

**ООО «МИРТЕК»**

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

**С КОМПЛЕКТОМ ШИН И ВНЕШНИМ БЛОКОМ**

**ИНСТРУКЦИЯ ПО ПОДКЛЮЧЕНИЮ  
ПО ИНТЕРФЕЙСАМ СВЯЗИ**

**RF433, GSM (M2MConnect, Ethernet), Bluetooth с помощью  
программы METER TOOLS 5 по СПОДЭС или протоколу  
МИРТЕК**

**МИРТ.411152.246ИМ3 (V1)**

**(ДОПОЛНЕНИЕ К МИРТ.411152.246 РЭ)**

# СОДЕРЖАНИЕ

<b>1 ПОДГОТОВКА К ПОДКЛЮЧЕНИЮ</b> .....	3
<b>2 ПОДКЛЮЧЕНИЕ ПО «СПОДЭС»</b> .....	6
2.1 Общие сведения.....	6
2.2 Идентификация в СПОДЭС - тип соединения «ПУБЛИЧНЫЙ КЛИЕНТ».....	7
2.3 Идентификация в СПОДЭС - тип соединения «СЧИТЫВАТЕЛЬ».....	8
2.4 Идентификация в СПОДЭС - тип соединения «КОНФИГУРАТОР» .....	9
2.4.1 Режим доступа «Стандартный» (включен по умолчанию).....	9
2.4.2 Режимы доступа «С проверкой подлинности», «С шифрованием», «С проверкой подлинности и шифрованием».....	9
2.5 Параметры подключения.....	11
2.6 Продвинутое настройки подключения.....	11
2.7 Настройка параметров доступа и шифрования.....	11
2.7.1 Настройка паролей .....	11
2.7.2 Настройка политики безопасности.....	12
2.7.3 Настройка комплекта безопасности.....	13
2.7.4 Настройка ключей шифрования.....	14
<b>3 ПОДКЛЮЧЕНИЕ ПО ПРОТОКОЛУ «МИРТЕК»</b> .....	14
3.1 Общие сведения.....	14
3.2 Идентификация в протоколе МИРТЕК .....	14
3.3 Параметры подключения.....	15
3.4 Параметры шифрования.....	15
<b>4 КАНАЛЫ СВЯЗИ</b> .....	16
4.1 RF433 и мастер считывания данных МИРТ-141 .....	16
4.2 GSM с SIM-картой с динамическим или статическим IP-адресом (M2MConnect) .....	17
4.3 GSM с SIM-картой со статическим IP-адресом (Ethernet) .....	18
4.4 Bluetooth.....	19
<b>5 ПОДКЛЮЧЕНИЕ СО СМАРТФОНА</b> .....	21
<b>ПРИЛОЖЕНИЕ А. Аутентификация в различных типах соединений «СПОДЭС»</b> .....	23
<b>ПРИЛОЖЕНИЕ Б. Ключи шифрования в «СПОДЭС»</b> .....	24

# 1 ПОДГОТОВКА К ПОДКЛЮЧЕНИЮ

## 1.1 Подготовка прибора

Если высоковольтный прибор учета (далее - ВПУ) МИРТЕК-135-РУ с комплектом шин и внешним блоком уже установлен в ячейку распределительного устройства (РУ) в рабочую сеть передачи электроэнергии, то его питание осуществляется в штатном режиме и подключения дополнительного питания не требуется. Если же ВПУ еще не установлен в ячейку РУ, необходимо подать питание на блоки измерительные (БИ1 и БИ2) по USB. Крышка отсека (рис. 1.2 а) должна быть в снятом состоянии (рис. 1.2 б). Питание необходимо подать через кабели USB type-C, поставляемые в комплекте (рис. 1.2 в, г).

Для питания одного блока устройства необходим источник питания постоянного напряжения +5В, способный отдавать не менее 1А. Питание ВПУ может осуществляться: от блока питания зарядки мобильного телефона, внешнего аккумулятора по типу Power Bank для зарядки мобильного телефона. Возможна подача питания от разъема USB компьютера, но надо иметь ввиду, что мощности может оказаться недостаточно.

После подачи питания на БИ1 и БИ2 на корпусе обоих блоков должен мигать красный светодиод – индикатор работоспособного состояния.

Если планируется подключение к ВПУ по GSM, то с помощью оптического кабеля из комплекта поставки необходимо соединить БИ1, который содержит модуль оптического сопряжения, с блоком внешним (рис. 1, г). На блок внешний следует подать питание 220 В, см паспорт МИРТ.656331.022 ПС.

**Внимание! Оптический кабель имеет две жилы, которые необходимо подключать в соответствии с маркировкой «IN» и «OUT», нанесенной на крышке отсека БИ1 и на модуле сопряжения с ВПУ во внешнем блоке.** Оптический вход «IN» на БИ1 соединяется с оптическим выходом «OUT» на модуле сопряжения внешнего блока; оптический выход «OUT» на БИ1 соединяется с оптическим входом «IN» на модуле сопряжения блока внешнего. Схематично оптический кабель изображен на рисунке 1.3. Одна из его жил содержит метку, чтобы ориентироваться по ней при соединении оптических портов ВПУ с оптическими портами внешнего блока.

Блок внешний ВПУ содержит GSM модем, в который можно установить до 2 SIM-карт одновременно. Порядок установки SIM-карт и настройки описан в документации на GSM модем.

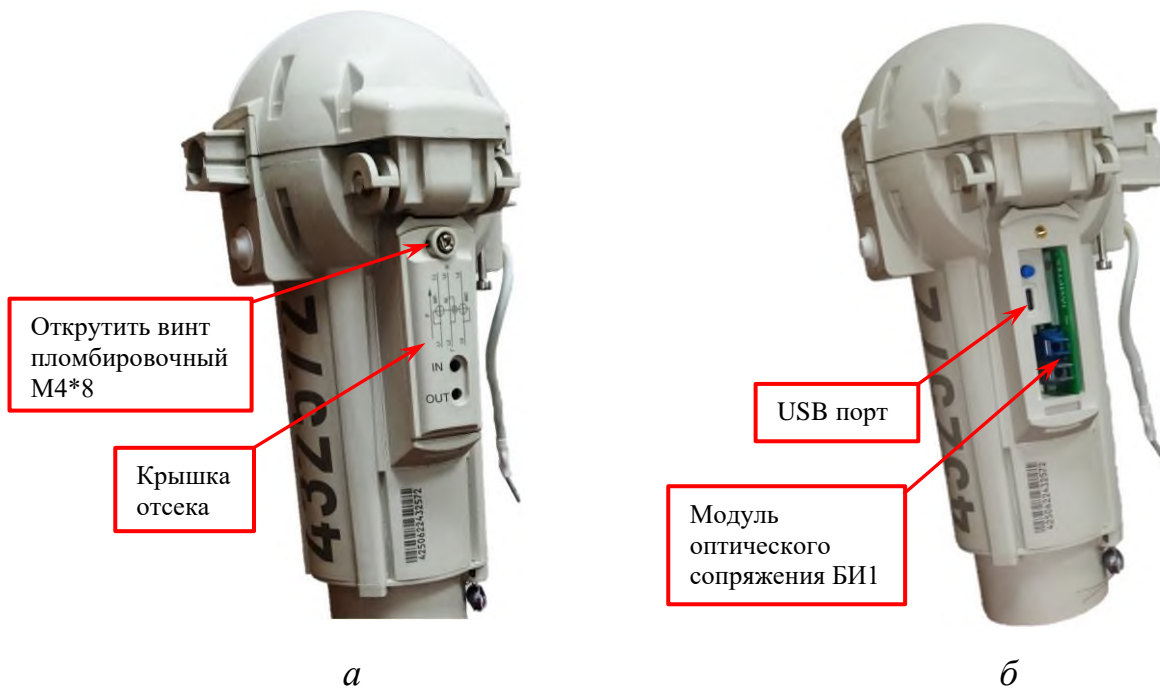


Рисунок 1.2 а, б – Снять крышку на БИ1 и БИ2.



