ООО «МИРТЕК»

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

ИНСТРУКЦИЯ ПО ПОДКЛЮЧЕНИЮ К ВПУ ПО ИНТЕРФЕЙСАМ СВЯЗИ

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

МИРТ.411152.205ИМ3 (V2)

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

СОДЕРЖАНИЕ

1 ПОДГОТОВКА К ПОДКЛЮЧЕНИЮ ... 3

2 ПОДКЛЮЧЕНИЕ ПО «СПОДЭС» ... 5

2.1 Общие сведения ... 5

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» ... 8

2.4.1 Режим доступа «Стандартный» (включен по умолчанию) ... 8

2.4.2 Режимы доступа «С проверкой подлинности», «С шифрованием», «С проверкой подлинности и шифрованием» ... 9

2.5 Параметры подключения ... 11

2.6 Продвинутые 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 ... 13

3 ПОДКЛЮЧЕНИЕ ПО ПРОТОКОЛУ «МИРТЕК» ... 14

3.1 Общие сведения ... 14

3.2 Идентификация в протоколе МИРТЕК ... 14

3.3 Параметры подключения ... 14

3.4 Параметры шифрования ... 14

3.5 Параметры ретрансляции ... 14

3.6 Пример подключения для считывания GSM настроек и изменения пароля ... 15

4 КАНАЛЫ СВЯЗИ ... 17

4.1 RF433 и мастер считывания данных МИРТ-141 ... 17

4.2 GSM с SIM-картой с динамическим или статическим IP-адресом (M2MConnect) ... 19

4.3 GSM с SIM-картой со статическим IP-адресом (Ethernet) ... 20

4.4 Bluetooth ... 20

5 ПОДКЛЮЧЕНИЕ СО СМАРТФОНА ... 22

ПРИЛОЖЕНИЕ А. Отличия исполнений ВПУ ... 24

ПРИЛОЖЕНИЕ Б. Аутентификация в различных типах соединений «СПОДЭС» ... 26

ПРИЛОЖЕНИЕ В. Ключи шифрования в «СПОДЭС» ... 27

1 ПОДГОТОВКА К ПОДКЛЮЧЕНИЮ

1.1 Установить ПО MeterTools с официального сайта ООО «МИРТЕК»:

https://mirtekgroup.com/produkciya/programmnoe-obespechenie/metertools

1.2 После установки рекомендуется проверить обновление, нажав *Сервис* → *Проверка обновлений* (рис. 1.1).

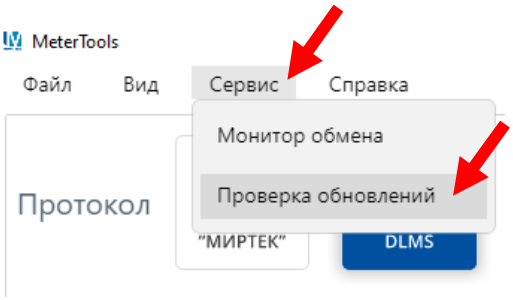
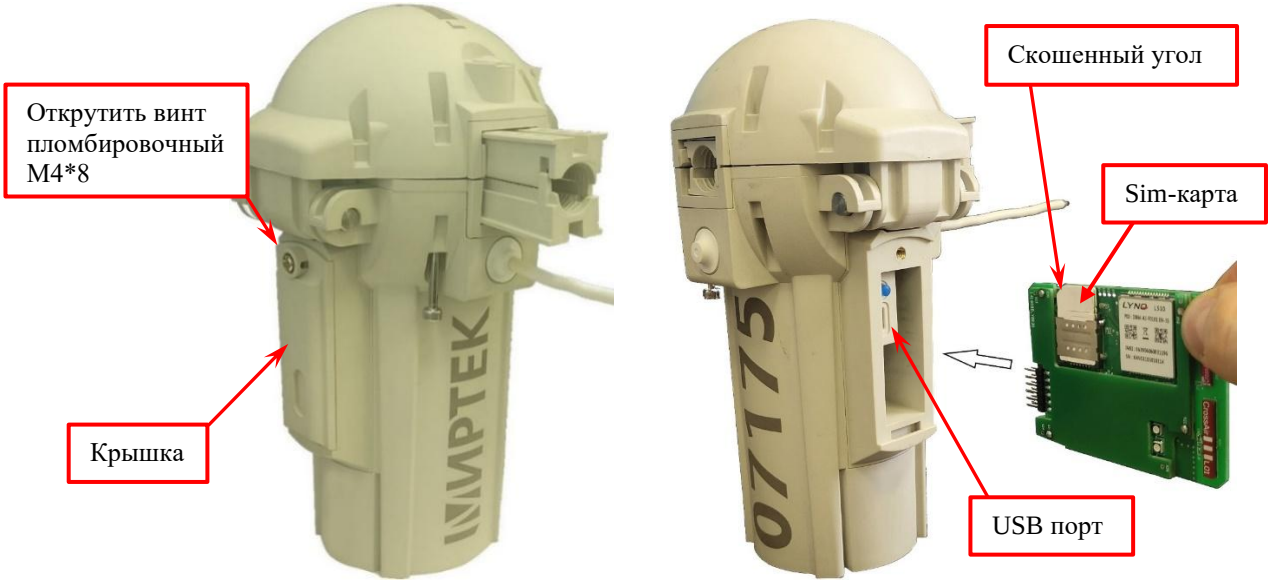


