

**ООО «МИРТЕК»**

**ВЫСОКОВОЛЬТНЫЕ ПРИБОРЫ УЧЕТА  
ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ  
ТРЕХФАЗНЫЕ МНОГОФУНКЦИОНАЛЬНЫЕ  
«МИРТЕК-135-РУ»**

**ИНСТРУКЦИЯ ПО ПОДКЛЮЧЕНИЮ  
К ВПУ МИРТЕК-135-РУ ПО RF433**

**или GSM с помощью программы METER TOOLS по  
СПОДЭС или протоколу МИРТЕК**

**МИРТ.411152.205ИМЗ (V.1)**

**(ДОПОЛНЕНИЕ К МИРТ.411152.136 РЭ  
и МИРТ.411152.187 РЭ)**

# СОДЕРЖАНИЕ

<b>ПОДГОТОВКА К ПОДКЛЮЧЕНИЮ .....</b>	<b>3</b>
<b>1 ВЫБОР КАНАЛА СВЯЗИ .....</b>	<b>5</b>
<b>2 ПАРАМЕТРЫ КАНАЛА СВЯЗИ .....</b>	<b>6</b>
2.1 Параметры канала связи RF433 и мастер считывания данных МИРТ-141 .....	6
2.2 Параметры канала связи GSM с SIM-картой с динамическим IP-адресом .....	7
2.3 Параметры канала связи GSM с SIM-картой со статическим IP-адресом .....	7
<b>3 ПАРАМЕТРЫ ОПРОСА .....</b>	<b>8</b>
<b>4 ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ .....</b>	<b>8</b>
4.1 ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ ПО ПРОТОКОЛУ «МИРТЕК» .....	9
4.2 ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ ПО «СПОДЭС» .....	12
4.2.1 Общие сведения .....	12
4.2.2 Тип соединения «ПУБЛИЧНЫЙ КЛИЕНТ» .....	13
4.2.3 Тип соединения «СЧИТЫВАТЕЛЬ ДАННЫХ» .....	14
4.2.3.1 Вариант политики безопасности «Стандартный» .....	15
4.2.3.2 Варианты политики безопасности «С проверкой подлинности», «С шифрованием», «С проверкой подлинности и шифрованием» .....	15
4.2.4 Тип соединения «КОНФИГУРАТОР» .....	16
4.2.4.1 Вариант политики безопасности «Стандартный» .....	17
4.2.4.2 Варианты политики безопасности «С проверкой подлинности», «С шифрованием», «С проверкой подлинности и шифрованием» .....	17
4.2.5 НАСТРОЙКА ПАРАМЕТРОВ ДОСТУПА И ШИФРОВАНИЯ .....	20
4.2.5.1 Настройка паролей .....	20
4.2.5.2 Настройка комплекта безопасности .....	21
4.2.5.3 Настройка политики безопасности .....	22
4.2.5.4 Настройка ключей шифрования .....	22
<b>ПРИЛОЖЕНИЕ А. Отличия исполнений ВПУ .....</b>	<b>23</b>
<b>ПРИЛОЖЕНИЕ Б. Аутентификация в различных типах соединений «СПОДЭС». ....</b>	<b>24</b>

## ПОДГОТОВКА К ПОДКЛЮЧЕНИЮ

Для подготовки подключения к ВПУ необходимо установить ПО MeterTools с официального сайта ООО «МИРТЕК»:

<https://mirtekgroup.com/produkcija/programmnoe-obespechenie/metertools>

При каждом запуске программа будет проверять обновление при наличии подключения к сети Интернет. При необходимости можно запустить обновление вручную (рисунок 1.1).

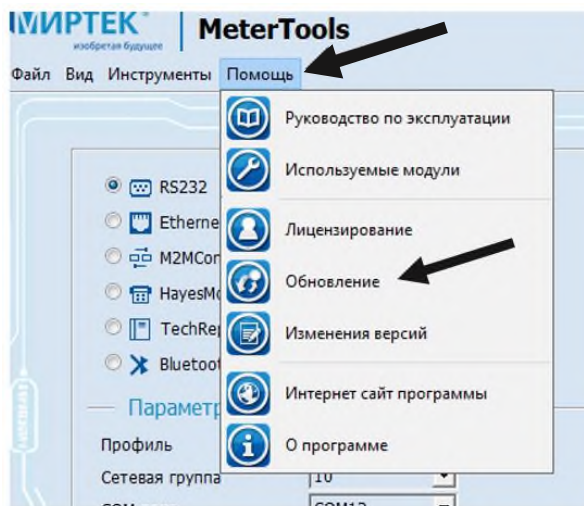


Рисунок 1.1 – Функция обновления в ПО «MeterTools»

Для подключения к высоковольтному прибору учета (ВПУ) МИРТЕК-135-РУ, **если он еще не установлен на ЛЭП**, необходимо подать питание на первый блок измерительный (БИ1). Для подачи питания по USB и установки SIM-карты крышка модуля связи блока БИ1 должна быть в снятом состоянии (рисунок 1.2 а, б). Питание необходимо подать через кабель mini USB (male) – USB-A (male), поставляемый в комплекте (рисунок 1.2 в). Если ваша модель ВПУ содержит GSM модуль в каждом измерительном блоке, то следует подать питание на оба измерительных блока (БИ1 и БИ2, рисунок 1.2 г).

В один измерительный блок ВПУ можно установить до 2 SIM-карт одновременно. Если ваша модель ВПУ содержит сменный модуль связи (показан на рисунке в приложении А), то установите SIM-карту и настройте его в соответствии с инструкцией МИРТ.411152.205 ИМ4.

Питание ВПУ может осуществляться: от блока питания для зарядки мобильного телефона, внешнего аккумулятора по типу Power Bank. Для питания одного блока устройства необходим источник питания постоянного напряжения +5В,

способный отдавать не менее 1А. Возможна подача питания от разъема USB компьютера, но надо иметь ввиду, что мощности может оказаться недостаточно.

