHCP** – если флаг в поле установлен, используются динамические IP-адреса;
- **Маршруты DHCP** – если флаг в поле установлен, используются динамические маршруты;
- **Использовать DNS адреса** – если флаг в поле установлен, можно использовать систему доменных имен в адресах.

Кнопки:

- **Обновить** – отображение текущего списка интерфейсов выбранного Ethernet порта УСПД, включая дополнительные сетевые адаптеры;
- **Считать** – считывание текущей сетевой конфигурации УСПД;
- **Добавить IP** – добавление нового IP-адреса;
- **Удалить IP** – удаление выбранного IP-адреса;
- **Записать** – запись параметров в память УСПД;
- **Применить** – применение записанных в память параметров без перезагрузки контроллера;
- **Отмена** – отмена процесса записи;
- **Добавить маршрут** – добавление нового маршрута;
- **Удалить маршрут** – удаление выбранного маршрута.

Запись IP адреса выполняется в виде: «192.168.2.59/24». Данный вид записи заменяет собой указание диапазона IP-адресов. Число после косой черты означает количество единичных разрядов в маске подсети. 24 в десятичном виде соответствует маске подсети: «255.255.255.0». Диапазон адресов хостов от 192.168.2.1 до 192.168.2.254, а также 192.168.2.0 – адрес сети и 192.168.2.255 – широковещательный адрес сети.



5.1.1 Чтение списка интерфейсов и сетевой конфигурации

Для чтения настроек порта Ethernet:

1. Выберите целевой Ethernet порт в выпадающем списке: eth0 – основной порт, eth1 – резервный порт.
2. Нажмите кнопку **Обновить** (1) (см. рисунок 14).

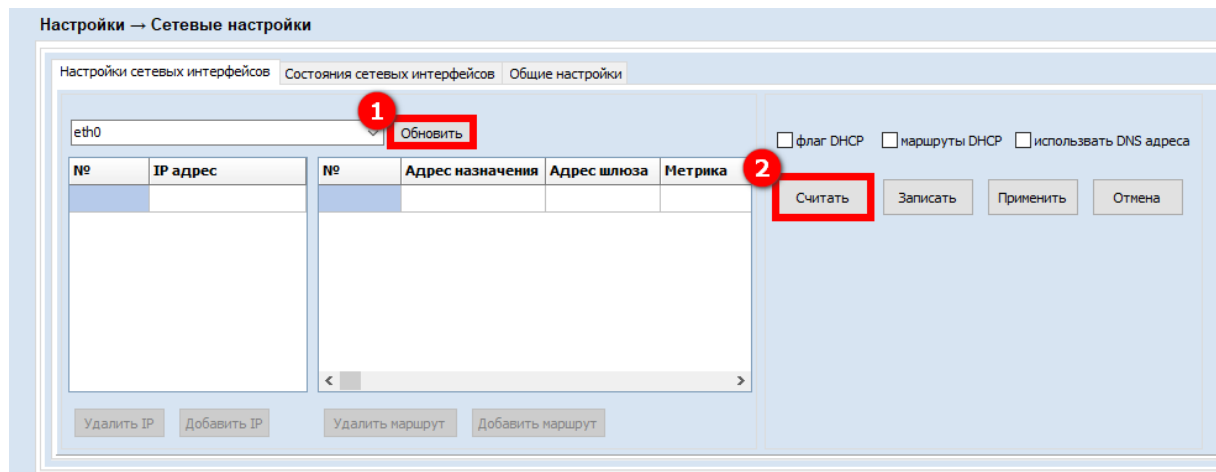


Рисунок 14 – Чтение сетевых параметров

3. Нажмите кнопку **Считать** (2).

5.1.2 Добавление IP-адреса

Для добавления IP-адреса:

1. Считайте список сетевых интерфейсов в соответствии с п. 5.1.1.
2. Нажмите кнопку **Добавить IP** (1) (см. рисунок 15).
3. Выберите ячейку в новой строке столбца IP-адрес.
4. Введите новый IP-адрес (2), например 192.168.2.99/24.
5. Нажмите кнопку **Записать** (3).
6. Нажмите кнопку **Применить** (4).

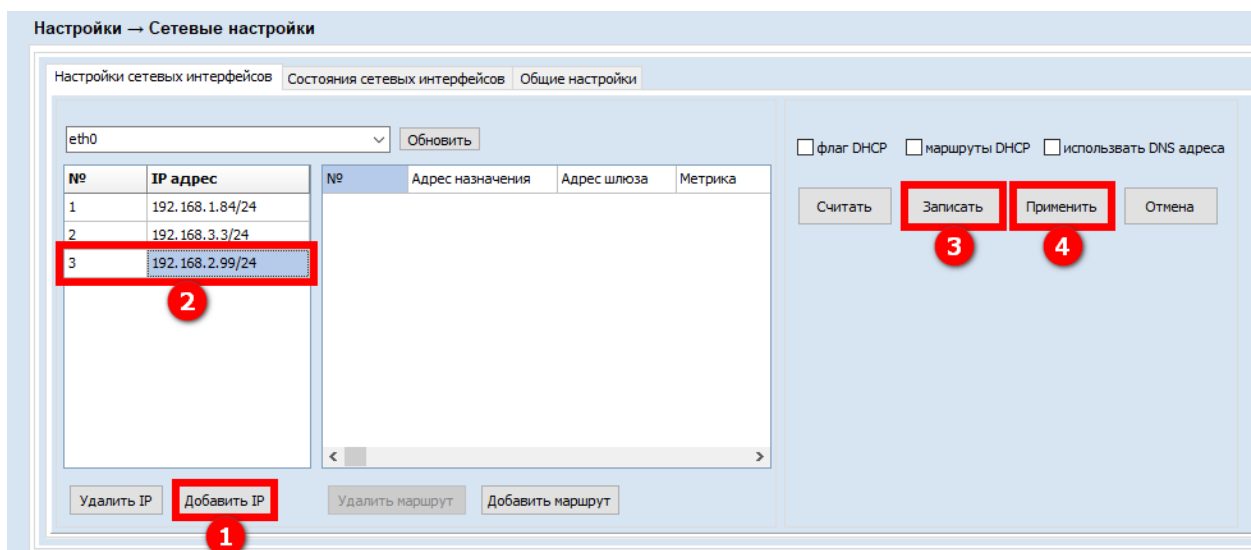


Рисунок 15 – Добавление IP-адреса

5.1.3 Изменение IP-адреса

Для изменения IP-адреса:

1. Считайте список сетевых интерфейсов в соответствии с п. 5.1.1.
2. Выберите ячейку IP-адреса, подлежащего изменению.
3. Введите новый IP-адрес (1), например 192.168.3.3/24 (см. рисунок 16).
4. Нажмите кнопку **Записать** (2).
5. Нажмите кнопку **Применить** (3).

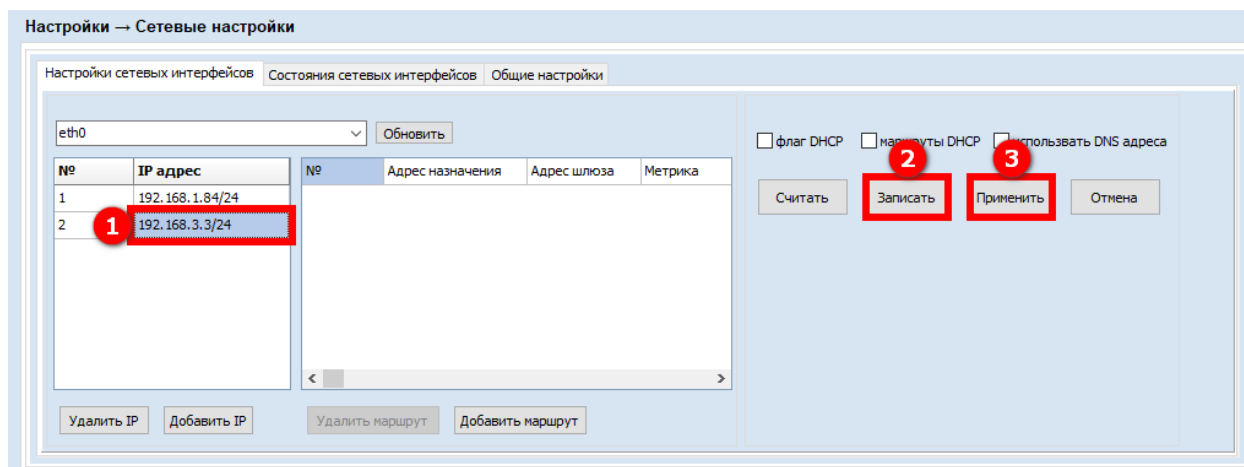


Рисунок 16 – Изменение IP-адреса

5.1.4 Удаление IP-адреса

Для удаления IP-адреса:

1. Считайте список сетевых интерфейсов в соответствии с п. 5.1.1.
2. Выберите ячейку IP-адреса, подлежащего удалению (1) (см. рисунок 17).
3. Нажмите кнопку **Удалить IP** (2).
4. Нажмите кнопку **Записать** (3).
5. Нажмите кнопку **Применить** (4).