Рисунок 1.2 в – USB Type-C кабель питания.

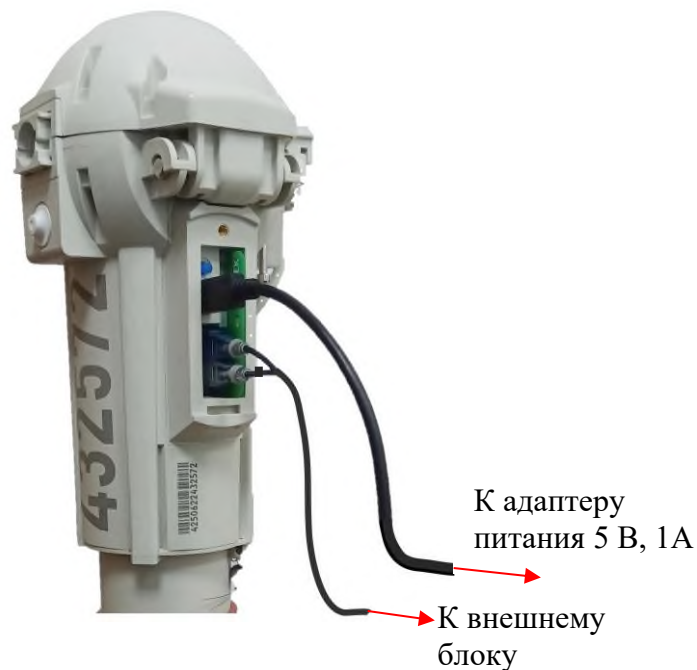


Рисунок 1.2 г – Подключить питание к БИ1 и БИ2, к БИ1 дополнительно подключить оптический кабель.

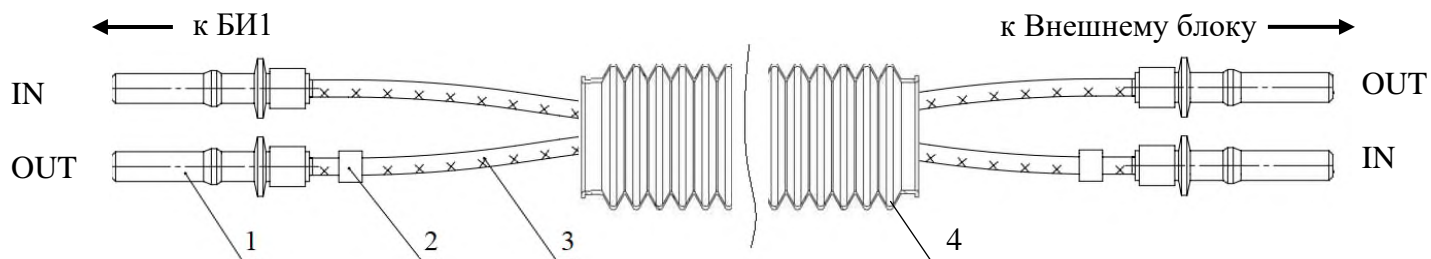


Рисунок 1.3 – Оптический кабель: 1 – коннекторы, 2 – метки порта подключения «OUT», 3 – пластиковые жилы, 4 – гофрированная труба.

## 1.2. Подготовка ПО

1.2.1. Установить ПО MeterTools с официального сайта ООО «МИРТЕК».

1.2.2 После установки рекомендуется проверить обновление, нажав *Сервис* → *Проверка обновлений* (рис. 1.4).

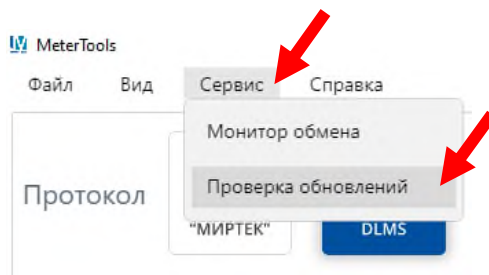


Рисунок 1.4 – Функция проверки обновления в ПО «MeterTools».

Основной интерфейс программы MeterTools для подключения к ВПУ показан на рисунке 1.5. В рабочем окне необходимо ввести данные для подключения. Рабочее окно содержит 2 тематических раздела:

- 1) **Протокол** (инструкции по заполнению - см п. 2, п.3);
- 2) **Каналы связи** (инструкция по заполнению - см п. 4).