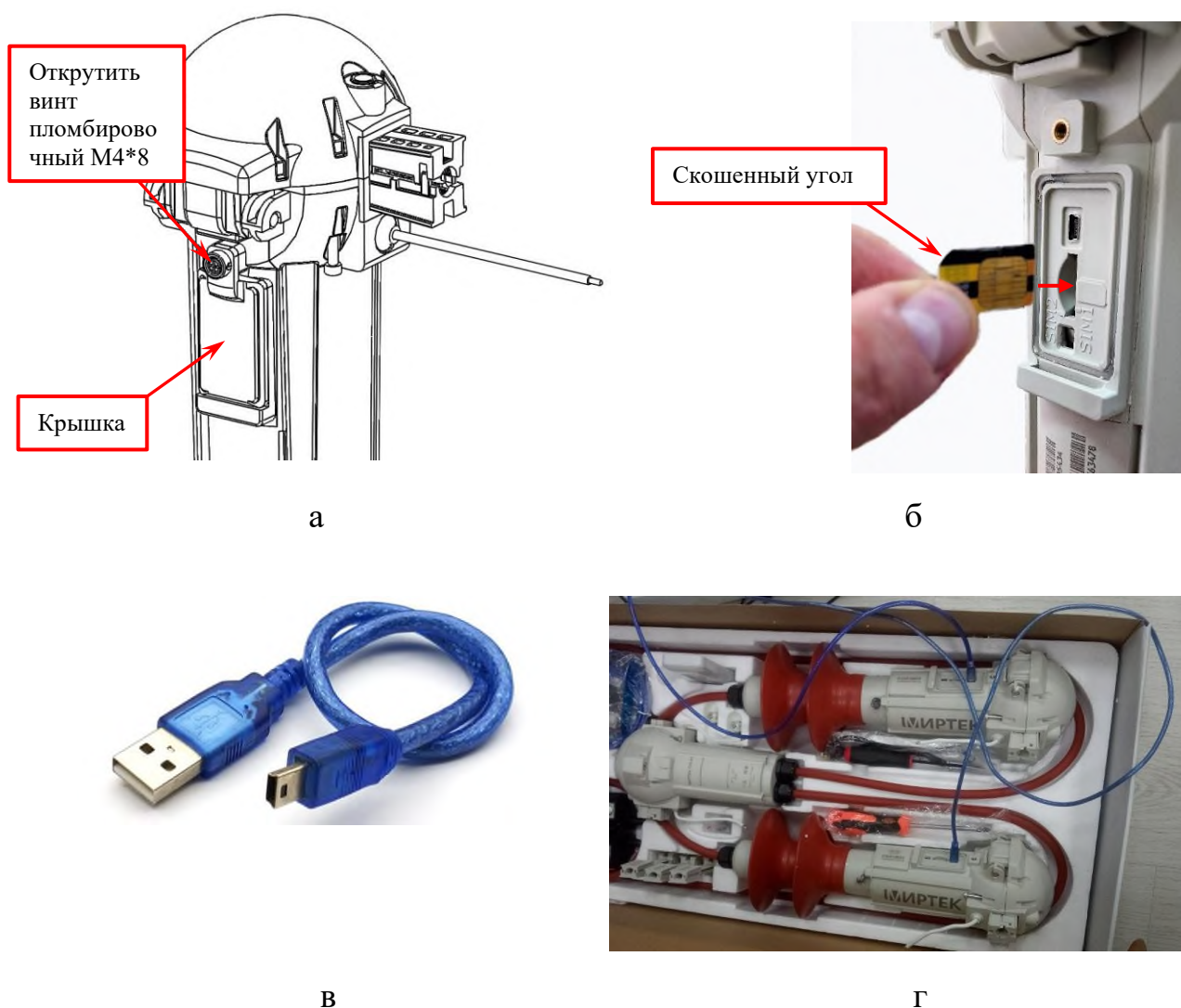


Рисунок 1.2. Необходимые действия для подключения:

- а – снять крышку модуля связи на БИ1 (БИ2);
- б – вставить SIM карту, если необходим GSM канал связи;
- в – взять кабель mini-USB из комплекта поставки;
- г – подключить питание к БИ1 через кабель mini-USB, в случае наличия модулей связи в обоих блоках подключить питание к БИ2 с помощью второго кабеля.

Интерфейс программы MeterTools для подключения к ВПУ показан на рисунке 1.3. В рабочем окне необходимо ввести необходимые для подключения данные, которые разбиты на 4 тематических блока: 1) канал связи; 2) параметры канала; 3) параметры опроса; 4) параметры подключения.

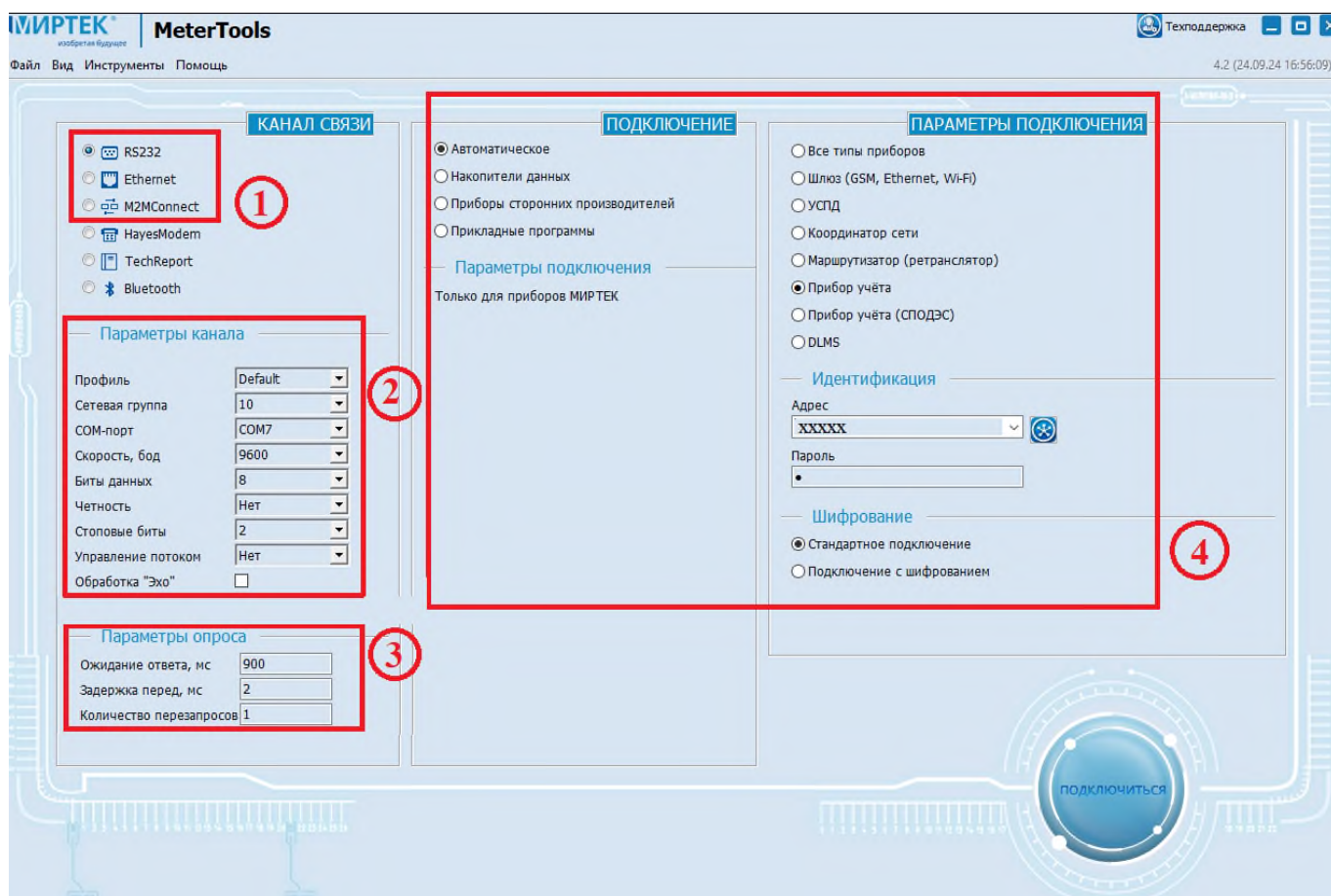


Рисунок 1.3. Интерфейс программы «MeterTools» для подключения к ВПУ, необходимо указать: 1) канал связи (п. 1);

2) параметры канала (п. 2);

3) параметры опроса (п. 3);

4) параметры подключения (п. 4.1 или п. 4.2).

## 1 ВЫБОР КАНАЛА СВЯЗИ

Шаг 1 при подключении к ВПУ – указать доступный канал связи. ВПУ поддерживает 3 канала связи для передачи данных и конфигурирования:

- RF433 (условное название RS232), п. 2.1;
- GSM dynamic IP SIM-card (условное название M2M), п. 2.2;
- GSM static IP SIM-card (условное название Ethernet), п. 2.3.

## 2 ПАРАМЕТРЫ КАНАЛА СВЯЗИ

Шаг 2 при подключении к ВПУ – указать параметры выбранного канала связи.