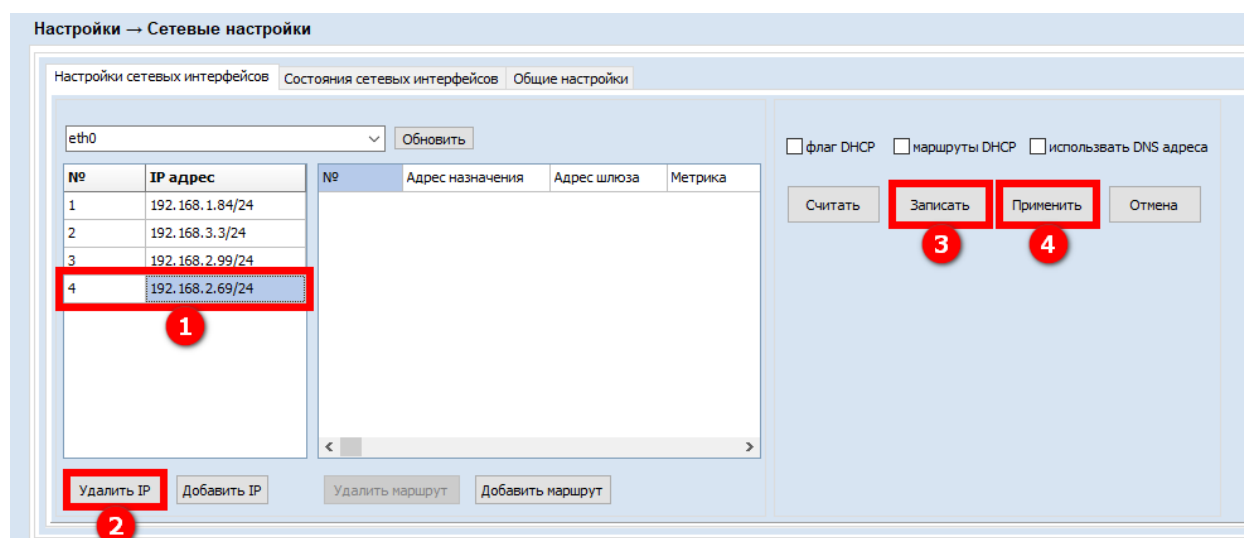


Рисунок 17 – Удаление IP-адреса

5.1.5 Добавление маршрута

Для добавления маршрута:

1. Считайте список сетевых интерфейсов в соответствии с п. 5.1.1.
2. Нажмите кнопку **Добавить Маршрут** (1) (см. рисунок 18).
3. Выберите ячейку в новой строке столбца **Адрес назначения**. Введите адрес назначения, например 10.1.0.0/16 (2).
4. Выберите ячейку столбца **Адрес шлюза**. Введите адрес шлюза.
5. Выберите ячейку столбца **Метрика**. Введите значение метрики. Метрика – это значение, назначенное маршруту IP для определенного сетевого интерфейса.
6. Нажмите кнопку **Записать** (3).
7. Нажмите кнопку **Применить** (4).

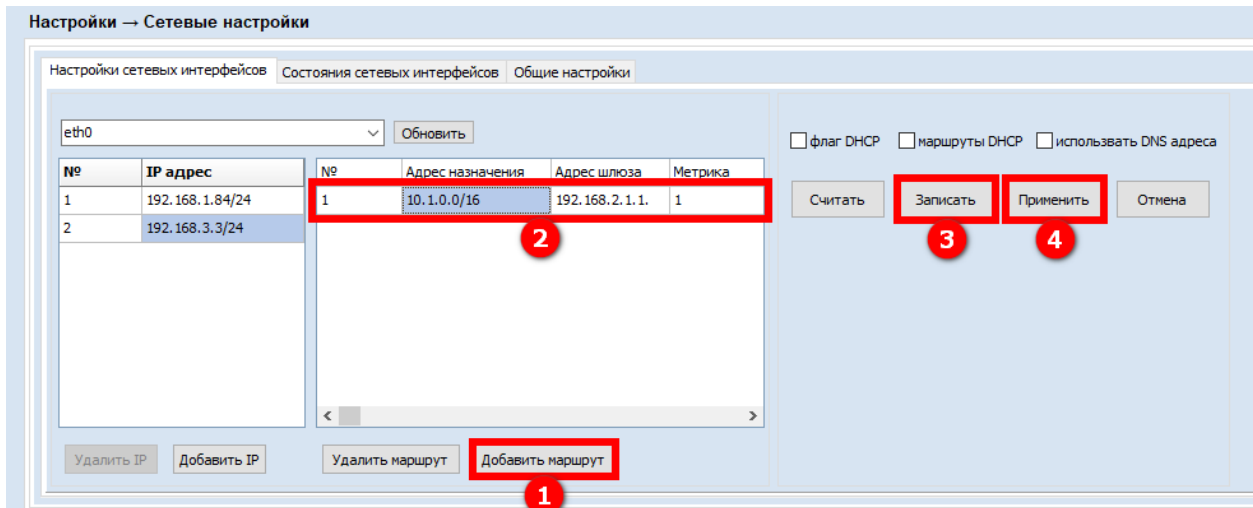


Рисунок 18 – Добавление маршрута

5.1.6 Изменение маршрута

Для изменения IP-адреса:

1. Считайте список сетевых интерфейсов в соответствии с п. 5.1.1.
2. Выберите целевую ячейку в строке маршрута, подлежащего изменению.
3. Введите новое значение в выбранной ячейке (1) (см. рисунок 19).
4. Нажмите кнопку **Записать** (2).
5. Нажмите кнопку **Применить** (3).

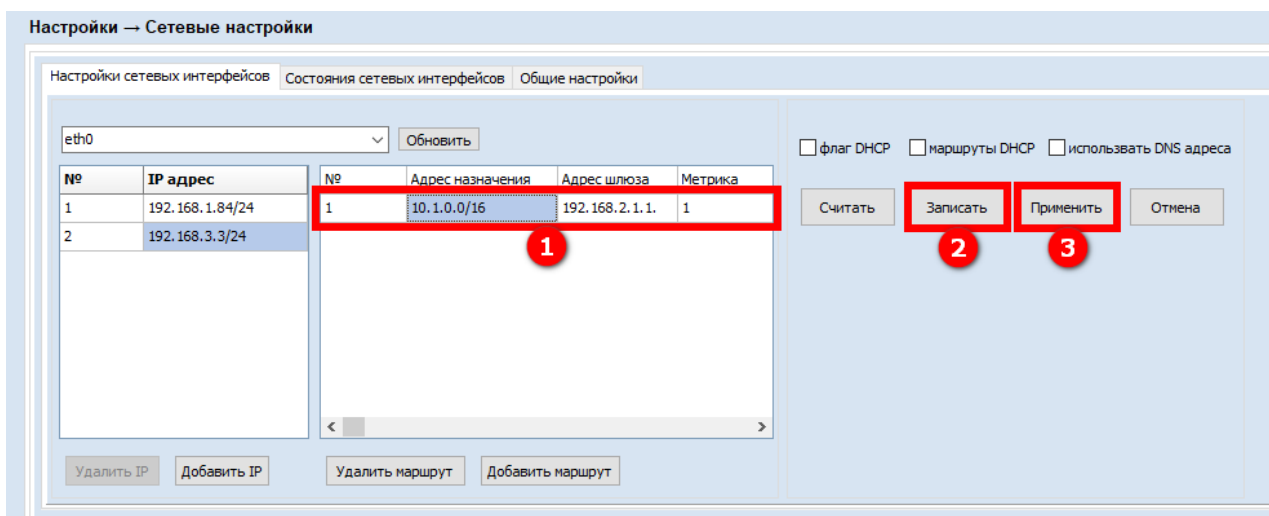


Рисунок 19 – Изменение маршрута

5.1.7 Удаление маршрута

Для удаления маршрута:

1. Считайте список сетевых интерфейсов в соответствии с п. 5.1.1.
2. Выберите строку маршрута, подлежащего удалению (1) (см. рисунок 20).
3. Нажмите кнопку **Удалить маршрут** (2).
4. Нажмите кнопку **Записать** (3).
5. Нажмите кнопку **Применить** (4).

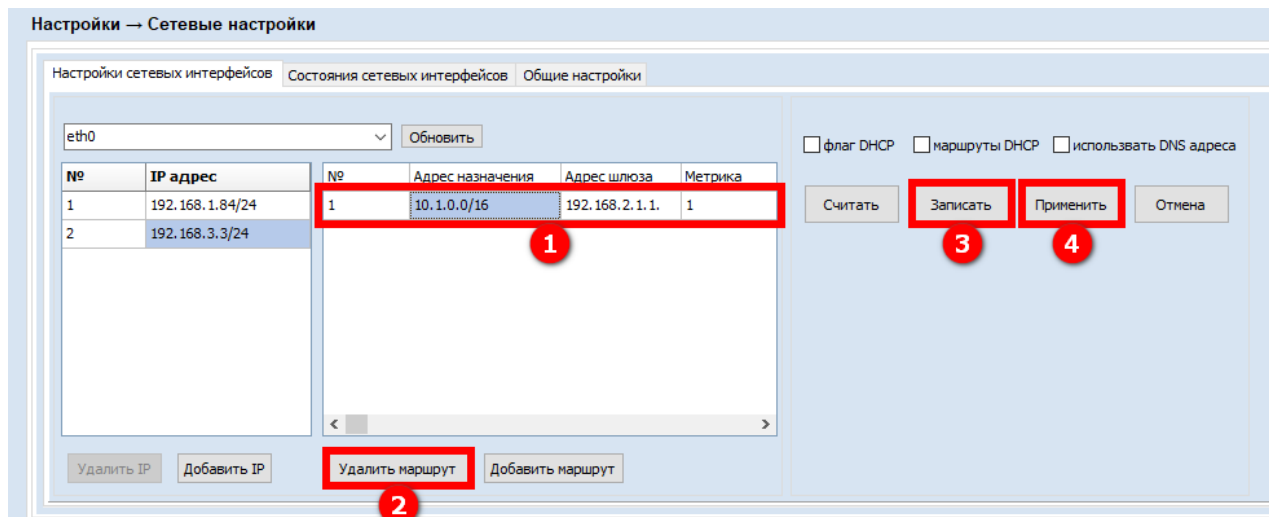


Рисунок 20 – Удаление маршрута

5.2 Общие настройки

Настройки → Сетевые настройки → Общие настройки

На вкладке **Общие настройки** вводятся общие правила работы УСПД в сети.

Кнопки:

- **Считать** – считывание параметра настройки;
- **Записать** – запись параметра настройки.