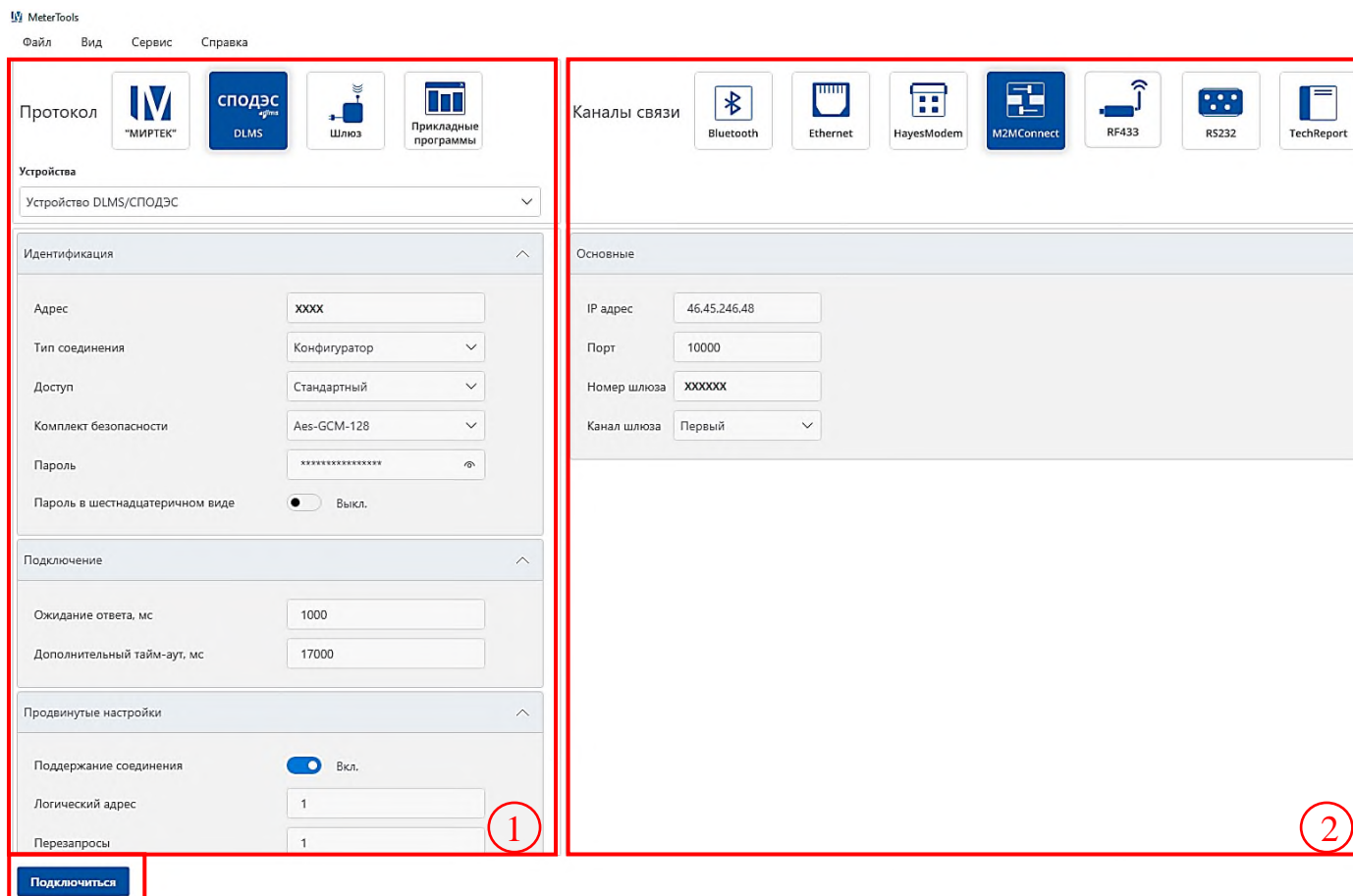


Рисунок 1.5. Интерфейс программы «MeterTools» для подключения к ВПУ, необходимо указать: 1) протокол, 2) канал связи. Символами «х» отмечены поля ввода численных значений, указанных в формуляре на ВПУ.

## 2 ПОДКЛЮЧЕНИЕ ПО «СПОДЭС»

(доступно для всех исполнений ВПУ)

### 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.

Программа «MeterTools» позволяет выполнить подключение по «СПОДЭС» к ВПУ всех исполнений. Для этого в разделе *Протокол* нажать кнопку *СПОДЭС*. В выпадающем меню *Устройства* должно быть выбрано *Устройство DLMS / СПОДЭС*, рис. 1.3.

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 (полный) номер указан в формуляре).

В выпадающем меню *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*: 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 А.

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».

В выпадающем меню *Доступ* при типе соединения *Конфигуратор* предоставляется 4 режима:

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

Пользователю предлагается дополнительно выбрать *комплект безопасности*:

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

Кроме того, потребуется ввести ключи шифрования и аутентификации.

Подробнее это будет рассмотрено далее.

Порядок настройки параметров доступа и шифрования описан в [п.2.7](#).

## 2.2 Идентификация в СПОДЭС - тип соединения «ПУБЛИЧНЫЙ КЛИЕНТ»

Для соединения «Публичный клиент» в подразделе *Идентификация* в поле *Адрес* ввести четыре последние цифры номера ВПУ, в выпадающем меню *Тип соединения* указать *Публичный клиент*, рис. 2.1.

После подключения для считывания доступна только общая информация об устройстве: дата и время, логическое имя, включающее зав. номер ВПУ, рис. 2.2.

Рисунок 2.1. Пример заполнения подраздела *Идентификация* при типе соединения *Публичный клиент*.

Общая	
Логическое имя устройства	MRT422029181XXXX
Время компьютера	17.01.2025 09:47:58
Время	17.01.2025 09:48:45
Расхождение времени	0 сут 0 ч 0 мин -47 с

**Считать**

Рисунок 2.2. Вид меню при типе соединения *Публичный клиент*.

### 2.3 Идентификация в СПОДЭС - тип соединения «СЧИТЫВАТЕЛЬ»

Тип соединения *Считыватель*, как следует из названия, дает возможность считывать данные из ВПУ и устанавливать сдвиг времени. Тип соединения *Считыватель* имеет один режим доступа: *стандартный*, который задан по умолчанию.

Для типа соединения *Считыватель* в подразделе *Идентификация* в поле *Адрес* следует ввести четыре последние цифры номера ВПУ, в выпадающем меню *Тип соединения* выбрать *Считыватель*. В поле *Пароль* вводится пароль **низкой** секретности по умолчанию *12345678*, рис. 2.3.

Идентификация	
Адрес	xxxx
Тип соединения	Считыватель
Пароль	12345678
Пароль в шестнадцатеричном виде	<input type="checkbox"/> Выкл.

Ввести последние 4 цифры номера ВПУ

Рисунок 2.3. Пример заполнения подраздела *Идентификация* при типе соединения *Считыватель*.

В типе соединения *Считыватель* предоставляются ограниченные права для выполнения записи настроек.

## 2.4 Идентификация в СПОДЭС - 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 режима доступа.

### 2.4.1 Режим доступа «Стандартный» (включен по умолчанию)

В режиме доступа *Стандартный* комплект безопасности используется только для шифрования пароля. Для подключения в поле *Идентификация* необходимо указать *Адрес* – последние 4 цифры номера ВПУ и пароль **высокой** секретности – *MeterCorporation* (рис. 2.4).

Идентификация

Адрес	xxxx
Тип соединения	Конфигуратор
Доступ	Стандартный
Комплект безопасности	Aes-GCM-128
Пароль	*****
Пароль в шестнадцатеричном виде	<input type="checkbox"/> Выкл.

Ввести последние 4 цифры номера ВПУ

Ввести пароль (по умолчанию «MeterCorporation»)

Рисунок 2.4. Пример заполнения подраздела *Идентификация* при типе соединения *Конфигуратор*, вариант доступа *Стандартный*.

### 2.4.2 Режимы доступа «С проверкой подлинности», «С шифрованием», «С проверкой подлинности и шифрованием»

В типе соединения *Конфигуратор* при выборе режимов: *С проверкой подлинности* или *С шифрованием* или *С проверкой подлинности и шифрованием* в подразделе *Идентификация* необходимо указать (рис. 2.5):

- 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**

- ключ аутентификации для **высокой** секретности:

по AES-GCM-128 – **AuthKeyHLS000001**

по KUZN-CTR-CMAC – **0000000000000000000000000000000001**

Подробнее ключи шифрования (заводские настройки) описаны в Приложении Б.