### 2.1 Параметры канала связи RF433 и мастер считывания данных МИРТ-141

2.1.1 Канал связи RF433 рассчитан на расстояние до 100 м между компьютером и ВПУ при условии прямой видимости.

2.1.2 Вставить в USB-порт ПК мастер считывания данных МИРТ-141, поставляемый опционально вместе с ВПУ МИРТЕК-135-РУ (рисунок 2.1). Мастер считывания дополнительно может быть укомплектован антенной, увеличивающей стабильность и дальность приема / передачи данных. Если комплектация вашего прибора не предусматривает наличие мастера считывания, то вы можете подключиться к прибору по каналу GSM (п.2.2-2.3).



Рисунок 2.1 – Мастер считывания данных по RF433 МИРТ-141.

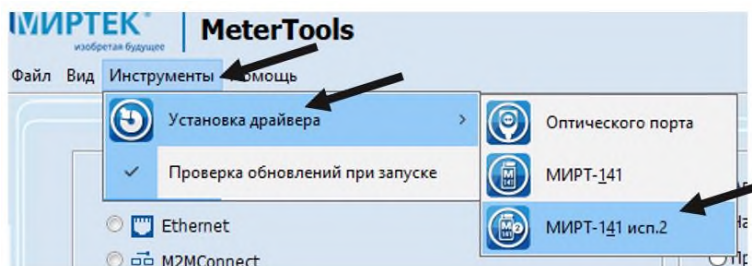


Рисунок 2.2 – Установка драйвера МИРТ-141.

2.1.3 При первом запуске необходимо установить драйвер «МИРТ-141 исполнение 2» (рисунок 2.2), если на самом мастере считывания есть маркировка «исполнение 2». В ином случае, установить основной драйвер «МИРТ-141».

2.1.4 Выбрать в разделе «Канал связи» опцию с условным обозначением «RS232», которая в программе «MeterTools» отвечает за связь по RF433.

2.1.5 В разделе «Параметры канала» выбрать из раскрывающегося списка COM-порт, который определила операционная система для МИРТ-141.

2.1.6 Для параметра «Сетевая группа» выбрать из раскрывающегося списка значение «10» либо режим «Авто», рисунок 1.3, шаг 2.

## **2.2 Параметры канала связи GSM с SIM-картой с динамическим IP-адресом**

- 2.2.1 Для подключения с помощью GSM и SIM-карты с динамическим IP-адресом необходимо, чтобы как минимум одна активная SIM-карта с динамическим IP-адресом была вставлена в слот ведущего измерительного блока (рисунок 1.2 б).
- 2.2.2 В меню «Каналы связи» необходимо выбрать опцию с условным обозначением «M2MConnect», которая отвечает за подключение по GSM с динамическим IP-адресом.
- 2.2.3 В меню «Параметры канала» ввести данные: номер шлюза из формуляра, IP адрес сервера – по умолчанию 46.45.246.48 (сервер 1) или 213.222.245.173 (сервер 2, резервный), порт подключения – по умолчанию 10000 (рисунок 2.3 а).

## **2.3 Параметры канала связи GSM с SIM-картой со статическим IP-адресом**

- 2.3.1 Для подключения с помощью GSM и SIM-карты со статическим IP-адресом необходимо вставить по меньшей мере одну активную SIM-карту со статическим IP-адресом в первый слот ведущего измерительного блока.
- 2.3.2 Необходимо узнать у оператора фактический IP-адрес своей SIM-карты, либо определить его с помощью «Meter tools» путем подключения по п.2.1 или п.2.2 и считывания данных (рисунок 4.3).
- 2.3.3 Запустить приложение «Meter Tools», открыв программу в новом окне.
- 2.3.4 В меню «Каналы связи» выбрать опцию с условным обозначением «Ethernet», которая отвечает за подключение по GSM со статическим IP-адресом.
- 2.3.5 В меню «Параметры канала», если было соединение по RS232 программа обычно заполняет параметры автоматически. В другом случае заполнить данные из формуляра. «Порт подключения» по умолчанию равен 10000 (рисунок 2.3 б).



а

б

Рисунок 2.3 – Пример ввода параметров канала для подключения по GSM с: динамическим IP-адресом (а), статическим IP-адресом (б).

### 3 ПАРАМЕТРЫ ОПРОСА

Шаг 3 при подключении к ВПУ – указать параметры опроса. Для этого в разделе «Параметры опроса» (рисунок 1.3, шаг 3) рекомендуется ввести значения:

- в поле «Ожидание ответа» – от 900 мс для RF433 и от 5000 мс для GSM;
- в поле «Задержка перед» – 0 мс,
- в поле «Количество перезапросов» – от 2.

При плохом уровне сигнала «Ожидание ответа» возрастает. Конкретное значение определяется эмпирическим путем, т.к. зависит от условий связи в месте установки ВПУ.

### 4 ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ

Шаг 4 при подключении к ВПУ – указать параметры подключения.

Сначала следует выбрать протокол подключения (рисунок 4.0). Для этого посмотрите полное наименование вашей модели ВПУ (указано в формуляре). Если присутствует символ:

- «P1» – доступен протокол DLMS/COSEM/СПОДЭС;
- «P2» – доступны протоколы «МИРТЕК» и DLMS/COSEM/СПОДЭС.



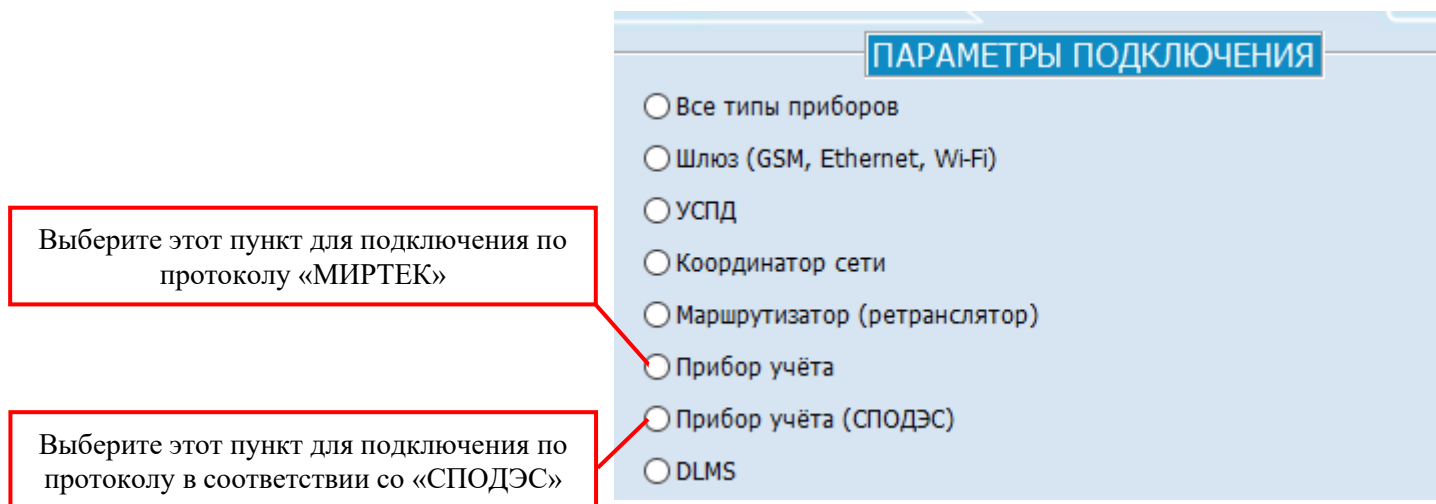


Рисунок 4.0. Выбор протокола подключения.