Поля:

- **Защита от DDoS-атак** – если флаг в поле установлен, будет выполняться защита от DDoS атак.
- **Лимит подключений** – максимальное количество TCP-подключений в заданный промежуток времени для защиты от DDoS атак. Если количество подключений превышает лимит, интерфейс блокируется.
- **Промежуток времени, с** – промежуток времени для контроля количества подключений при защите от DDoS атак.
- **Время блокировки интерфейса, с** – блокировка интерфейса на указанное время после отключения для защиты от DDoS атак.
- **Разрешить УСПД отвечать на пинг ICMP** – если флаг в поле установлен, УСПД будет посылать подтверждение нахождения в сети в ответ на команду ping.

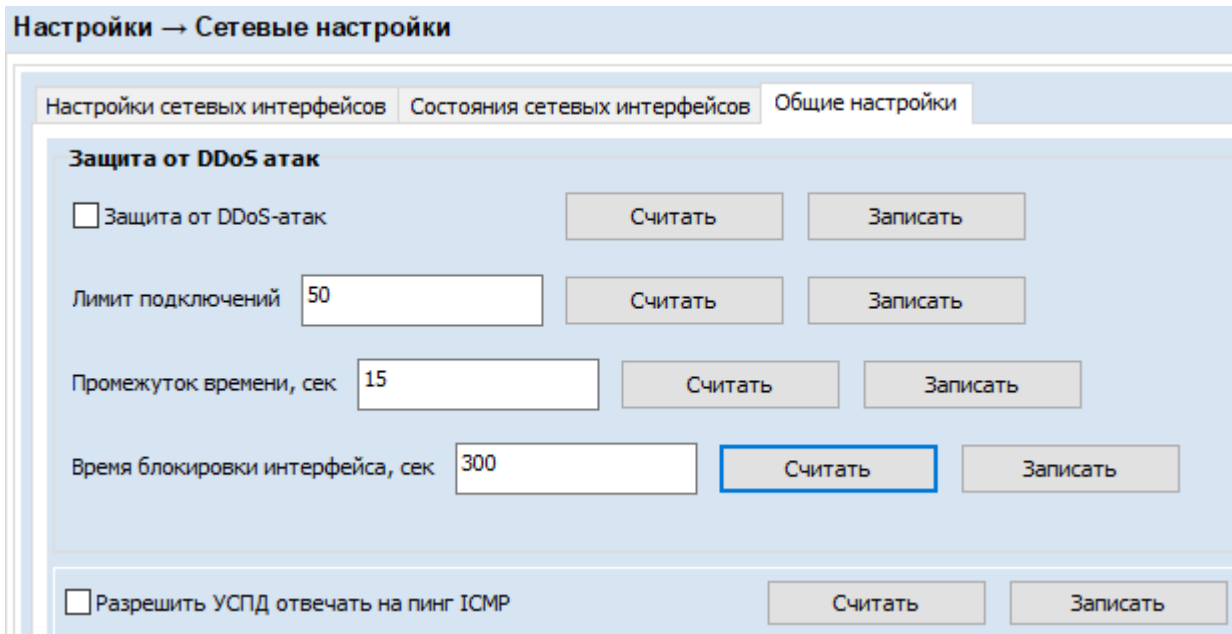


Рисунок 21 – Общие настройки

5.3 Состояние сетевых интерфейсов

Настройки → Сетевые настройки → Состояние сетевых интерфейсов
Вкладка доступна для чтения пользователям, описание см. РП.

5.4 SSL-сертификаты

Настройки → Сетевые настройки → SSL-сертификаты

На вкладке **SSL-сертификаты** выполняется считывание списка загруженных сертификатов, импорт новых сертификатов, выбор и запись сертификата Веб-сервера.

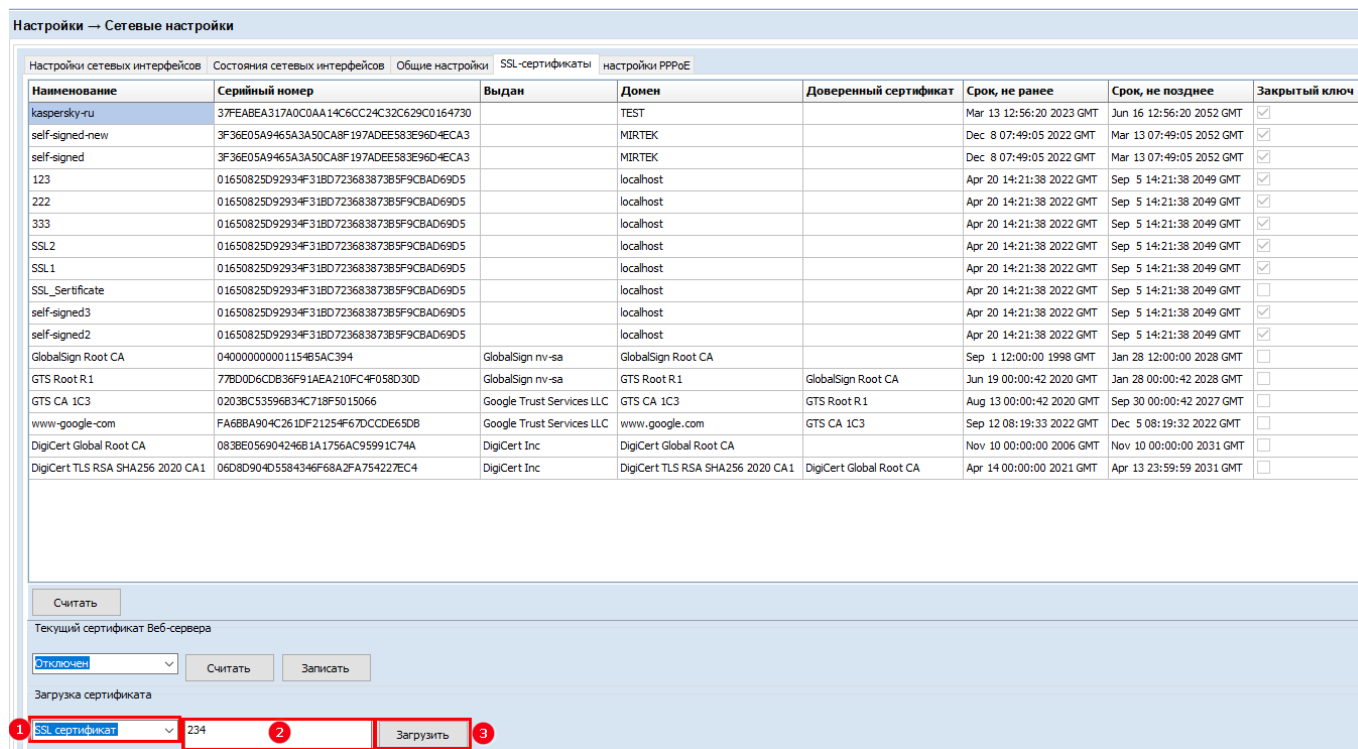


Рисунок 22 – SSL-сертификаты

Выполняется импорт самоподписанных SSL-сертификатов и SSL-сертификатов, выпущенных в стороннем центре сертификации. При импорте сертификата указывается сертификат и его приватный ключ.

Требования к сертификату:

- Сертификат должен быть актуален на момент импорта.
- Не допускается импорт сертификата до начала и после окончания срока его действия.
- Не допускается импорт приватного ключа, который защищен паролем.
- Сертификат и приватный ключ должны импортироваться в PEM-encoded формате.



Чтобы обеспечить бесперебойную работу с сертификатом, своевременно обновляйте его.

Кнопки:

- **Считать** – считывание списка сертификатов или считывание текущего сертификата Веб-сервера;
- **Записать** – запись выбранного сертификата Веб-сервера в память устройства;
- **Загрузить** – загрузка SSL-сертификата или приватного ключа.

Поля:

- **Текущий сертификат Веб-сервера** – сертификат, записанный в память устройства, для записи выбирается из списка доступных сертификатов;
- **Загрузка сертификата** – выбор варианта для загрузки: «SSL-сертификат» / «Закрытый ключ SSL-сертификата».

Поля таблицы загруженных SSL-сертификатов:

- **Наименование**;
- **Серийный номер**;
- **Выдан** – информация об издателе;
- **Домен** – доменное имя;
- **Срок, не ранее** – дата начала действия сертификата;
- **Срок не позднее** – дата окончания действия сертификата;
- **Закрытый ключ** – если флаг в поле установлен, приватный ключ для сертификата загружен.

5.4.1 Загрузка сертификата

Предварительные условия: Необходимо выпустить самоподписанный сертификат и приватный ключ или получить их в стороннем центре сертификации. Файлы сертификата и приватного ключа должны быть размещены на компьютере или на доступных сетевых ресурсах. Доступ к данным файлам должен быть разрешен только Администратору.

1. Выберите значение «SSL-сертификат» в поле **Загрузка сертификата** (1) (см. рисунок 22).
2. Введите наименование сертификата в поле справа (2). Под данным наименованием сертификат будет фигурировать в таблице SSL-сертификатов.
3. Нажмите кнопку **Загрузить** (3).
4. Выберите файл SSL-сертификата (sert.pem), пользуясь стандартными средствами ОС Windows.
5. Выберите значение «Закрытый ключ SSL-сертификата» в поле **Загрузка сертификата**.
6. Нажмите кнопку **Загрузить**.

7. Выберите файл приватного ключа (key.pem), пользуясь стандартными средствами ОС Windows.

В результате выполненных действий SSL-сертификат и приватный ключ будут загружены в устройство.

5.4.2 Запись сертификата Веб-сервера

1. Выберите имя сертификата в выпадающем списке в поле **Текущий сертификат Веб-сервера**.
2. Нажмите кнопку **Записать**.

В результате выполненных действий сертификат будет записан в память устройства.

6 Обновление ПО и дополнительные настройки

6.1 Дополнительно

Настройки → Дополнительно

Блок предназначен для дополнительных настроек, в т. ч. загрузки (выгрузки) конфигурационного файла УСПД, обновление встроенного ПО, перезагрузки УСПД.