В зависимости от типа соединения при подключении (*Считыватель* или *Конфигуратор*) доступное меню MeterTools будет отличаться, пример приведен на рис. 2.6. Отличие состоит в рабочем интерфейсе для выполнения настроек.

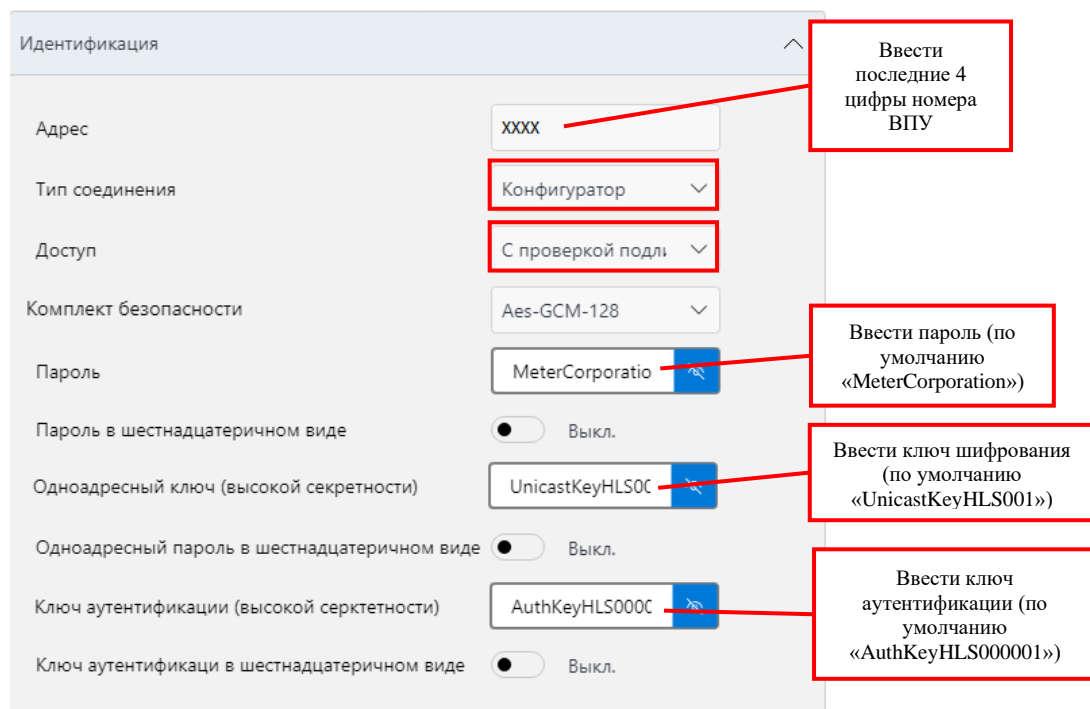
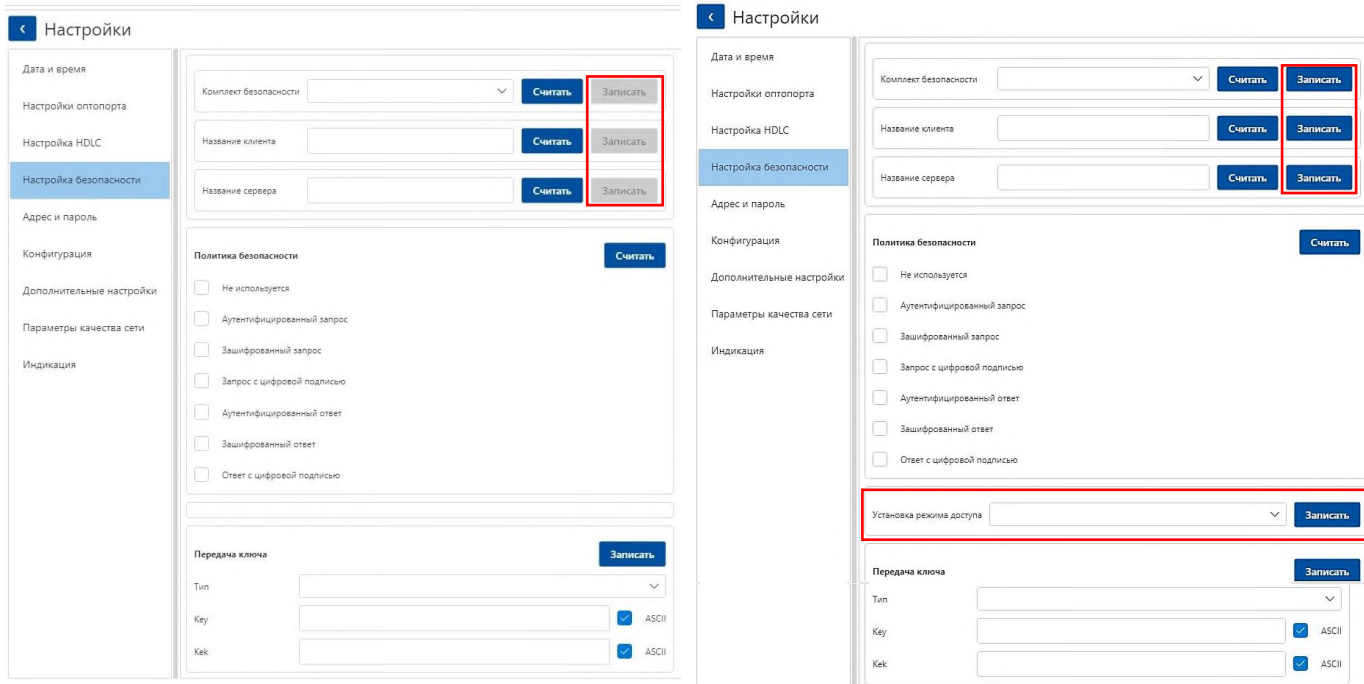


Рисунок 2.5. Пример заполнения подраздела *Идентификация* при типе соединения *Конфигуратор*, и в режимах доступа: *С проверкой подлинности*, *С шифрованием*, *С проверкой подлинности и шифрованием*.



а

б

Рисунок 2.6. Вид меню *Настройки* → *Настройки безопасности* после подключения с типом соединения: а – *Считыватель*, б – *Конфигуратор*.

## 2.5 Параметры подключения

Подраздел *Подключение* заполняется автоматически и обычно не требует корректировок со стороны пользователя. В случае нестабильной работы радиосвязи, когда MeterTools выдает ошибку подключения, в строке *Ожидание ответа* рекомендуется увеличить численные значения в диапазоне от 900 до 15000 мс.

## 2.6 Продвинутое настройки подключения

Подраздел *Продвинутое настройки* заполняется автоматически. Возможность редактирования продвинутых настроек предназначена главным образом для разработчиков.

## 2.7 Настройка параметров доступа и шифрования

### 2.7.1 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 рис. 2.7.

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.