#### 4.1 ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ ПО ПРОТОКОЛУ «МИРТЕК» (для исполнений ВПУ с символом «P2» в полном наименовании)

- 4.1 Для подключения к ВПУ по протоколу «МИРТЕК» в разделе «Подключение» выбрать «Автоматическое», а в разделе «Параметры подключения» – «Прибор учета».
- 4.2 В подразделе «Идентификация» в поле «Адрес» указать последние **5 цифр** заводского номера ВПУ (на корпусе прибора маркированы 6 последних цифр заводского номера, заводской номер указан также в формуляре).
- 4.3 В поле «Пароль» указать пароль, записанный в формуляре (по умолчанию «0»).
- 4.4 После ввода необходимых параметров (пример на рисунок 4.1) нажать кнопку «Подключиться».
- 4.5 Рассмотрим конкретный пример считывания данных и изменения пароля при подключении по протоколу «МИРТЕК» с использованием любого из каналов связи. Считаем данные об уровне сигнала и настройках GSM модуля прибора.
- 4.6 После подключения в меню «Настройки» слева выбрать «GSM».
- 4.7 В конце списка настроек нажать «Считать все» (рисунок 4.2).
- 4.8 Результат считывания IP-адреса SIM-карты отобразится в строке «IP адрес шлюза в GPRS» (рисунок 4.3).

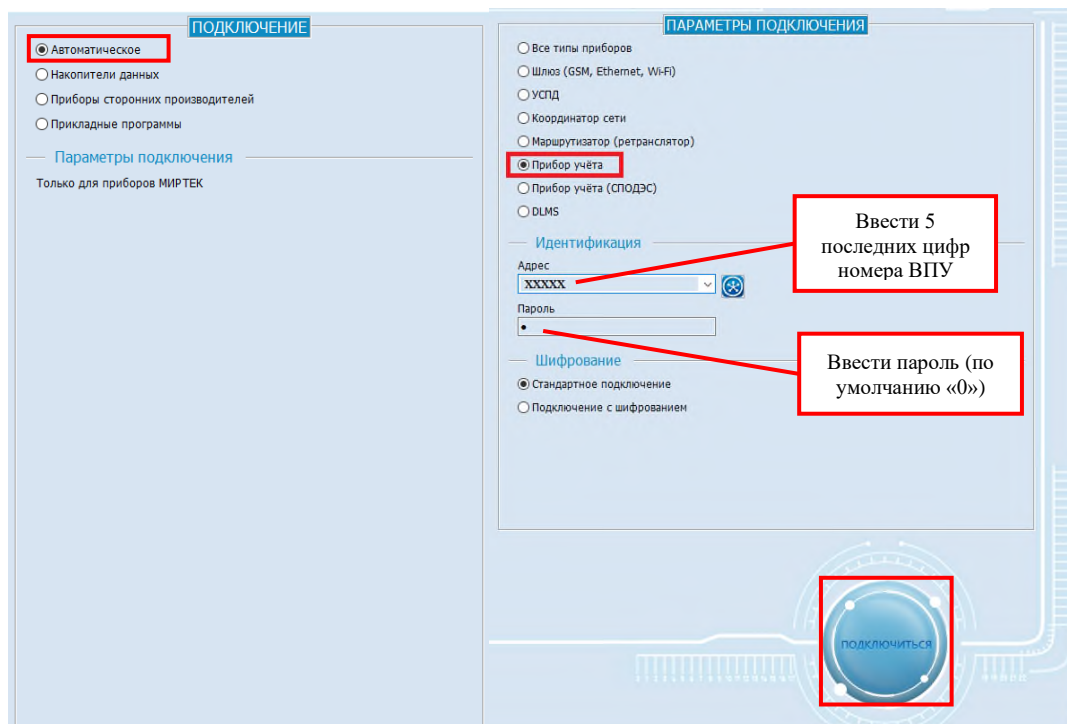


Рисунок 4.1 Параметры подключения по протоколу «МИРТЕК».

4.9 В списке параметров найти «Уровень сигнала активной SIM-карты» и нажать кнопку «Считать». При устойчивом соединении значение находится в диапазоне от – 78 до 0.

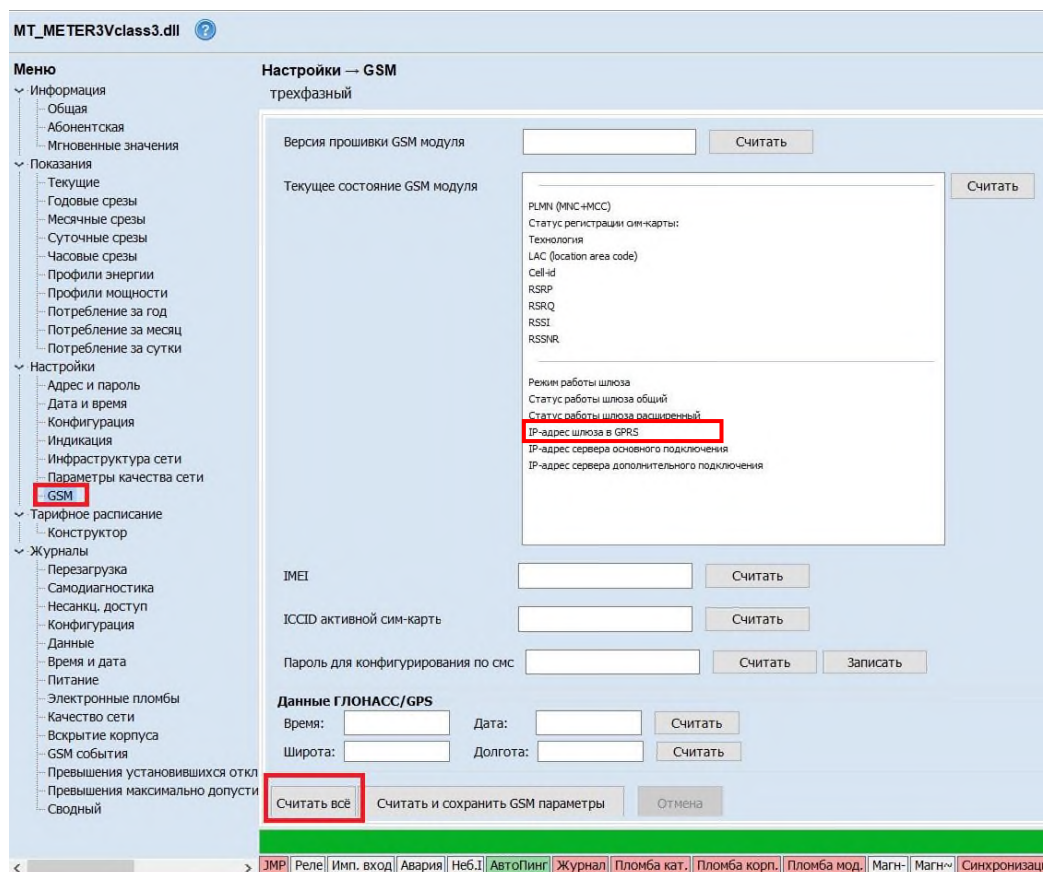


Рисунок 4.2 – Считывание данных о настройках GSM модуля прибора.