Следующие поля блока могут быть изменены только для администратором:



- **Разрешить доступ суперпользователя по SSH**
- **Разрешить обновление с USB-устройства**
- **Разрешить загрузку файлов только при подключении с шифрованием**

Кнопки:

- **Получить файл** – запросить образец конфигурационного файла (1) (см. рисунок 23).
- **Остановить** – остановить запрос образца файла (1), остановить обновление (3).
- **Загрузить конф-й файл** – загрузить конфигурационный файл (1).
- **Считать** – считать адрес ASDU mek 104 (2) или флаг в поле блока **Дополнительные параметры** (5), максимальное количество ПУ (6).
- **Записать** – записать адрес ASDU mek 104 (2) или флаг в поле блока **Дополнительные параметры** (5), максимальное количество ПУ (6).
- **...** – выбор файла.
- **Обновить** – обновление ВПО (3).
- **Перезагрузка** – выполнить перезагрузку устройства (4).

Поля:

- **Новый адрес устройства** – новый адрес УСПД.
- **Имя файла** – имя конфигурационного файла
- **Адрес ASDU mek 104**
- **Авторегистрация** – если флаг в поле установлен, выполняется авторегистрация ПУ в таблице счетчиков.
- **Разрешить обновление с USB-устройства** – если флаг в поле установлен, выполняется обновление с USB-устройств.
- **Разрешить доступ для суперпользователя по SSH** – технологическое поле, используется только для доступа разработчика.
- **Разрешить загрузку файлов только при подключении с шифрованием** – если флаг в поле установлен, загрузка файлов выполняется только при подключении с шифрованием.

- **Максимальное количество приборов учета для опроса** – предельное количество ПУ, доступных для опроса.

Настройки → Дополнительно

1 Запрос/загрузка файлов

Имя файла

... Имя файла

2 Получить/записать адрес ASDU mek 104

3 Обновление встроенного ПО

...

4 Действия

5 Дополнительные параметры

<input type="checkbox"/> Авторегистрация	<input type="button" value="Считать"/>	<input type="button" value="Записать"/>
<input type="checkbox"/> Разрешить доступ суперпользователю по SSH	<input type="button" value="Считать"/>	<input type="button" value="Записать"/>
<input type="checkbox"/> Разрешить обновление с USB-устройства	<input type="button" value="Считать"/>	<input type="button" value="Записать"/>
<input type="checkbox"/> Разрешить загрузку файлов только при подкл. с шифрованием	<input type="button" value="Считать"/>	<input type="button" value="Записать"/>

6 Максимальное количество приборов учета для опроса

Рисунок 23 – Блок Настройки – Дополнительно

6.1.1 Загрузка конфигурационного файла МЭК 104

Загрузка карты регистров для протокола МЭК 104 осуществляется с помощью загрузки конфигурационного файла.

Конфигурационный файл предоставляется в текстовом формате с разделителем между полями ";". В одной строке файла содержится описание диапазона адресов карты. Строки, начинающиеся с ";", игнорируются.

Поля файла:

- 1 – начальный адрес диапазона;
- 2 – количество последовательных адресов;
- 3 – тип данных. Через символ "-" могут задаваться дополнительные параметры, например ad1 – адрес устройства "1";
- 4 – дополнительные опции.

В таблице 7 приведены типы устройств (данных), их описание, дополнительная информация и примеры применения.

Таблица 7 – Описание типов устройств

Тип устройства	Описание типа	Применение
TS	сигналы TS УСПД	Пример: "100;4;TS;" Начальный адрес диапазона 100; диапазон 100 – 103; Сигналы TS;

Тип устройства	Описание типа	Применение
RealLab_NL_16HV	состояние DI модулей семейства RealLab_NL_16	Устройство RealLab должно быть внесено в список устройств, с протоколом modbus, на порту подключения устройства, должен быть разрешен протокол modbus. Пример: "200;16;RealLab_NL_16HV-ad1;"
IEC101	адрес устройства, с протоколом МЭК 101	В дополнительных опциях необходимо указать TYPE – тип объекта информации и IOA – адрес объекта информации в устройстве. Устройство должно быть внесено в список устройств, с протоколом МЭК 101, на порту подключения устройства должен быть разрешен протокол МЭК 101. Пример: "301;3;IEC101-ad1;TYPE=45,IOA=51; "
InstantValues	мгновенные значения собираемые ПУ	ПУ должен быть внесен в таблицу счетчиков. В третьем поле необходимо указать тип мгновенного значения (например it4), см. приложение В. Пример: "400;1;InstantValues-ad24810-it4;"

Для получения образца конфигурационного файла:

1. Введите путь к файлу и имя файла в поле Имя файла в блоке Запрос/загрузка файла (1).
2. Нажмите кнопку Получить файл.

Для загрузки конфигурационного файла:

1. Нажмите кнопку ... в блоке Запрос/загрузка файла (1).
2. Выберите файл, пользуясь стандартными средствами ОС Windows.
3. Нажмите кнопку Загрузить конф-й файл.

6.1.2 Изменение адреса ASDU mek 104

1. Нажмите кнопку **Считать** в блоке **Получить/записать адрес ASDU mek 104** (2).
2. Введите новый адрес.
3. Нажмите кнопку **Записать**.

6.1.3 Обновление ВПО



Новые версии ВПО распространяются бесплатно в электронном виде на сайте www.mirtekgroup.com. Скачайте файлы обновлений.

Файлы обновлений ВПО:

- файл обновления программы модема (пример: ull_modem20210208.bin);
- файл обновления основной программы УСПД (пример: ull_update20210208.bin).

1. Нажмите кнопку ... в блоке **Обновление встроенного ПО** (3).
2. Выберите файл, пользуясь стандартными средствами ОС Windows.
3. Нажмите кнопку **Обновить**.



Проконтролируйте обновления значений идентификатора базы данных и профиля модема см. п. 4.1.

6.1.4 Перезагрузка УСПД

1. Нажмите кнопку **Перезагрузка** в блоке **Действия** (4).
2. Дождитесь окончания перезагрузки контроллера.

6.1.5 Изменение флага в блоке **Дополнительные параметры**

Для разрешения/запрещения ввода в действие дополнительного параметра настройки:

1. Нажмите кнопку **Считать** рядом с полем параметра в блоке **Дополнительные параметры** (5).
2. Установите/снимите флаг в поле параметра.
3. Нажмите кнопку **Записать** рядом с полем параметра в блоке **Дополнительные параметры**.

6.1.6 Ограничение количества ПУ для опроса

Для ограничения количества опрашиваемых ПУ:

1. Нажмите кнопку **Считать** рядом с полем **Дополнительные параметры** (6).
2. Установите/снимите флаг в поле параметра.
3. Нажмите кнопку **Записать** рядом с полем параметра в блоке **Дополнительные параметры**.

7 Действие с конфигурацией

Настройки → Действие с конфигурацией

Блок предназначен для загрузки/выгрузки параметров конфигурации УСПД, а также включения режима проверки времени.

7.1 Вкладка **действие с конфигурацией**

Настройки → Действие с конфигурацией → Действие с конфигурацией

Вкладка предназначена для загрузки/выгрузки параметров конфигурации УСПД в файл конфигурации.



Следующие поля блока могут быть изменены только для администратором:

- **Запрет изменений настроек УСПД при закрытой крышке**
- **Запрет экспорта паролей**

Состав параметров конфигурации:

- часовой пояс;
- настройки синхронизации времени приборов учета;
- сервер точного времени;
- параметры опроса;
- таблица счетчиков (опционально);
- пользователи (опционально);
- настройки координаторов;
- тарифное расписание.

Кнопки:

- **Сохранить конфигурацию с УСПД** – сохранение параметров конфигурации УСПД в файл.
- **Загрузить конфигурацию с ПК** – загрузка параметров конфигурации из файла.
- **Считать** – считать флаг запрета изменения настроек УСПД при закрытой крышке или флаг проверки.
- **Записать** – записать флаг запрета изменения настроек УСПД при закрытой крышке или флаг проверки.

Поля:

- **Сохранить пользователей** – если флаг в поле установлен, параметры зарегистрированных пользователей выгружаются в файл.
- **Сохранить приборы учета** – если флаг в поле установлен, параметры подключенных ПУ (таблица счетчиков) выгружаются в файл.
- **Загрузить пользователей** – если флаг в поле установлен, параметры зарегистрированных пользователей загружаются из файла.
- **Загрузить приборы учета** – если флаг в поле установлен, параметры подключенных ПУ (таблица счетчиков) загружаются из файла.
- **Запрет изменений настроек УСПД при закрытой крышке** – если флаг в поле установлен, запрещены изменения конфигурации, если крышка УСПД закрыта.
- **Запрет экспорта паролей** – если флаг в поле установлен, запрещен экспорт паролей.

7.1.1 Сохранение файла конфигурации

1. Установите флаги в полях вкладки **Действие с конфигурацией** в соответствии с описанием.
2. Нажмите кнопку **Сохранить конфигурацию с УСПД** (1) (см. рисунок 24).
3. Сохраните файл, пользуясь стандартными средствами ОС Windows.