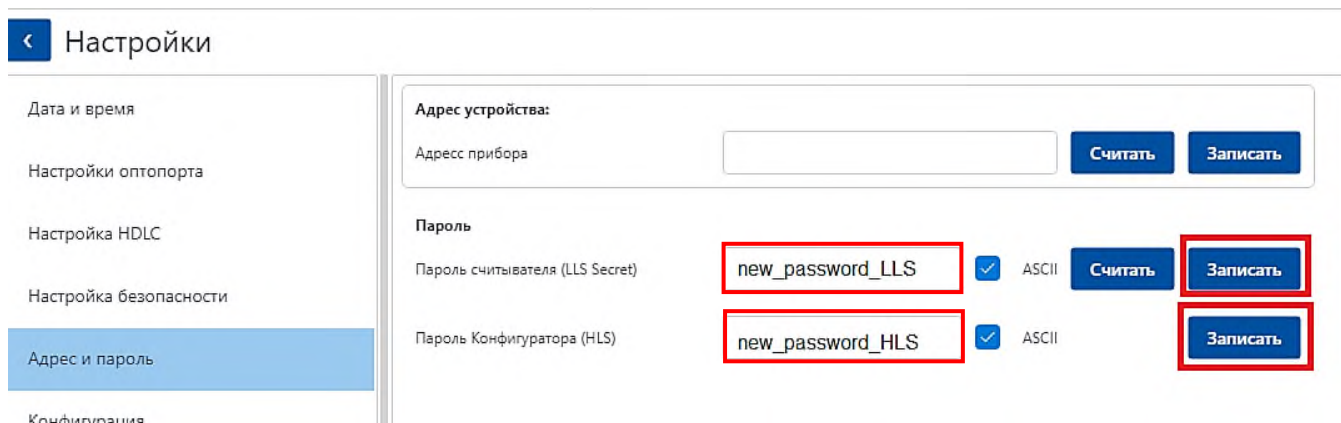


Рисунок 2.7. Задание паролей СПОДЭС.

### 2.7.2 Настройка политики безопасности

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

На вкладке **Настройки** → **Настройки безопасности** в выпадающем меню **Установка режима безопасности** предоставляется выбор из 4 вариантов, рис. 2.8. Установите необходимый вариант, нажмите **Записать**.

Нажмите кнопку **Отключиться** и выполните подключение снова, указав в строке **Доступ** выбранный до этого вариант режима безопасности. Зайдите в **Настройки** → **Настройки безопасности** и в поле **Политика безопасности** нажмите **Считать**. MeterTools отметит символом «V» используемый в настоящее время вариант политики. Если установлен режим безопасности **Стандартный**, то политика безопасности не используется.

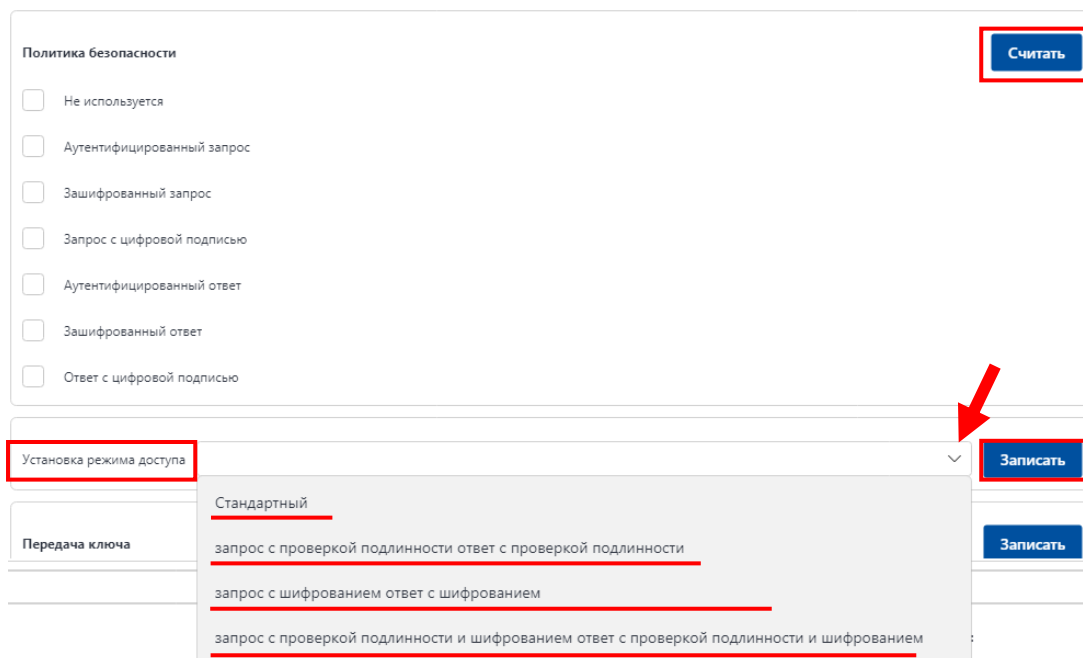


Рисунок 2.8. Настройка режима доступа (политики безопасности).

Обратите внимание, что записанный режим доступа должен быть указан в подразделе **Идентификация** в поле **Доступ** при следующем подключении к данному прибору. Далее, при успешном подключении, MeterTools запомнит указанный параметр и это поле будет заполняться автоматически при последующих подключениях.

### 2.7.3 Настройка комплекта безопасности

Настроить комплект безопасности возможно выполнив подключение с любым режимом доступа (политики безопасности). Смысл данной настройки состоит в изменении метода шифрования. На вкладке **Настройки** → **Настройки безопасности** в выпадающем меню **Комплект безопасности** предоставляется возможность задать один из двух комплектов безопасности: AES-GCM-128 (установлен по умолчанию) или ГОСТ 34.12-2018 «Кузнечик». Выбор необходимо сопроводить нажатием кнопки **Записать** (рис. 2.9).

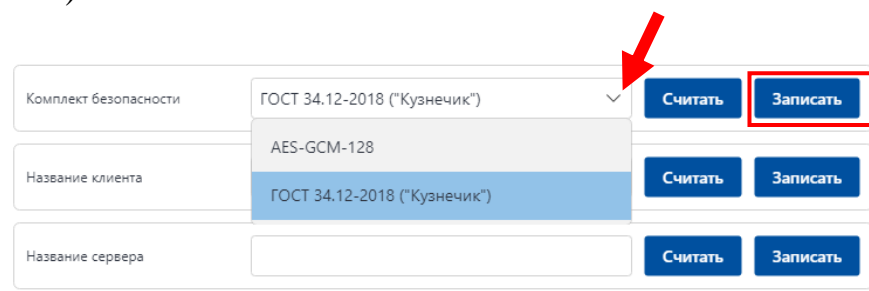


Рисунок 2.9. Изменение комплекта безопасности.

Обратите внимание, что записанный в настройках комплект безопасности необходимо будет указать в подразделе **Идентификация** в поле **Комплект безопасности** при следующем подключении к данному прибору. Далее, при успешном подключении, MeterTools запомнит указанный параметр и это поле будет заполняться автоматически при последующих подключениях.