Версия прошивки GSM модуля: EG91EXGAR08A05M1 [Считать]

Текущее состояние GSM модуля [Считать]

PLMN (MNC+MCC)	25099
Статус регистрации сим-карты:	зарегистрирована
Технология	GSM compact
LAC (location area code)	0x00
Cell-id	0x0000
RSRP	0
RSRQ	0
RSSI	0
RSSNR	0

Режим работы шлюза: сервер

Статус работы шлюза общий: подключение активно

Статус работы шлюза расширенный: 27

**IP-адрес шлюза в GPRS: 85.115.236.XX**

IP-адрес сервера основного подключения: 213.222.245.173

IP-адрес сервера дополнительного подключения: 0.0.0.0

IMEI: 8667280635271XX [Считать]

ICCID активной сим-карты: 89701991902270293XX [Считать]

Пароль для конфигурирования по смс: 123456XX [Считать] [Записать]

Данные ГЛОНАСС/GPS

Время: 10:35:52 Дата: 03.11.2022 [Считать]

Рисунок 4.3 – Считывание статического IP-адреса.

- 4.10 Если используется 2 SIM-карты, то выбрать номер нужной в раскрывающихся списках «Активная SIM-карта» и «Приоритет SIM-карты». Подтвердить выбор нажатием кнопки «Записать».
- 4.11 Задание нового пароля для подключения к ВПУ производится на вкладке «Адрес и пароль», рисунок 4.4.

MT\_METER3Vclass3.dll ?

Меню

- Информация
  - Общая
  - Абонентская
  - Мгновенные значения
- Показания
  - Текущие
  - Годовые срезы
  - Месячные срезы
  - Суточные срезы
  - Часовые срезы
  - Профили энергии
  - Профили мощности
  - Потребление за год
  - Потребление за месяц
  - Потребление за сутки
- Настройки
  - Адрес и пароль**
  - Дата и время
  - Конфигурация
  - Индикация
  - Инфраструктура сети
  - Параметры качества сети
  - GSM
- Тарифное расписание
  - Конструктор

Настройки → Адрес и пароль

МИРТЕК-135-PY-SPHV1-A0,5R1-10K-5-100A-RGC2-RF433/1-G/1-RF2400/6-P2-HMV4-D, трехфаз:

**Изменение адреса**

Новый адрес устройства: 17193 [Изменить]

**Изменение паролей**

Текущий пароль доступа: [ ]

☒ скрывать символы паролей

**Основной пароль**

Новый пароль: [ ] [Записать]

Повтор пароля: [ ]

**Дополнительный пароль**

Новый пароль: [ ] [Записать]

Повтор пароля: [ ]

**Сброс паролей**

Сброс работает только при снятой клеммной крышке [Сбросить]

**Дополнительные настройки безопасности**

Количество попыток ввода пароля (0 - отключено): [ ] [Считать] [Записать]

☐ требовать пароль для считывания абонентских данных [Считать] [Записать]

☐ проверка пароля для всех типов команд "МИРТЕК" [Считать] [Записать]

Рисунок 4.4 – Задание нового пароля.

## 4.2 ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ ПО «СПОДЭС»

(для исполнений ВПУ с символом «Р1» в полном наименовании)

### 4.2.1 Общие сведения

Настоящая инструкция содержит сведения, необходимые для установления защищенного соединения с ВПУ «МИРТЕК-135-РУ» с применением программы «Meter Tools» в соответствии со стандартом СТО 34.01-5.1-006-2023 «Приборы учёта электрической энергии. Требования к информационной модели обмена данными».

Примечание – ВПУ может выпускаться в различных исполнениях, общая информация о которых содержится в Описании типа СИ. Дополнительно необходимо ознакомиться с отличиями исполнений ВПУ, приведенными в приложении А.

4.2.1.1 Программа «MeterTools» позволяет выполнить подключение к прибору учета по «СПОДЭС». Для этого в разделе меню «Параметры подключения» необходимо выбрать «**Прибор учета (СПОДЭС)**», рисунок 4.5.

4.2.1.2 В подразделе «Идентификация» в поле «Адрес» необходимо указать последние **4 цифры** заводского номера ВПУ (на корпусе прибора маркированы 6 последних цифр заводского номера, также заводской номер указан в формуляре).

4.2.1.3 В подразделе «Тип соединения» необходимо указать один из трёх доступных типов в зависимости от целей подключения:

- **публичный клиент:** минимальный доступ на чтение, запись и выполнение методов запрещены, беспарольный доступ для проверки наличия подключения к ВПУ;
- **считыватель показаний:** доступ для всех объектов на чтение разрешён, разрешён метод для коррекции времени на +/- 900 секунд в сутки для объекта «Часы» для опроса ВПУ;
- **конфигуратор:** полный доступ ко всем объектам для опроса и настройки ВПУ.

Общее описание аутентификации для каждого типа соединения приведено в таблице в приложении Б.

4.2.1.4 Доступ к параметрам и данным со стороны интерфейсов связи защищен паролями на чтение и запись. По умолчанию установлены следующие пароли:

- пароль **низкой** секретности – **12345678** для типа соединения «Считыватель данных»;
- пароль **высокой** секретности – **MeterCorporation** для типа соединения «Конфигуратор».

4.2.1.5 В разделе меню «Доступ» для подключения предоставляется 4 варианта политики безопасности (рисунок 4.9):

- стандартный (установлен по умолчанию),
- с проверкой подлинности,
- с шифрованием,
- с проверкой подлинности и шифрованием.

Дополнительно предоставляется 2 варианта комплекта безопасности:

- AES-GCM-128 (установлен по умолчанию),
- KUZN-CTR-CMAC (ГОСТ 34.12-2018 «Кузнечик»).

Настройка комплекта и политики безопасности описана в п.4.2.5.2 - 4.2.5.3.

#### **4.2.2 Тип соединения «ПУБЛИЧНЫЙ КЛИЕНТ»**

Для соединения «Публичный клиент» в разделе «Подключение» указать «Автоматическое», рисунок 4.1, в разделе «Параметры подключения» указать «Прибор учета СПОДЭС», в поле «Идентификация» – адрес в виде четырех последних цифр номера ВПУ, в строке тип соединения выбрать «Публичный клиент», рисунок 4.5.

После подключения для считывания доступна только общая информация: дата и время устройства, логическое имя, включающее зав. номер ВПУ (рисунок 4.6).

**ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ**

☐ Все типы приборов  
☐ Шлюз (GSM, Ethernet, Wi-Fi)  
☐ УСПД  
☐ Координатор сети  
☐ Маршрутизатор (ретранслятор)  
☐ Прибор учёта  
☒ **Прибор учёта (СПОДЭС)**  
☐ DLMS

**Тип соединения**

☒ **Публичный клиент**  
☐ Считыватель данных  
☐ Конфигуратор

**Идентификация**

Адрес: XXXX

Ввести последние 4 цифры номера ВПУ

Рисунок 4.5. Соединение «Публичный клиент».

MT\_SPODES.dll

Канал связи

Меню: Информация, Настройки

Информация — Общая

Дата и время	30.08.2024 15:04:12
Время ПК	30.08.2024 15:04:14
Расхождение времени	01 сек
Автопереход на зимнее/летнее время	
Режим подключения	Публичный клиент
Предупреждение	Внимание, в режиме подключения "публичный клиент" функционал ограничен!

Логическое имя устройства	MBT4220291817193
Сетевой адрес	7193
Версия спецификации СПОДЭС	

Рисунок 4.6. Вид меню при типе соединения «Публичный клиент».

### 4.2.3 Тип соединения «СЧИТЫВАТЕЛЬ ДАННЫХ»

Тип соединения «Считыватель данных», как следует из названия, дает возможность считывать данные из ВПУ и устанавливать сдвиг времени. Тип соединения «Считыватель данных» имеет четыре варианта политики безопасности.