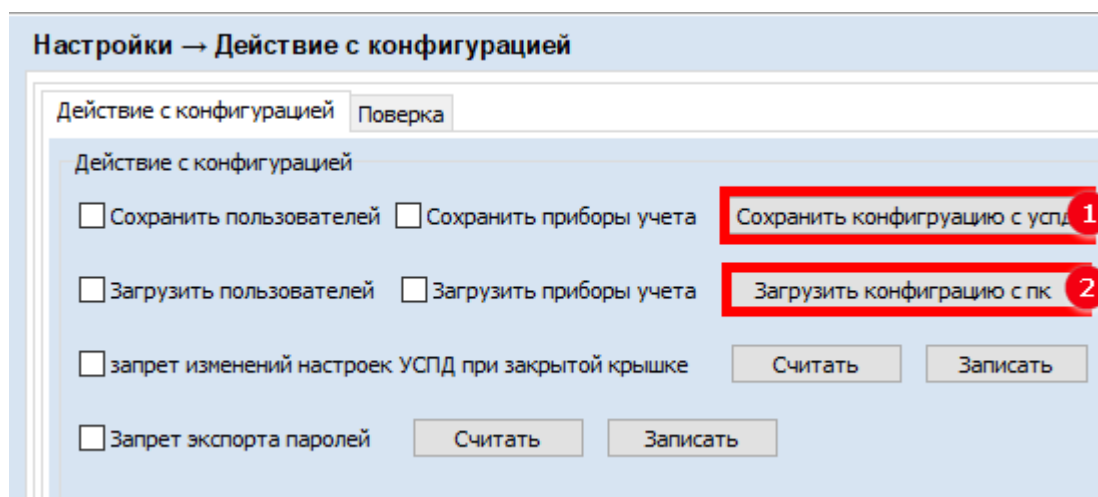


Рисунок 24 – Блок Настройки – Действие с конфигурацией – Действие с конфигурацией

7.1.2 Загрузка файла конфигурации

1. Установите флаги в полях вкладки **Действие с конфигурацией** в соответствии с описанием.
2. Нажмите кнопку **Загрузить конфигурацию с ПК** (2).
3. Выберите файл, пользуясь стандартными средствами ОС Windows.



Если флаг в поле **Запрет изменений настроек УСПД при закрытой крышке** установлен, конфигурирование УСПД может быть выполнено только после открытия крышки УСПД (см. рисунок 43).

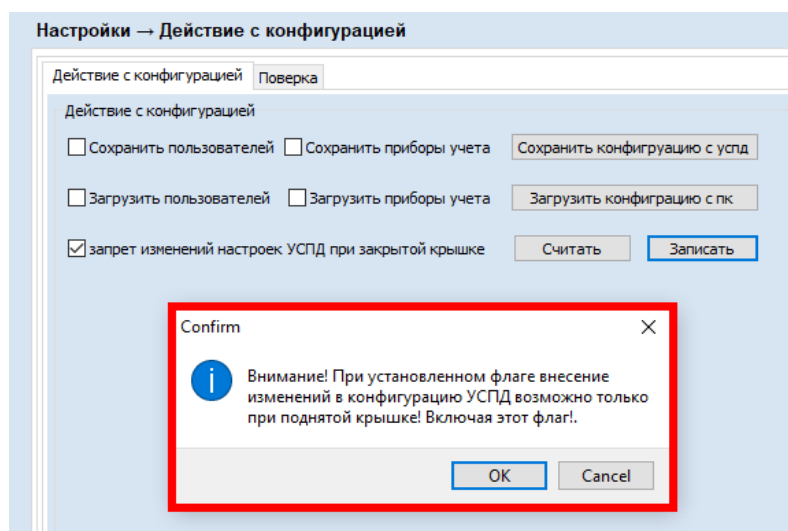


Рисунок 25 – Блок Настройки – Действие с конфигурацией – Действие с конфигурацией – флаг запрета изменений

8 Чтение и анализ журналов

В журналы в автоматическом режиме выполняются записи о событиях УСПД и других подключенных устройств. Журналы содержат информацию, необходимую администратору для анализа работы УСПД и подключенных устройств, а также событий безопасности.

При чтении журналов используются следующие кнопки:

- **Считать** – в зависимости от положения в интерфейсе и выполненных действий чтение списка устройств, списка журналов, журнала.
- **Отмена** – отмена чтения журнала.
- **Экспорт в Excel** – экспорт записей журнала в файл формата Excel.

Для эффективного анализа событий в журналах используются возможности фильтрации и сортировки данных (см. рисунок 26). Для выполнения фильтрации по заданному значению нажмите значок фильтра в целевом столбце таблицы и выберите значение в выпадающем списке.

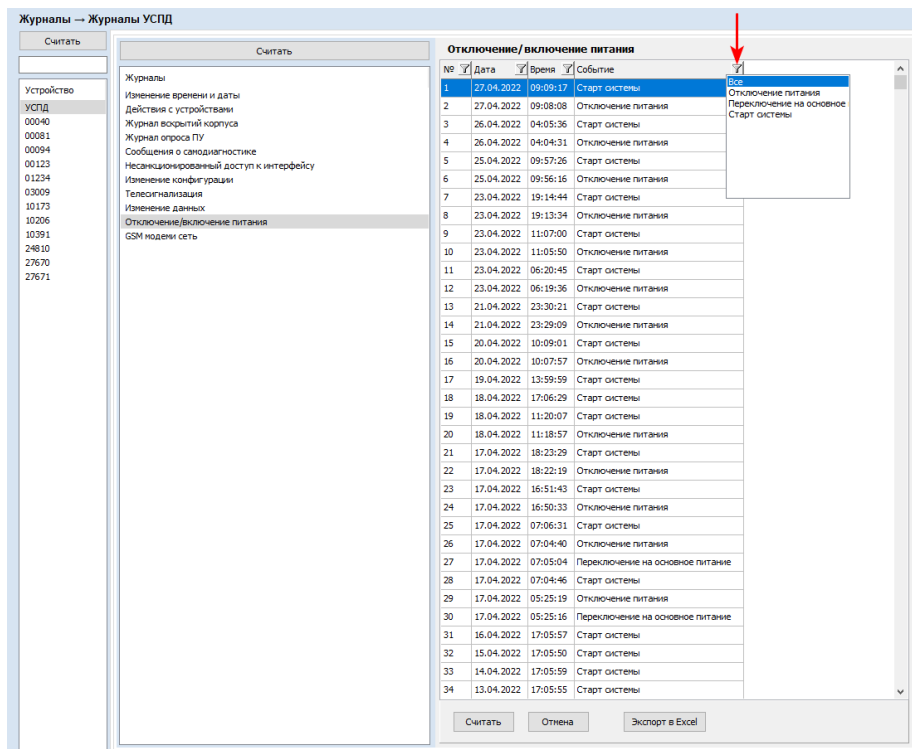


Рисунок 26 – Фильтрация в журналах событий

8.1 Журналы УСПД

Журналы → Журналы УСПД

Форма предназначена для анализа журналов событий УСПД. Доступны следующие журналы событий:

- Изменение времени и даты;
- Действия с устройствами;
- Журнал вскрытий корпуса;
- Журнал опроса ПУ;
- Сообщения о самодиагностике;
- Несанкционированный доступ к интерфейсу;
- Изменение конфигурации;
- Телесигнализация;
- Отключение/включение питания;
- GSM модем и сеть.

8.1.1 Чтение журнала УСПД

Для чтения журнала УСПД:

1. Нажмите кнопку **Считать** в левом верхнем углу формы (1) (см. рисунок 27). В блоке ниже будет отображен список: УСПД, номера ПУ и других устройств, подключенных к УСПД (2).

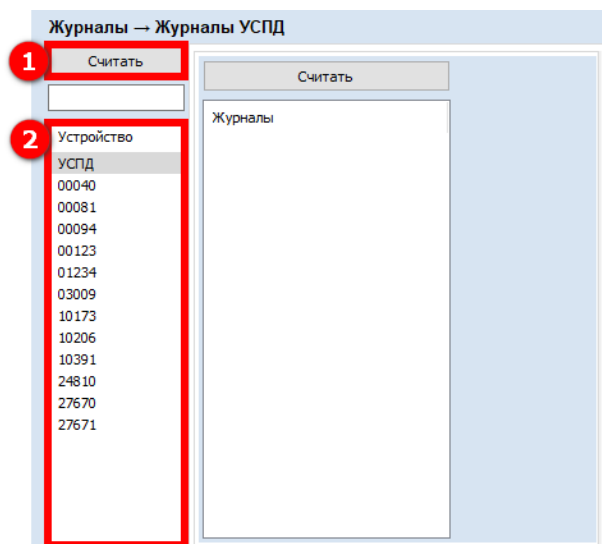


Рисунок 27 – Считывание доступных устройств

2. Выберите «УСПД» в списке приборов (1) (см. рисунок 28).
3. Нажмите кнопку **Считать** в правом блоке (2). Ниже в блоке будет выведен список доступных журналов.

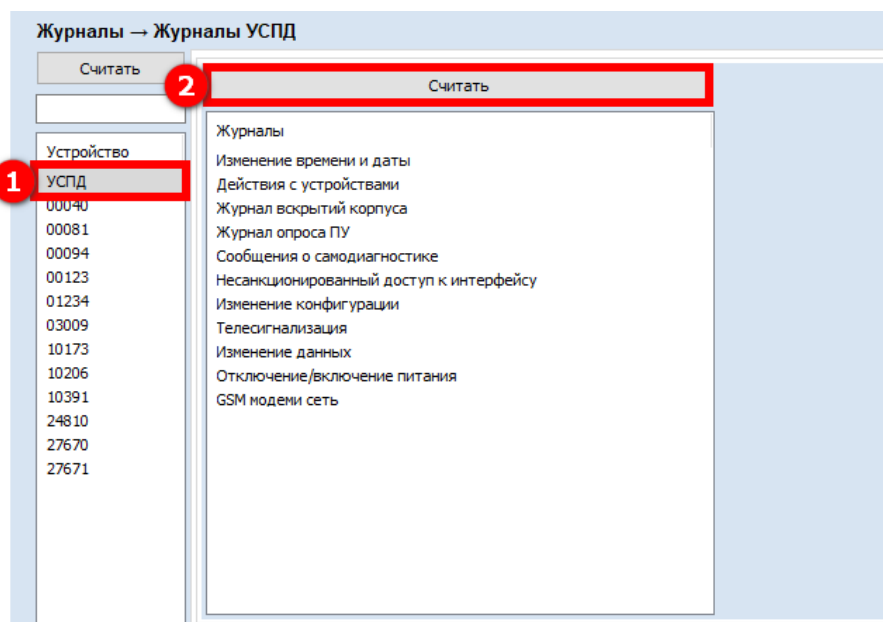


Рисунок 28 – Считывание списка доступных журналов УСПД

4. Выберите целевой журнал (1) (см. рисунок 29).