Рисунок 1.1 – Функция проверки обновления в ПО «MeterTools».

Для подключения к высоковольтному прибору учета (далее - ВПУ) МИРТЕК-135-РУ, если он еще не установлен на ЛЭП, необходимо подать питание на блоки измерительные (БИ). Для подачи питания по USB и установки SIM-карты крышка отсека модуля связи GSM должна быть в снятом состоянии (рис. 1.2 а, б). В один измерительный блок ВПУ можно установить до 2 SIM-карт одновременно. По умолчанию ВПУ имеет один модуль связи GSM, расположенный в БИ1. Питание необходимо подать через кабели USB type-C, поставляемые в комплекте (рис. 1.2в). Подать питание следует на оба измерительных блока, как на БИ1, так и на БИ2 (рис. 1.2г).

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.



а б

Рисунок 1.2а – Снять крышку модуля связи на БИ1, б – вставить SIM карту mini-SIM (2FF) любого оператора, если необходим GSM канал связи.

Рисунок 1.2в – USB кабель питания.

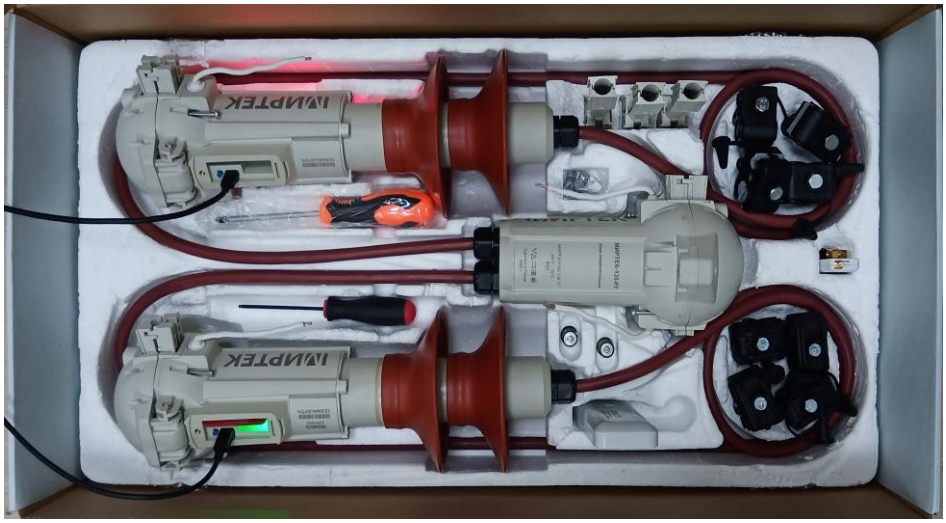


Рисунок 1.2г – Подключить питание к БИ1 и БИ2.