Для соединения «Считыватель данных» в разделе «Подключение» указать «Автоматическое», рисунок 4.1, в разделе «Параметры подключения» указать «Прибор учета СПОДЭС», в поле «Идентификация» – адрес в виде четырех последних цифр номера ВПУ, в строке тип соединения выбрать «Считыватель данных», рисунок 4.7.

#### 4.2.3.1 Вариант политики безопасности «Стандартный»

По умолчанию ВПУ настроен на вариант политики безопасности «Стандартный».

В варианте «Стандартный» в поле «Идентификация» необходимо указать адрес – последние **4 цифры** серийного номера ВПУ и пароль **низкой** секретности – **12345678**.

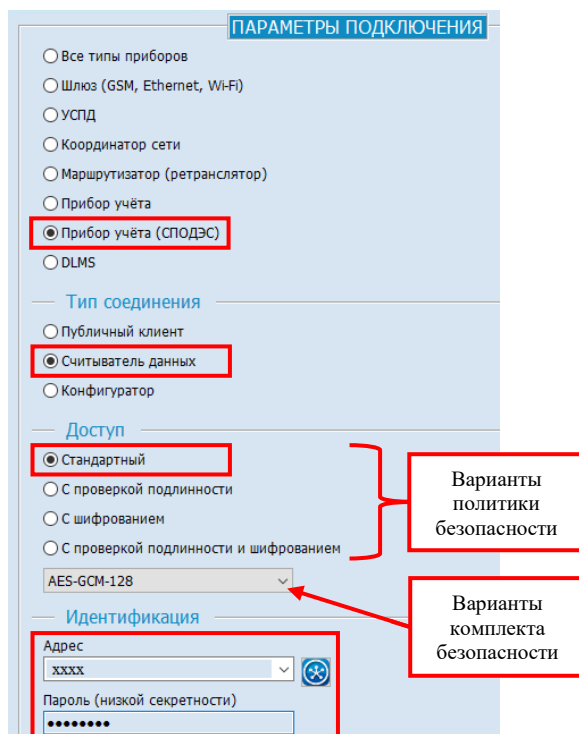


Рисунок 4.7. Соединение «Считыватель данных», вариант доступа «Стандартный».

#### 4.2.3.2 Варианты политики безопасности «С проверкой подлинности», «С шифрованием», «С проверкой подлинности и шифрованием»

В типе соединения «Считыватель данных» варианты политик безопасности «С проверкой подлинности» или «С шифрованием» или «С проверкой подлинности и шифрованием» применимы только к ВПУ со встроенным модулем связи (см. приложение А). Для активации любого из этих вариантов необходимо в поле «Идентификация» указать (рисунок 4.8):

- Адрес – последние **4 цифры** серийного номера ВПУ;
- пароль **низкой** секретности – **12345678**;
- одноадресный ключ шифрования для **низкой** секретности:  
по AES-GCM-128 – **UnicastKeyLLS001**,



по KUZN-CTR-CMAC – 00000000000000000000000000000001.

- ключ аутентификации для **низкой** секретности:

по AES-GCM-128 – AuthKeyLLS000001,

по KUZN-CTR-CMAC – UnicastKeyLLS00000000000000000000.

The figure consists of three side-by-side screenshots of a software interface titled 'ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ' (Connection Parameters). Each screenshot shows the same configuration options, but with different security settings highlighted by red boxes:

- а (left):** The 'Доступ' (Access) section has 'С проверкой подлинности' (With authentication) selected. The 'Идентификация' (Authentication) section has 'Адрес' (Address) set to 'xxxx'.
- б (middle):** The 'Доступ' section has 'С шифрованием' (With encryption) selected. The 'Идентификация' section has 'Адрес' set to 'xxxx'.
- в (right):** The 'Доступ' section has 'С проверкой подлинности и шифрованием' (With authentication and encryption) selected. The 'Идентификация' section has 'Адрес' set to 'xxxx'.

Common settings across all three screenshots include: 'Тип соединения' (Connection type) set to 'Считыватель данных' (Data reader), 'Доступ' (Access) set to 'Стандартный' (Standard), and 'Идентификация' (Authentication) set to 'AES-GCM-128'.

а

б

в

Рисунок 4.8. Тип соединения «Считыватель данных», варианты доступа:

а - «С проверкой подлинности»,

б - «С шифрованием»,

в - «С проверкой подлинности и шифрованием».

#### 4.2.4 Тип соединения «КОНФИГУРАТОР»

Для соединения типа «Конфигуратор» используется механизм аутентификации высокого уровня безопасности.

Тип соединения «Конфигуратор» помимо считывания данных, предоставляет возможность настройки параметров ВПУ. В этом типе соединения существует четыре варианта политики безопасности.

Для соединения «Конфигуратор» в разделе «Подключение» указать «Автоматическое», рисунок 4.1, в разделе «Параметры подключения» указать «Прибор учета СПОДЭС», в поле «Идентификация» – адрес в виде четырех

последних цифр номера ВПУ, в строке тип соединения выбрать «Конфигуратор», рисунок 4.9.

#### 4.2.4.1 Вариант политики безопасности «Стандартный»

В варианте «Стандартный» в поле «Идентификация» необходимо указать адрес – последние 4 цифры номера ВПУ, и пароль **высокой** секретности – **MeterCorporation**.

ПАРАМЕТРЫ ПОДКЛЮЧЕНИЯ

☐ Все типы приборов

☐ Шлюз (GSM, Ethernet, Wi-Fi)

☐ УСПД

☐ Координатор сети

☐ Маршрутизатор (ретранслятор)

☐ Прибор учёта

☒ Прибор учёта (СПОДЭС)

☐ DLMS

Тип соединения

☐ Публичный клиент

☐ Считыватель данных

☒ Конфигуратор

Доступ

☒ Стандартный

☐ С проверкой подлинности

☐ С шифрованием

☐ С проверкой подлинности и шифрованием

AES-GCM-128

Идентификация

Адрес

xxxx

Пароль (высокой секретности)

.....

Варианты политики безопасности

Варианты комплекта безопасности

Рисунок 4.9. Тип соединения «Конфигуратор», вариант политики безопасности «Стандартный».

#### 4.2.4.2 Варианты политики безопасности «С проверкой подлинности», «С шифрованием», «С проверкой подлинности и шифрованием»

В типе соединения «Конфигуратор» при выборе варианта «С проверкой подлинности» или «С шифрованием» или «С проверкой подлинности и шифрованием» в поле «Идентификация» необходимо указать (рисунок 4.10):

- адрес – последние 4 цифры серийного номера,
- пароль **высокой** секретности – **MeterCorporation**,
- одноадресный ключ шифрования для **высокой** секретности:  
по AES-GCM-128 – **UnicastKeyHLS001**,

по KUZN-CTR-CMAC – **UnicastKeyHLS00000000000000000000.**

в - «С проверкой подлинности и шифрованием».