#### 2.7.4 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](mailto:support@mirtekgroup.ru).

### 3 ПОДКЛЮЧЕНИЕ ПО ПРОТОКОЛУ «МИРТЕК»

(доступно для ВПУ, имеющих символ «P2» в структуре условного обозначения, указанной в формуляре)

#### 3.1 Общие сведения

Для подключения к ВПУ по протоколу «МИРТЕК» в разделе **Протокол** нажать кнопку **МИРТЕК**, а в выпадающем меню **Устройства** выбрать **Высоковольтный прибор учета**, рис. 3.1.

#### 3.2 Идентификация в протоколе МИРТЕК

3.2.1 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 в формуляре).

3.2.2 В поле **Пароль** указать пароль согласно формуляру (по умолчанию «0»).

### 3.3 Параметры подключения

В подразделе *Подключение* рекомендуется ввести значения:

- в поле *Ожидание ответа* – от 700 мс для RF433 и от 5000 мс для GSM (п.4);
- в поле *Задержка перед* – 10 мс,
- в поле *Количество перезапросов* – от 1.

При плохом уровне сигнала ожидание ответа и кол-во перезапросов возрастают. Оптимальные значения определяются эмпирическим путем, т.к. зависят от условий связи в месте установки ВПУ.

### 3.4 Параметры шифрования

Подраздел *Шифрование* предназначен для защиты соединения по протоколу МИРТЕК от несанкционированного доступа. Имеется функция записи *Параметра шифрования* (по умолчанию 0) в разделе *Настройки*.

Протокол: МИРТЕК, СПОДЭС DLMS, Шлюз, Прикладные программы

Устройства: Высоковольтный прибор учета

Идентификация

Адрес прибора: xxxxx

Пароль: 0

Подключение

Ожидание ответа, мс: 700

Задержка, мс: 10

Перезапросы: 1

Шифрование

Параметр шифрования: 0

Шифрование: Выкл.

Ретрансляция

Очистить ретрансляцию: Выкл.

Первая точка: 0

Ввести 5 последних цифр номера ВПУ

Ввести пароль (по умолчанию «0»)

Рисунок 3.1 Параметры подключения по протоколу «МИРТЕК».

## 4 КАНАЛЫ СВЯЗИ

Для подключения к ВПУ указывается доступный канал связи. ВПУ поддерживает 4 радио канала связи для передачи данных и конфигурирования:

- RF433, п. 4.1;
- GSM dynamic / static IP SIM-card (условное название M2MConnect), п. 4.2;
- GSM static IP SIM-card (условное название Ethernet), п. 4.3;
- Bluetooth (дополнительный канал связи), п. 4.4.

### 4.1 RF433 и мастер считывания данных МИРТ-141

4.1.1 Канал связи RF433 рассчитан на небольшое расстояние между компьютером и ВПУ, обычно до 100 м при условии прямой видимости.

4.1.2 Вставить в USB-порт ПК мастер считывания данных МИРТ-141, поставляемый опционально вместе с ВПУ МИРТЕК-135-РУ (рисунок 4.1). Мастер считывания дополнительно может быть укомплектован антенной, увеличивающей стабильность и дальность приема / передачи данных. Если вариант комплектации вашего прибора не предусматривает наличие мастера считывания, то вы можете подключиться к прибору по другому каналу (п.4.2 - 4.4).



Рисунок 4.1 – Мастер считывания данных по RF433 МИРТ-141.

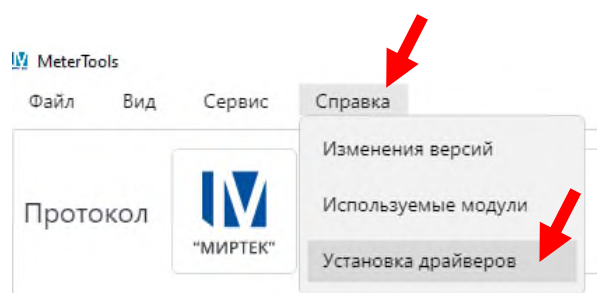


Рисунок 4.2 – Установка драйвера МИРТ-141.

4.1.3 При первом запуске необходимо установить драйвер (рисунок 4.2). В меню **Справка** → **Установка драйверов** выберите команду **Установка драйвера МИРТ-141 исп.2**. Примечание – применимо также для МИРТ-141 исп.4.

4.1.4 Нажать кнопку **RF433** в блоке **Каналы связи**.

4.1.5 В разделе **Основные** для параметра «Сетевая группа» выбрать из раскрывающегося списка значение по умолчанию «10» либо режим «Авто», рисунок 4.3.

4.1.6 В разделе **Основные** выбрать из раскрывающегося списка СОМ-порт, который определила операционная система для МИРТ-141.

4.1.7 Параметр **Скорость, бод** и параметры в разделе **Дополнительные** заполняются в Meter Tools автоматически.

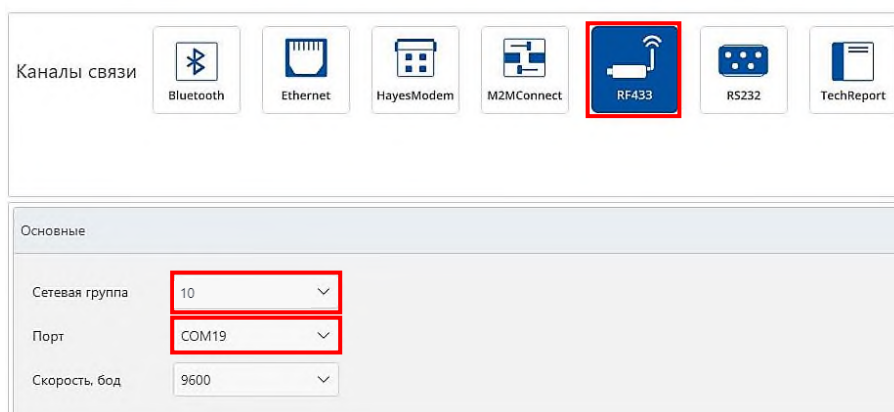


Рисунок 4.3. Пример ввода основных параметров для канала связи RF433.

## 4.2 GSM с SIM-картой с динамическим или статическим IP-адресом (M2MConnect)

4.2.1 Для подключения с помощью GSM необходимо, чтобы как минимум одна активная SIM-карта с динамическим или статическим IP-адресом была вставлена в слот GSM модема, расположенного во внешнем блоке.

4.2.2 В разделе **Каналы связи** необходимо нажать кнопку с условным обозначением **M2MConnect**, которая отвечает за подключение по GSM с динамическим или статическим IP-адресом.

4.2.3 В подразделе **Основные** ввести данные: IP адрес сервера – по умолчанию 46.45.246.48 (сервер 1) или 213.222.245.173 (сервер 2, резервный), порт подключения – по умолчанию 10000, номер шлюза (соответствует 8-ми последним цифрам IMEI GSM модема, который указан в паспорте GSM модема в комплекте документации к ВПУ, также IMEI указан на самом GSM модеме), канал шлюза – первый, рис. 4.4.