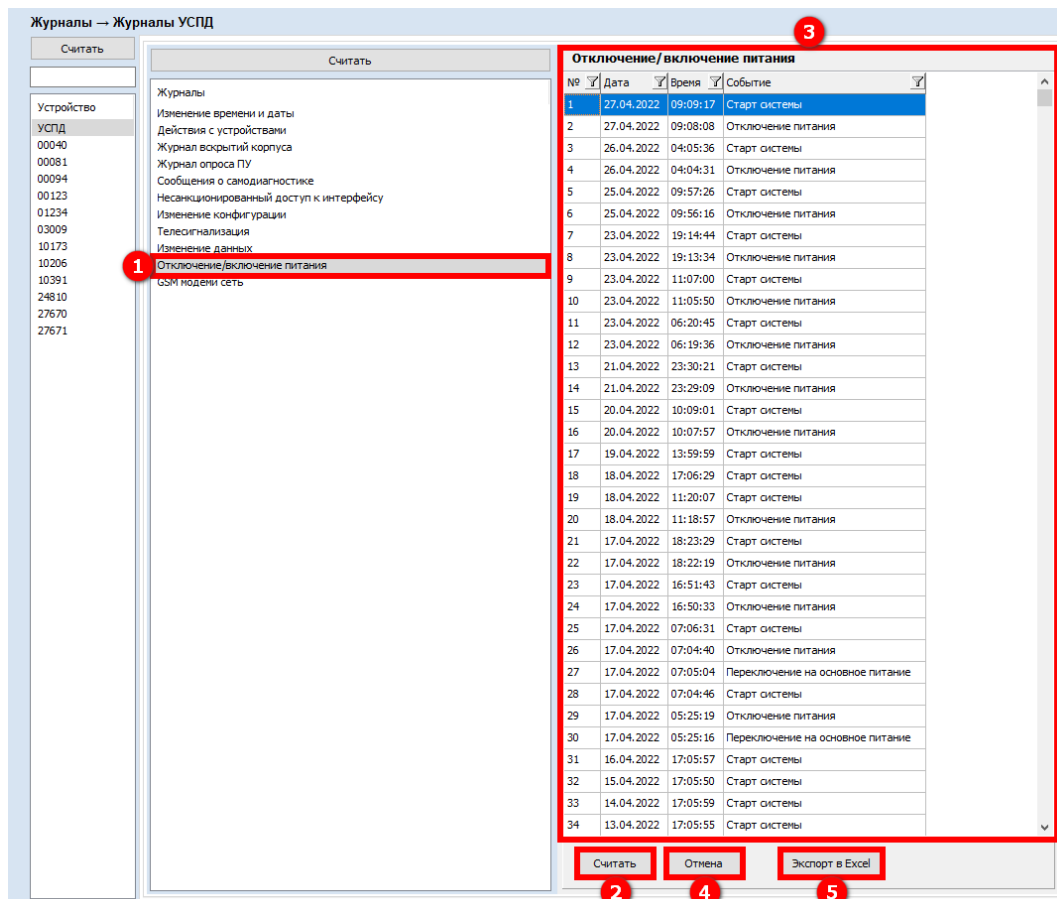


Рисунок 29 – Просмотр журнала

5. Нажмите кнопку **Считать** (2). В блоке <Название журнала> будут отображены записи в выбранном журнале (3).

8.2 Журналы ПУ

Журналы → Журналы ПУ

УСПД принимает все события от приборов учета, в том числе события безопасности ПУ, передаваемые по протоколу СПОДЭС.

Форма предназначена для анализа журналов событий подключенных ПУ. Доступны следующие журналы событий:

- Журнал отключения/включения питания;
- Журнал перезагрузок устройства;
- Журнал сообщений о самодиагностике;
- Журнал попыток несанкционированного доступа;
- Журнал управления нагрузкой;
- Журнал изменения конфигурации;
- Журнал изменения данных;
- Журнал изменений времени и даты;
- Журнал фиксации неверной фазировки;
- Журнал событий электронных пломб;
- Журнал параметров качества сети;
- Журнал потребительского баланса;
- Журнал вскрытий корпуса;
- Журнал событий платы коммутаторов.

8.2.1 Чтение журнала ПУ

Для чтения журнала ПУ:

1. Нажмите кнопку **Считать** в левом верхнем углу формы (1) (см. рисунок 30). В блоке ниже будет отображен список: номера ПУ, подключенных к УСПД (2).

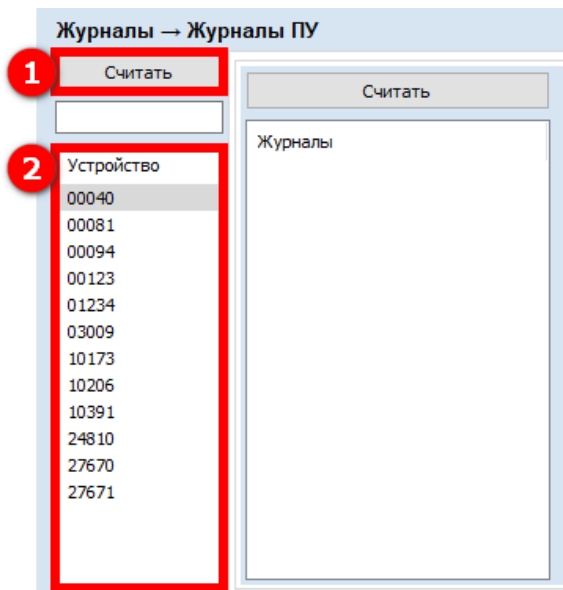


Рисунок 30 – Считывание доступных ПУ

2. Выберите номер ПУ в списке приборов (1) (см. рисунок 31).
3. Нажмите кнопку **Считать** в правом блоке (2). Ниже в блоке будет выведен список доступных журналов.

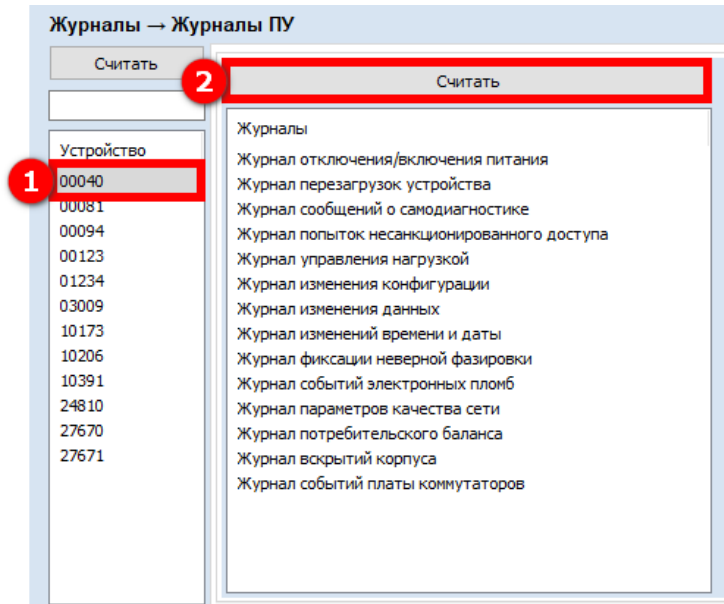


Рисунок 31 – Считывание списка доступных журналов ПУ

4. Выберите целевой журнал (1) (см. рисунок 32).

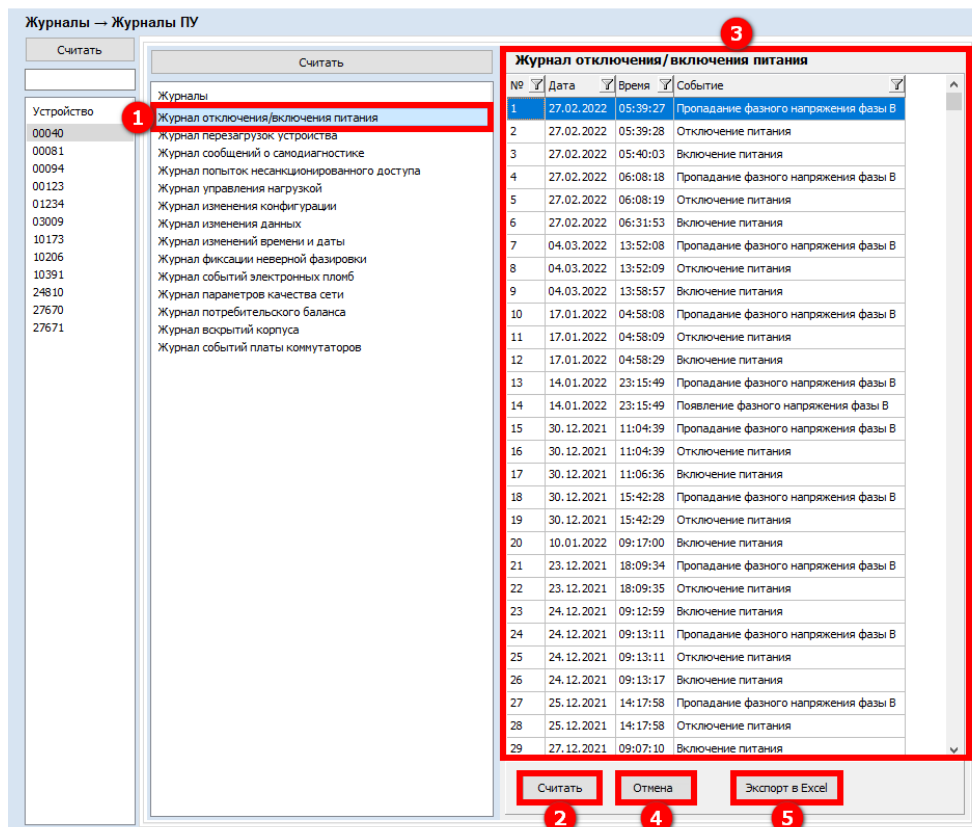


Рисунок 32 – Просмотр журнала ПУ

5. Нажмите кнопку **Считать** (2). В блоке <Название журнала> будут отображены записи в выбранном журнале (3).