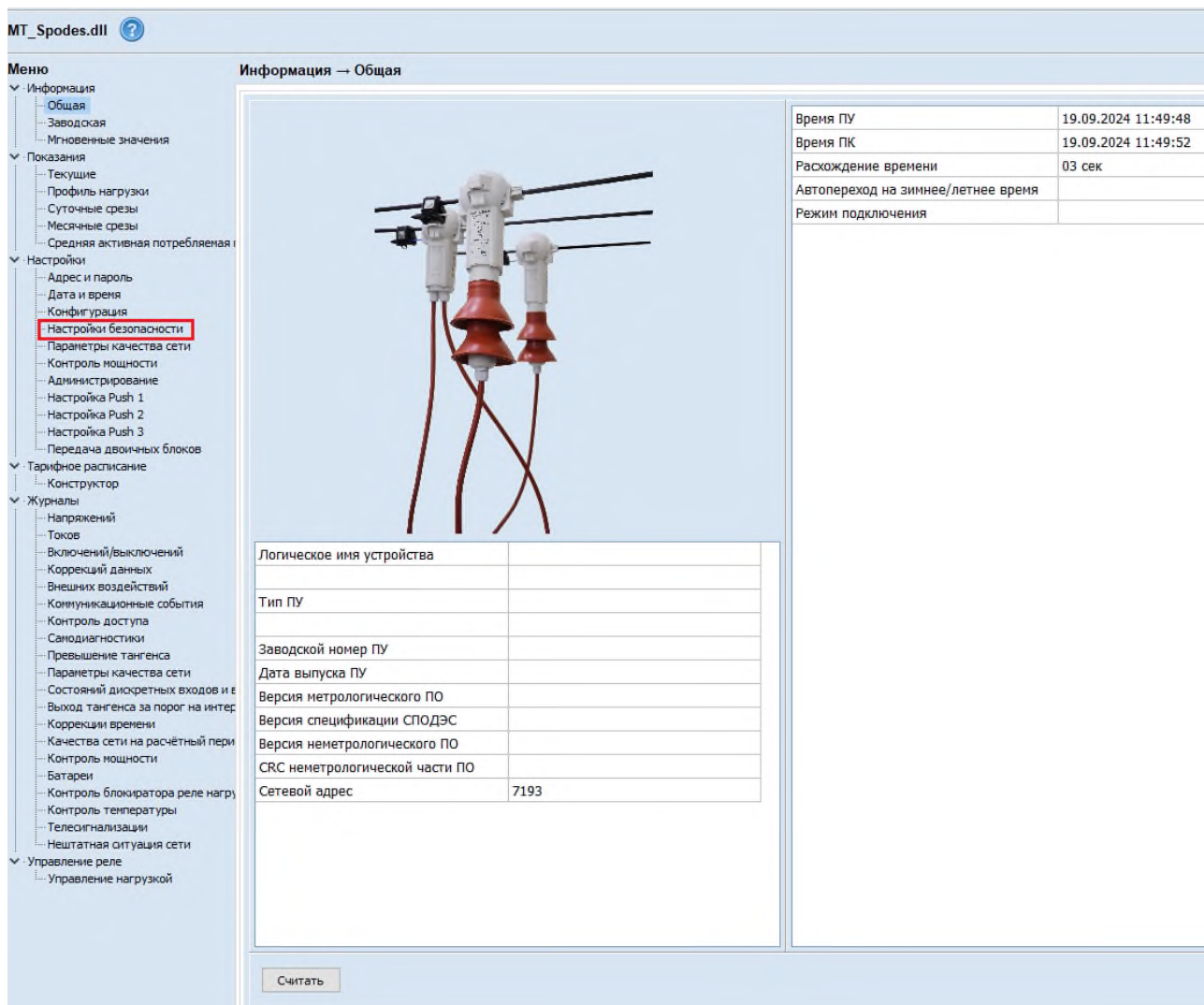


Рисунок 4.11. Рабочий интерфейс после подключения с типом соединения «Считыватель данных» или с типом соединения «Конфигуратор». Примечание — вкладка «Настройки безопасности» доступна только в типе соединения «Конфигуратор».

## Конфигуратор

Порог фиксации воздействий на сеть	Считать	Записать
Порог для фиксации превышения тангенса нагрузки	0,9	Записать
Порог для фиксации коэффициента несимметрии напряжений		Записать
Порог для фиксации провала напряжения		Записать
Согласованное напряжение питания		Записать
Пороговое напряжение для фиксации перерыва питания		Записать
Порог для фиксации перенапряжения		Записать
Порог отклонения частоты		Записать

а

## Считыватель данных

Порог фиксации воздействий на сеть	Считать	Записать
Порог для фиксации превышения тангенса нагрузки	0,9	Считать
Порог для фиксации коэффициента несимметрии напряжений		Считать
Порог для фиксации провала напряжения		Считать
Согласованное напряжение питания		Считать
Пороговое напряжение для фиксации перерыва питания		Считать
Порог для фиксации перенапряжения		Считать
Порог отклонения частоты		Считать

б

Настройки → Дата и время

Дата/время: 15:12:01, 29 августа 2024 г. Считать Записать Запись в устройство времени ПК

Девияция: 180

Часовой пояс, мин. 0 Считать Записать

Сдвиг времени, сек. 0 Записать

Дополнительно

☐ Переход часов на зимнее время Считать Записать

Источник времени Считать

в

Настройки → Дата и время

Дата/время: 0:00:00, 1 января 2014 г. Считать

Девияция:

Часовой пояс, мин. 0 Считать

Сдвиг времени, сек. 0 Записать

Дополнительно

☐ Переход часов на зимнее время Считать

Источник времени Считать

г

Настройки → Адрес и пароль

Текущие адрес и пароль

Адрес устройства Считать

Адрес клиентского подключения

Изменение пароля для доступа с низким уровнем безопасности

Новый пароль Записать

Изменение пароля доступа с высоким уровнем безопасности

Новый пароль Записать

д

Настройки → Адрес и пароль

Текущие адрес и пароль

Адрес устройства Считать

Адрес клиентского подключения

е

Рисунок 4.12. Рабочий интерфейс некоторых вкладок с настройками: (а), (в), (д) – при типе соединения «Конфигуратор», (б), (г), (е) – тех же вкладок при типе соединения «Считыватель данных».

## 4.2.5 НАСТРОЙКА ПАРАМЕТРОВ ДОСТУПА И ШИФРОВАНИЯ

### 4.2.5.1 Настройка паролей

При подключении с типом соединения «Конфигуратор» доступна настройка параметров, в том числе параметров безопасности.

Пароли низкой и высокой секретности могут быть изменены пользователем, как показано на рисунок 4.13.

Минимальная длина паролей как низкой, так и высокой секретности составляет 1 символ. Максимальная длина паролей низкой и высокой секретности составляет 16

символов. Могут использоваться прописные латинские буквы, строчные латинские буквы, цифры, спецсимволы.

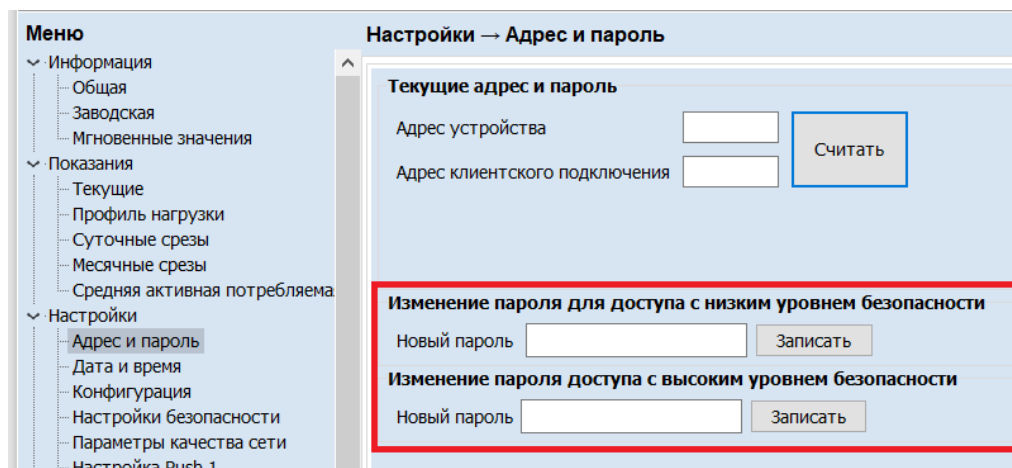


Рисунок 4.13. Задание паролей.