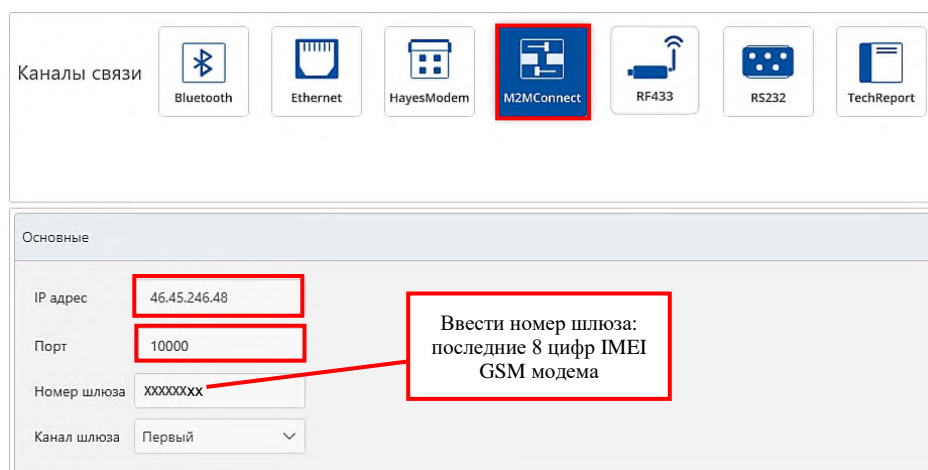


Рисунок 4.4. Пример ввода основных параметров для канала связи *M2MConnect*.

4.2.4 В канале связи *M2MConnect* может использоваться SIM-карта как с динамическим, так и со статическим IP. Это более универсальный канал по сравнению с *Ethernet* (п.4.3).

### 4.3 GSM с SIM-картой со статическим IP-адресом (Ethernet)

4.3.1 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 слот GSM модема.

4.3.2 Необходимо узнать локальный адрес своей SIM-карты. В случае с GSM модемами iRZ (устанавливаются по умолчанию) для этого потребуется установить программный продукт iRZ collector

4.3.3 Запустить приложение iRZ dispatcher, пример на рисунке 4.5.

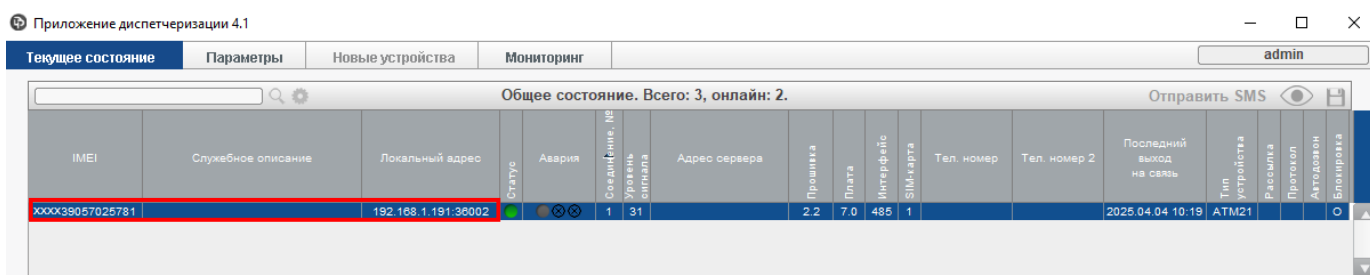


Рисунок 4.5 – Пример определения локального адреса по IMEI с помощью iRZ dispatcher.

4.3.4 Найти в открывшемся окне IMEI GSM модема (указан в паспорте GSM модема в комплекте документации к ВПУ, также указан на самом GSM модеме). В строке с IMEI вашего модема будет указан локальный адрес. Скопируйте его (только символы до знака « : ») и вставьте в окно программы Meter Tools, как это показано на рисунке 4.6, предварительно нажав в разделе **Каналы связи** кнопку с условным обозначением **Ethernet**, которая отвечает за подключение по GSM со статическим IP-адресом.

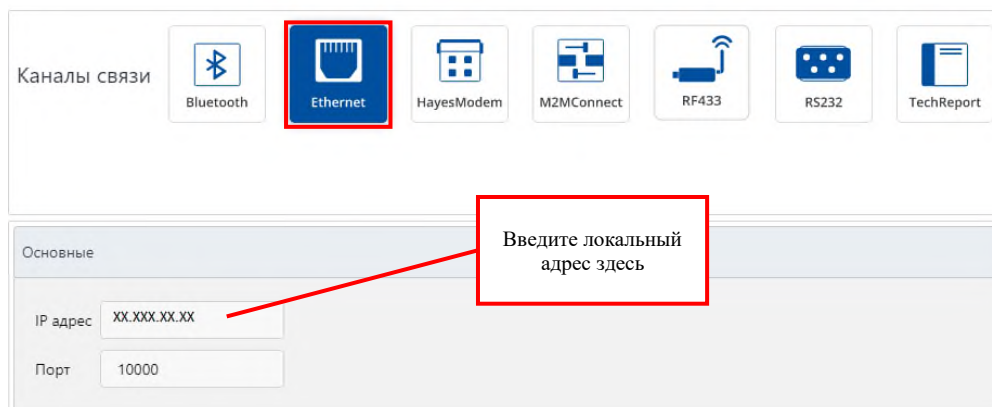


Рисунок 4.6 – Ввод параметров канала для подключения по GSM со статическим IP-адресом: в подразделе **Основные**, ввести статический **IP-адрес** SIM-карты и **Порт** - по умолчанию 10000.

## 4.4 Bluetooth

4.4.1 Для подключения к ВПУ по каналу связи Bluetooth убедитесь, что ваш компьютер имеет соответствующий адаптер. Компьютеры типа «ноутбук» или «планшет» обычно имеют встроенный Bluetooth адаптер. Для компьютера стационарной установки может потребоваться USB Bluetooth адаптер.

4.4.2 В разделе **Каналы связи** нажмите кнопку **Bluetooth**.

4.4.3 В подразделе **Основные** в строке **Имя устройства** необходимо ввести данные в формате: MIRTEK135\_последние 5 цифр серийного номера ВПУ\_номер сетевой группы. Пример имени устройства: **MIRTEK135\_43347\_15**. Для определения имени устройства нажмите на панели задач Windows значок стрелки, а затем на значок Bluetooth, как показано на рис. 4.7. Выберите команду **Добавление устройства Bluetooth**.

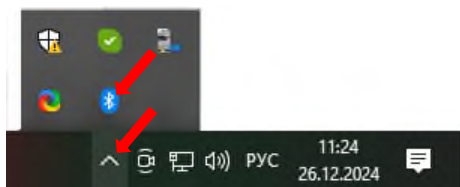


Рисунок 4.7. Панель ОС Windows.

На панели *Параметры* нажмите *Добавление Bluetooth или другого устройства*. В открывшемся окне нажмите *Bluetooth*. Запустится поиск устройств Bluetooth, где должно появиться имя устройства ВПУ в указанном формате (рис. 4.8).