8.3 Журнал безопасности

Журналы → Журнал безопасности

Форма предназначена для анализа событий журнала безопасности УСПД.



Предварительно необходимо поставить отметку о необходимости записывать журнал безопасности, а также настроить глубину хранения записей в журнале в соответствии см. п. 4.2.

В журнал безопасности УСПД записываются следующие события безопасности:

- загрузка (останов), сбой, перезагрузка программного обеспечения;
- запуск/останов сервисов, в том числе нештатное завершение сервиса;
- проверка контрольных сумм файлов программного обеспечения и конфигурации, подсистемы связи, веб-интерфейса;
- подключение к интерфейсам управления;
- запрос на параллельный сеанс доступа к УСПД;
- использование механизма аутентификации;
- превышение количества неудачных попыток аутентификации;
- обновление (модификация встроенного) программного обеспечения;
- несанкционированная попытка обновления;
- ограничение функциональности УСПД при обнаружении нарушения целостности ВПО;
- изменение конфигурации (параметров настройки);
- включение и выключение портов связи;
- вскрытие шкафа с УСПД;

- дата и время вскрытия корпуса;
- дата и время последнего перепрограммирования (параметрирования);
- дата и время фиксации данных об аппаратном или программном сбое;
- дата и время попытки несанкционированного нарушения целостности программного обеспечения и параметров;
- дата и время сеанса связи с устройством, приведшего к изменению параметров конфигурации, режимов функционирования (в том числе введение полного и (или) частичного ограничения (возобновления) режима потребления электрической энергии (управление нагрузкой);
- изменение текущих значений времени и даты при синхронизации времени в журнале событий времени до и после коррекции или величины коррекции времени, на которую было скорректировано значение;
- создание, редактирование, отключение пользователей, изменение паролей и криптографических ключей;
- использование съемных носителей информации.

8.3.1 Чтение журнала безопасности

Для чтения журнала безопасности:

1. Выберите «УСПД» в левом блоке формы (1) (см. рисунок 33).
2. Нажмите кнопку **Считать** в правом блоке формы (2).

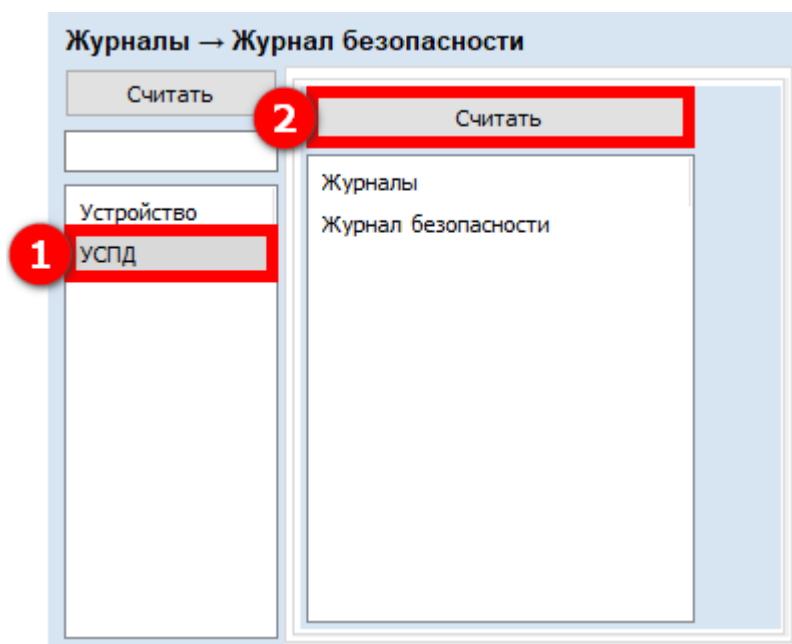


Рисунок 33 – Считывание журнала безопасности

3. Выберите «Журнал безопасности» в правом блоке формы.
4. Нажмите кнопку **Считать**. В блоке **Журнал безопасности** (2) (см. рисунок 34). В результате выполненных действий будут считаны записи журнала безопасности.

Журналы → Журнал безопасности УСПД

Считать

Журнал безопасности

№	Id записи	Дата	Время	Событие	Результат События	Id сессии	Источник События	Логин пользователя	Роль пользователя	Протокол соединения
1	4528	06.10.2022	11:11:49	Использование механизма аутентификации	успешно	10462	mir1	admin	Администратор	МІРТЕК
2	4527	06.10.2022	11:11:49	Событие успешной аутентификации пользователя (192.168.1.2:50931, admin 1)	успешно	10462	mir1	admin	Администратор	МІРТЕК
3	4526	06.10.2022	10:53:47	Unknown_code \$0278	успешно	0	не определен		Администратор	не определен
4	4525	06.10.2022	10:51:41	Использование механизма аутентификации	успешно	10461	mir1	admin	Администратор	МІРТЕК
5	4524	06.10.2022	10:51:41	Событие успешной аутентификации пользователя (192.168.1.45:43008, admin 1)	успешно	10461	mir1	admin	Администратор	МІРТЕК
6	4523	06.10.2022	10:47:15	Unknown_code \$0278	успешно	0	не определен		Администратор	не определен
7	4522	06.10.2022	10:46:20	Unknown_code \$0277	успешно	10459	mir1	admin	Администратор	МІРТЕК
8	4521	06.10.2022	10:46:09	Изменение параметра Разрешить только подключение с шифрованием (TRUE, FALSE)	успешно	10459	mir1	admin	Администратор	МІРТЕК
9	4520	06.10.2022	10:46:05	Unknown_code \$0278	успешно	0	не определен		Администратор	не определен
10	4519	06.10.2022	10:45:53	Использование механизма аутентификации	успешно	10459	mir1	admin	Администратор	МІРТЕК
11	4518	06.10.2022	10:45:53	Событие успешной аутентификации пользователя (192.168.1.45:47184, admin 1)	успешно	10459	mir1	admin	Администратор	МІРТЕК
12	4517	06.10.2022	10:41:25	Unknown_code \$0278	успешно	0	не определен		Администратор	не определен
13	4516	06.10.2022	10:39:10	Изменение параметра Разрешить только подключение с шифрованием (FALSE, TRUE)	успешно	10457	mir1	admin	Администратор	МІРТЕК
14	4515	06.10.2022	10:38:55	Использование механизма аутентификации	успешно	10457	mir1	admin	Администратор	МІРТЕК
15	4514	06.10.2022	10:38:55	Событие успешной аутентификации пользователя (192.168.1.45:34696, admin 1)	успешно	10457	mir1	admin	Администратор	МІРТЕК
16	4513	06.10.2022	10:34:01	Unknown_code \$0277	успешно	10456	mir1	admin	Администратор	МІРТЕК
17	4512	06.10.2022	10:33:57	Использование механизма аутентификации	успешно	10456	mir1	admin	Администратор	МІРТЕК
18	4511	06.10.2022	10:33:57	Событие успешной аутентификации пользователя (192.168.1.253:59168, admin 1)	успешно	10456	mir1	admin	Администратор	МІРТЕК
19	4510	06.10.2022	10:33:28	Unknown_code \$0277	успешно	10455	mir1	admin	Администратор	МІРТЕК
20	4509	06.10.2022	10:33:24	Использование механизма аутентификации	успешно	10455	mir1	admin	Администратор	МІРТЕК
21	4508	06.10.2022	10:33:24	Событие успешной аутентификации пользователя (192.168.1.253:59154, admin 1)	успешно	10455	mir1	admin	Администратор	МІРТЕК
22	4507	06.10.2022	10:32:02	Unknown_code \$0278	успешно	0	не определен		Администратор	не определен
23	4506	06.10.2022	10:29:38	Использование механизма аутентификации	успешно	10454	mir1	admin	Администратор	МІРТЕК
24	4505	06.10.2022	10:29:38	Событие успешной аутентификации пользователя (192.168.1.45:56564, admin 1)	успешно	10454	mir1	admin	Администратор	МІРТЕК
25	4504	06.10.2022	10:29:03	Unknown_code \$0277	успешно	10453	mir1	admin	Администратор	МІРТЕК
26	4503	06.10.2022	10:27:47	Использование механизма аутентификации	успешно	10453	mir1	admin	Администратор	МІРТЕК
27	4502	06.10.2022	10:27:47	Событие успешной аутентификации пользователя (192.168.1.45:40034, admin 1)	успешно	10453	mir1	admin	Администратор	МІРТЕК
28	4501	06.10.2022	10:26:51	Unknown_code \$0278	успешно	0	не определен		Администратор	не определен
29	4500	06.10.2022	10:24:34	Использование механизма аутентификации	успешно	10452	mir1	admin	Администратор	МІРТЕК
30	4499	06.10.2022	10:24:34	Событие успешной аутентификации пользователя (192.168.1.45:60102, admin 1)	успешно	10452	mir1	admin	Администратор	МІРТЕК

Считать Отмена Экспорт в Excel

Рисунок 34 – Просмотр журнала безопасности

Поля журнала:

- ID записи;
- Дата события;
- Время события;
- Событие;
- Результат события;
- ID сессии;
- Источник события;
- Логин пользователя;
- Роль пользователя;
- Протокол соединения;
- IP-адрес;
- Порт.

8.3.2 Проверка контрольных сумм системного ПО

Проверка целостности ПО выполняется в процессе самодиагностики после включения/перезагрузки УСПД, а затем ежедневно.

События начала проверки целостности ПО, контрольные суммы компонентов системного ПО, завершения проверки целостности ПО сохраняются в журнале безопасности УСПД.

Для выбора событий, в которых выводятся значения контрольных сумм:

1. Считайте журнал безопасности согласно п. 8.3.1 (см. рисунок 35).
2. Если события проверки контрольных сумм найти сложно, воспользуйтесь фильтром в столбце **Событие**.