#### 4.2.5.2 Настройка комплекта безопасности

На вкладке «Настройки безопасности» предоставляется возможность задать один из двух комплектов безопасности: AES-GCM-128 (установлен по умолчанию) или KUZN-CTR-CMAC. Выбор необходимо сопровождать нажатием кнопки «Записать» (рисунок 4.14).

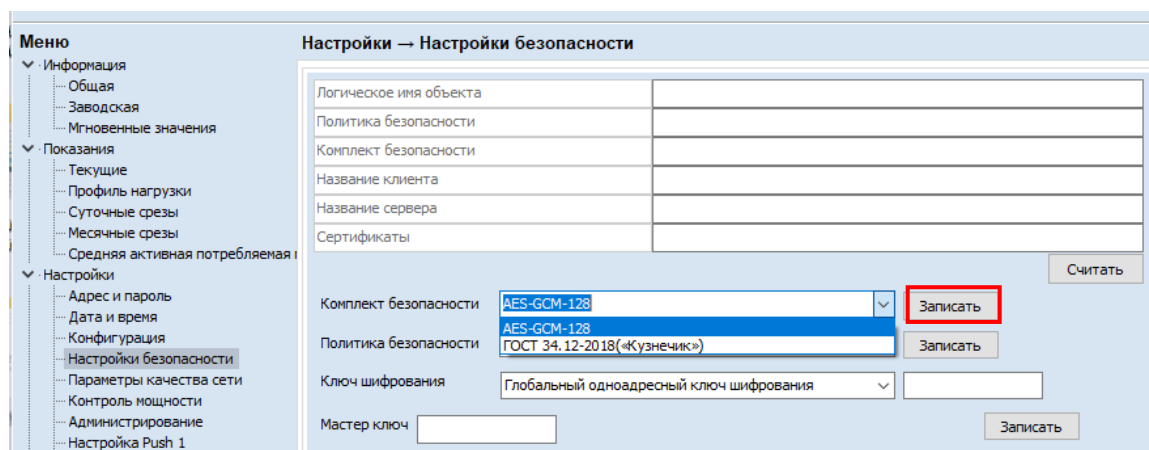


Рисунок 4.14. Настройка комплекта безопасности.

### 4.2.5.3 Настройка политики безопасности

По умолчанию в ВПУ задан вариант политики безопасности «Стандартный».

На вкладке «Настройки безопасности» в строке «Политика безопасности» можно установить один из 4 вариантов доступа (рисунок 4.15):

- стандартный;
- с проверкой подлинности;
- с шифрованием;
- с проверкой подлинности и шифрованием.

После выбора варианта политики безопасности нажмите «Записать».

Меню

- Информация
  - Общая
  - Заводская
  - Мгновенные значения
- Показания
  - Текущие
  - Профиль нагрузки
  - Суточные срезы
  - Месячные срезы
  - Средняя активная потребляемая
- Настройки
  - Адрес и пароль
  - Дата и время
  - Конфигурация
  - Настройки безопасности**
  - Параметры качества сети
  - Контроль мощности
  - Администрирование
  - Настройка Push 1
  - Настройка Push 2

Настройки → Настройки безопасности

Логическое имя объекта	
Политика безопасности	
Комплект безопасности	
Название клиента	
Название сервера	
Сертификаты	

Считать

Комплект безопасности: AES-GCM-128

Политика безопасности: Стандартный

Ключ шифрования: Стандартный, С проверкой подлинности, С шифрованием, С проверкой подлинности и шифрованием

Мастер ключ:

Записать

Рисунок 4.15. Настройка политики безопасности.

### 4.2.5.4 Настройка ключей шифрования

Ключи шифрования, заданные по умолчанию, указаны в формуляре. Для того, чтобы изменить их необходимо обратиться за дополнительной инструкцией МИРТ.411152.205ИМ7 в службу технической поддержки МИРТЕК любым из нижеперечисленных способов:

- по телефону: +7(988)7000123;
- по электронной почте: support@mirtekgroup.ru.



## ПРИЛОЖЕНИЕ А. Отличия исполнений ВПУ

	Исполнения со встроенным модулем связи	Исполнения со сменным модулем связи
		
1. При первом подключении к ВПУ	Вариант политики безопасности «Стандартный» включается независимо от вашего выбора в подразделе в «Параметры подключения». Т.е. попытка выбрать другие режимы доступа пока не будет произведена настройка доступа через тип соединения «Конфигуратор» (см п.6) не даст результатов.	Можно выбрать любой вариант политики безопасности, и он сразу же будет функционировать в полном объеме.
2. Политика безопасности при типе соединения «Считыватель данных»	Имеется 4 варианта политики безопасности: 1. Стандартный 2. С проверкой подлинности 3. С шифрованием 4. С проверкой подлинности и шифрованием.	Имеется только вариант «Стандартный» (согласно версии 4 стандарта СТО 34.01-5.1-006-2023).
3. Выбор политики безопасности	Можно выбрать любую политику безопасности: «Стандартный» (включен по умолчанию), «С проверкой подлинности», «С шифрованием», «С проверкой подлинности и шифрованием». После выбора режима шифрования на вкладке «Настройка безопасности» и нажатия кнопки «Записать» подключение к ВПУ будет происходить только в выбранном варианте политики безопасности независимо от пользовательских установок в графе «Параметры подключения → Доступ» при подключении.	Каждая политика безопасности может быть заменена на следующую, т.е. если в ВПУ установлена политика безопасности "Стандартная", то к прибору можно подключиться, используя любую из 4 политик безопасности. Если прибор настроен на политику безопасности с проверкой подлинности, то к нему можно подключиться с использованием одноименной политики безопасности, а также двух последующих.

	Исполнения со встроенным модулем связи	Исполнения со сменным модулем связи
4. Версия СПОДЭС	2.0	4.0
5. Смена паролей	Отсутствуют ограничения	Нельзя изменить пароли на те, которые были использованы ранее, глубина – 3 пароля.
6. Доступные каналы связи при подключении по СПОДЭС	GSM	RF433, GSM

### ПРИЛОЖЕНИЕ Б. Аутентификация в различных типах соединений «СПОДЭС».

	Тип соединения	Публичный клиент	Считыватель данных				Конфигуратор			
	Права	Ограниченное считывание	Считывание				Считывание и изменение настроек			
	Доступ		Стандартный	С проверкой подлинности	С шифрованием	С проверкой подлинности с шифрованием	Стандартный	С проверкой подлинности	С шифрованием	С проверкой подлинности с шифрованием
Аутентификация	Пароль (низкой секретности)	–	+	+	+	+	–	–	–	–
	Одноадресный ключ (низкой секретности)	–	–	+	+	+	–	–	–	–
	Ключ аутентификации (низкой секретности)	–	–	+	+	+	–	–	–	–
	Пароль (высокой секретности)	–	–	–	–	–	+	+	+	+
	Одноадресный ключ (высокой секретности)	–	–	–	–	–	–	+	+	+
	Ключ аутентификации (высокой секретности)	–	–	–	–	–	–	+	+	+
	Адрес	Последние 4 цифры номера ВПУ								

\* для исполнений ВПУ со встроенным модулем связи, см. Приложение А.