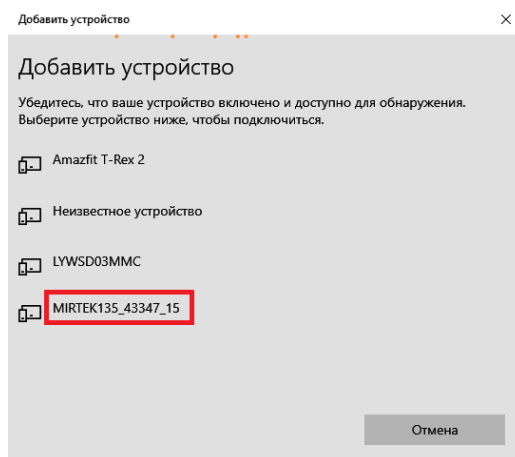


Рисунок 4.8. Поиск устройств Bluetooth в ОС Windows.

Введите это имя в строку *Имя устройства*, как показано на рис. 4.9.

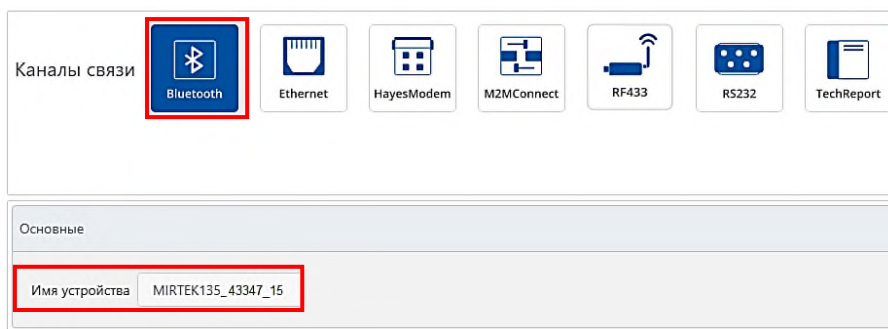


Рисунок 4.9. Пример ввода имени устройства канала связи Bluetooth в MeterTools.

Если имя устройства в указанном формате не появилось, то проверьте адаптер Bluetooth на вашем компьютере и наличие питания ВПУ, сократите по возможности расстояние между ПК и ВПУ и уберите источники электромагнитных помех. Затем повторите поиск. Контрольный поиск доступных Bluetooth устройств для проверки готовности ВПУ для связи по Bluetooth можно произвести в смартфоне.

## 5 ПОДКЛЮЧЕНИЕ СО СМАРТФОНА

5.1 Для подключения к ВПУ можно воспользоваться смартфоном. Подключение со смартфона производится по Bluetooth.

5.2 Для первого подключения на смартфоне с ОС Android нужно запустить браузер, например *Google Chrome*, и ввести в строке поиска *Rustore для андроид*. Программа найдет сайт *Rustore*, нужно зайти на этот сайт и нажать *Скачать*, а затем открыть скачанный файл *Rustore.apk* и установить приложение *Rustore*.

5.3 Запустить установленное приложение *Rustore*. В строке поиска приложений ввести *МИРТЕК*. Программа найдет приложение *МИРТЕК: мобильный учет*. Скачайте его и установите.

5.4 Активировать функцию Bluetooth на смартфоне. Затем открыть *Настройки* → *Bluetooth* → *Добавить устройство*. ВПУ должен появиться в списке найденных устройств под наименованием *MIRTEK135\_XXXXX\_XX*.

5.5 Запустите приложение *МИРТЕК: мобильный учет*. Приложение запросит предоставить разрешения на доступ к местоположению и мультимедиа данным смартфона. Согласитесь предоставить.

5.6 Нажмите кнопку *Найти*. Появится список всех устройств Миртек, доступных для подключения по Bluetooth. Выберите ваш ВПУ из списка нажав на строку с его обозначением: *MIRTEK135* и последние цифры номера ВПУ, рис. 5.1.

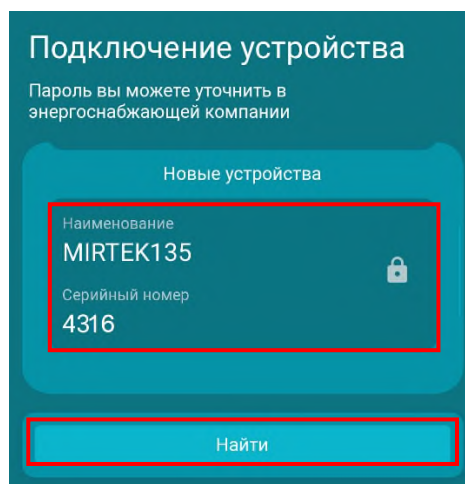


Рисунок 5.1. Пример поиска устройств в *МИРТЕК: мобильный учет*.

5.7 После появления диалогового окна, указать протокол подключения. По умолчанию указан протокол МИРТ (МИРТЕК). При подключении по МИРТЕК ввести пароль, по умолчанию *0*. При подключении по СПОДЭС также понадобится указать пароль для считывания данных, по умолчанию – *12345678*, а также адрес (по умолчанию

это последние **4 цифры** номера ВПУ, например 4316). Внизу диалогового окна нажать кнопку **Подключить**, рис. 5.2.

The screenshot shows a configuration dialog box for the MIRTEK135 device. It contains the following fields and options:

- Наименование: MIRTEK135
- Серийный номер: 4316
- Выберите протокол: СПОДЭС (highlighted with a red box)
- Адрес: 4316 (highlighted with a red box)
- Пароль: 12345678 (highlighted with a red box)
- Запомнить пароль: checked
- Подключить (button, highlighted with a red box)

Рисунок 5.2. Пример ввода параметров подключения.

5.8 После успешного подключения появится меню **Информация о приборе учета**, рис. 5.3.



Рисунок 5.3. В случае успешного подключения открывается информация о приборе.

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

**Таблица А.1 Описание типов соединения 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.

**Таблица А.2 Протоколы и команды для передачи данных ВПУ.**

	Исполнения ВПУ «P1»	Исполнения ВПУ «P2»
Поддерживаемые протоколы	1. СПОДЭС (DLMS / COSEM)	1. СПОДЭС (DLMS / COSEM), 2. МИРТЕК
Поддержка SMS команд	нет	есть

## ПРИЛОЖЕНИЕ Б. Ключи шифрования в «СПОДЭС»

Комплект безопасности		AES-GCM-128	ГОСТ 34.12-2018 «Кузнечик»
Ключи			
Аутентификации	низкой секретности*	AuthKeyLLS000001	00000000000000000000000000000001
	высокой секретности	AuthKeyHLS000001	00000000000000000000000000000001
Одноадресный	низкой секретности*	UnicastKeyLLS001	UnicastKeyLLS00000000000000000000
	высокой секретности	UnicastKeyHLS001	UnicastKeyHLS00000000000000000000
Мастер ключ		MeterMasterKey01	MeterMasterKey00000000000000000000 00000000000000000000000000000001

\* в СПОДЭС 4 LLS ключи не используются.