Журнал безопасности							
№	Id записи	Дата	Время	Событие	Результат События	Id сессии	Источник
16	4802	06.10.2022	17:56:43	Начата проверка целостности системного ПО	успешно		система
17	4801	06.10.2022	17:56:43	Контрольная сумма подсистемы обновления (0xe105)	успешно		система
18	4800	06.10.2022	17:56:43	Контрольная сумма подсистемы связи (0x64ca)	успешно		система
19	4799	06.10.2022	17:56:42	Контрольная сумма ВПО (0x1407)	успешно		система
20	4798	06.10.2022	17:56:42	Контрольная сумма подсистемы веб-интерфейса (0xf74c)	успешно		система
21	4797	06.10.2022	17:56:39	Завершена проверка целостности ВПО (0/0)	успешно		система

Рисунок 35 – Считывание журнала безопасности

9 Сведения об уязвимостях

В соответствии с информацией банка данных угроз безопасности информации ФСТЭК России в программном обеспечении УСПД обнаружены следующие уязвимости:

1. Уязвимость в реализации системного вызова `mremap()` ядра операционной системы Linux, позволяющая нарушителю получить доступ к физической странице. Данная уязвимость не является угрозой безопасности, т.к. функция `mremap` не используется встроенным ПО, а запуск процессов, разработанных сторонними лицами, невозможен.
2. Уязвимость системы управления базами данных PostgreSQL, связанная с возможностью работы под учетной записью операционной системы без полномочий `root`, позволяющая нарушителю выполнить произвольный код. Данная уязвимость не является угрозой безопасности, т.к. нет возможности непосредственного подключения пользователя к встроенной базе данных УСПД.

10 Возможные проблемы и способы их решения

Разработчик гарантирует правильную работу ПО при соблюдении требований, изложенных в п. 2, а также устранение причин аварийных ситуаций ПО.

Услуга технической поддержки предоставляется бесплатно на соответствующий срок действия полученной лицензии.

В объем технической поддержки входит:

- консультирование по вопросам настройки ПО;
- диагностика и фиксация возникших ошибок ПО для последующего исправления в случае подтверждения ошибки;
- предоставление документации на ПО.

Для получения помощи в решении возникшей проблемы необходимо обратиться в службу технической поддержки любым из нижеперечисленных способов:

- связаться по телефону +7(988)7000123 (рабочие дни с 09:00 до 18:00 по московскому времени);
- связаться по электронной почте support@mirtekgroup.ru.

Для более эффективной организации обработки инцидента, при обращении в службу технической поддержки, необходимо в тексте обращения указать:

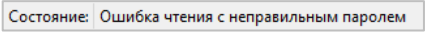
- наименование пользователя ПО;
- контактный телефон и email пользователя, на который будет отправляться вся информация по обращению;
- информацию о продукте (в т. ч. версии ПО продукта), по которому необходимо оказание услуги технической поддержки;
- подробное описание возникшей ситуации конкретный и пошаговый способ, приводящий к описываемому результату (в т.ч. прикрепить скриншоты экрана,

приложить файлы, на которых можно проверить изложенную в запросе информацию и т. д.).

Обращение в техническую поддержку должно содержать описание только одной проблемы. При наличии нескольких проблем необходимо создать и отправить несколько запросов.

Таблица 8 содержит перечень возможных ошибок, которые могут возникнуть у пользователя и способы их решения.

Таблица 8 – Возможные ошибки и рекомендации по их устранению

Описание ошибки	Рекомендации по устранению
Неверно введено значение логина и/или пароля 	1. Проверить корректность ввода значений логина и/или пароля. В случае повторной ошибки необходимо обратиться к администратору.
Ошибка при обновлении – отсутствие интернет-соединения	1. Проверить подключение к сети Интернет. Процесс обновления ПО возможен при наличии интернет-соединения. 2. Повторить запуск обновления. В случае повторной ошибки необходимо обратиться в службу технической поддержки.
Критическая ошибка в ПО	1. Перезапустить ПО. В случае повторной ошибки необходимо обратиться в службу технической поддержки.

11 Применение в составе объекта критической инфраструктуры

При применении УСПД в составе объекта критической информационной инфраструктуры необходимо обеспечение следующих требований:

- не допускается наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками владельца объекта КИИ, а также работниками его дочерних и зависимых обществ без контроля со стороны владельца объекта КИИ;
- не допускается наличие локального доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками владельца объекта КИИ, а также работниками его дочерних и зависимых Обществ без контроля со стороны владельца объекта КИИ;
- не допускается передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе средств защиты информации, или иным лицам без контроля со стороны владельца объекта КИИ.

Приложение А

Декларативные функции программного обеспечения и информационного обмена УСПД МИРТ-881

Встроенное в УСПД МИРТ-881 программное обеспечение «MIRTEK.5001» включает в себя встраиваемую операционную систему реального времени (далее – ОСРВ). ОСРВ предоставляет ряд функций, для управления задачами, и драйвера для доступа к аппаратным средствам целевой платформы: таймеры, устройства хранения данных, сетевые порты, последовательные порты, USB. ОСРВ представляет собой набор библиотек для вызова функций из исходного кода программного продукта «MIRTEK.5001». Функции администрирования пользователей, создания и изменения паролей учетных записей пользователей, поддержка сетевых и прикладных протоколов обмена данными реализуется в прикладной части «MIRTEK.5001».

Внешнее специальное программное обеспечение – программный комплекс «MeterTools», обеспечивает возможность конфигурирования всех настраиваемых параметров УСПД МИРТ-881.

Параметры информационного взаимодействия приведены в таблице А1.

Описание разграничения прав доступа пользователей УСПД МИРТ-881 приведены в таблице А2.

Таблица А1– Параметры информационного взаимодействия

№ п/п	Протоколы и функции	Интерфейсы /порты	Назначение/ Возможности	Учетная запись (роль)	Права доступа	Ссылки на пункты эксплуатационной документации	Примечание
1	2	3	4	5	6	7	8
1	МИРТЕК	RS-485 RS-232 CSD Ethernet (TCP порт 44445) GSM (TCP порт 44445)	Опрос УСПД	Роль согласно указанному пользователю при подключении	Чтение/Изменения данных		
2	RTU327	Ethernet (TCP порт 44445) GSM (TCP порт 44445)	Опрос УСПД	Оператор	Чтение		
3	МЭК 60870-5-104-2004	Ethernet (TCP порт 44445) GSM (TCP порт 44445)	Опрос УСПД	Телемеханика	Чтение/Изменения данных		
4	МЭК 61850	Ethernet (TCP порт 102) GSM (TCP порт 102)	Опрос УСПД	Телемеханика	Чтение/Изменения данных		

№ п/п	Протоколы и функции	Интерфейсы /порты	Назначение/ Возможности	Учетная запись (роль)	Права доступа	Ссылки на пункты эксплуатационной документации	Примечание
5	NTP	Ethernet (TCP порт 123) GSM (TCP порт 123)	Синхронизация времени УСПД	ntp	Чтение		
6	SSH	Ethernet (TCP порт 22) GSM (TCP порт 22)	Command Line Interface	cli	Чтение/Изменения данных		
7	SFTP	Ethernet (TCP порт 22) GSM (TCP порт 22)	Обновление УСПД	sftp	Обновление ВПО		
8	HTTP	Ethernet (TCP порт 80) GSM (TCP порт 80)	Web-интерфейс	Перенаправляется на HTTPS	Чтение/Изменения данных		
9	HTTPS	Ethernet (TCP порт 443) GSM (TCP порт 443)	Web-интерфейс	Роль согласно указанному пользователю при подключении	Чтение/Изменения данных		
10	SMS	GSM	Настройка передачи данных GSM	sms	Изменения данных		
11	Modbus/RTU	RS-485 RS-232 Ethernet (в режиме клиента)	Опрос устройств телемеханики				
12	МЭК 60870-5-101-2006	RS-485 RS-232	Опрос устройств телемеханики				
13	МЭК 60870-5-104-2004	Ethernet (TCP режим клиента) GSM (TCP режим клиента)	Опрос приборов учета				
14	МИРТЕК	RS-485 RS-232	Опрос приборов учета				

№ п/п	Протоколы и функции	Интерфейсы /порты	Назначение/ Возможности	Учетная запись (роль)	Права доступа	Ссылки на пункты эксплуатационной документации	Примечание
15	СПОДЭС	Ethernet (TCP режим клиента) GSM (TCP режим клиента)	Опрос приборов учета				
16	СЕТ4ТМ		Опрос приборов учета				
17	Меркурий		Опрос приборов учета				
18	A18xx		Опрос приборов учета				

Таблица А2 – Разграничение прав доступа пользователей УСПД МИРТ-881

	Роли								
	Права	Администратор	Оператор	Пользователь	sms	ntp	Телемеханика	cli	sftp
Чтение собранных данных	Чтение	+	+	-	-	-	+	-	-
	Запись	-	-	-	-	-	-	-	-
Конфигурирование параметров УСПД	Чтение	+	+	-	-	-	-	+	-
	Запись	+	+	-	-	-	-	+	-
Редактирование настроек безопасности	Чтение	+	-	-	-	-	-	-	-
	Запись	+	-	-	-	-	-	-	-
Администрирование пользователей (ввод, удаление)	Чтение	+	-	-	-	-	-	-	-
	Запись	+	-	-	-	-	-	-	-
Администрирование настроек безопасности	Чтение	+	-	-	-	-	-	-	-
	Запись	+	-	-	-	-	-	-	-

	Роли								
	Права	Администратор	Оператор	Пользователь	sms	ntp	Телемеханика	cli	sftp
Чтение журнала событий безопасности	Чтение	+	-	-	-	-	-	-	-
	Запись	-	-	-	-	-	-	-	-
Установка настроек подключения передачи данных GSM	Запись	+	-	-	+	-	-	-	-
Чтение времени УСПД	Чтение	+	+	+	-	+	+	+	-
Телеуправление	Запись	+	-	-	-	-	+	-	-
Обновление ВПО	Обновление ВПО	+	-	-	-	-	-	-	+