Основной интерфейс программы MeterTools для подключения к ВПУ показан на рисунке 1.3. 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).

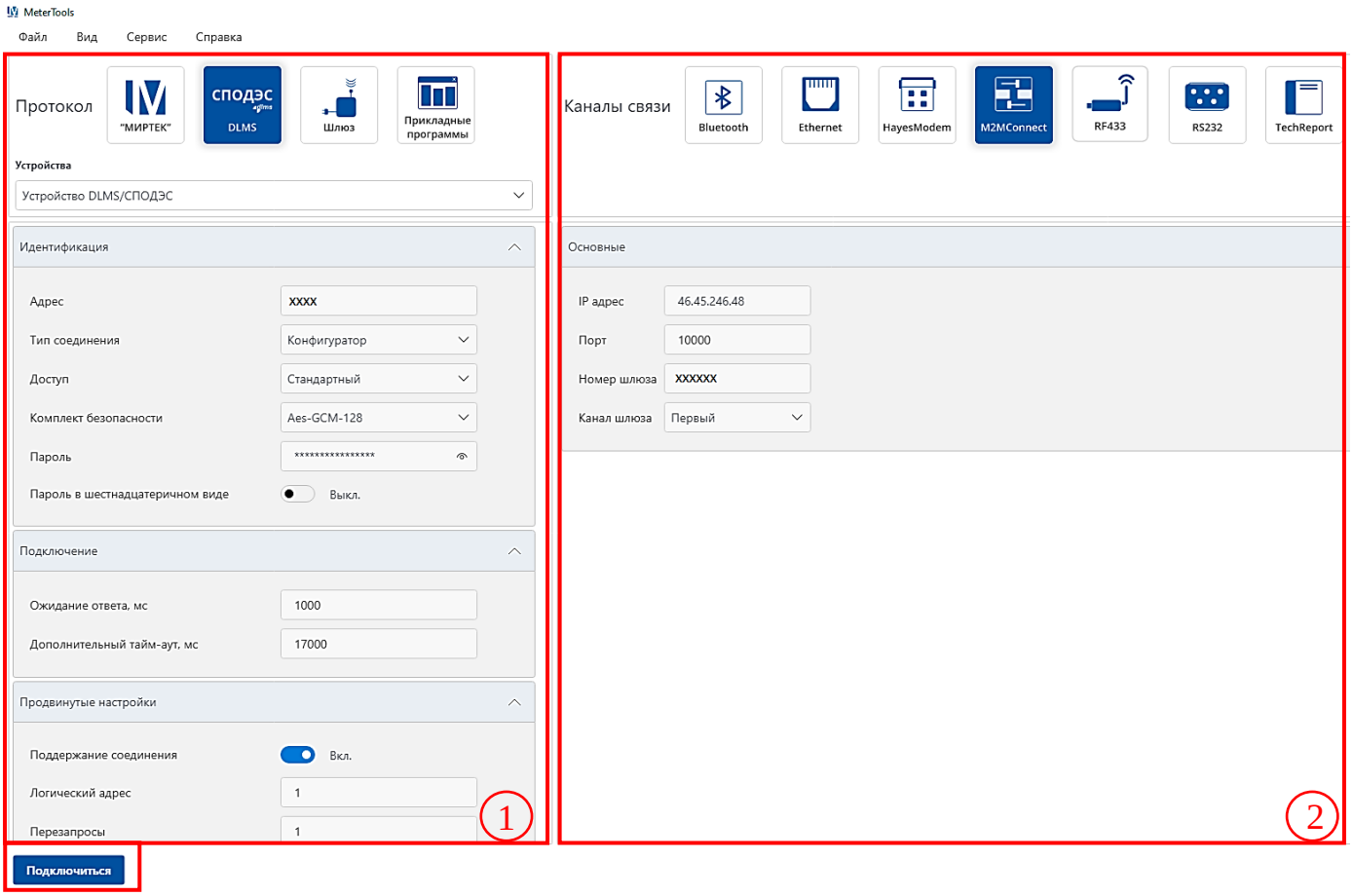


Рисунок 1.3. Интерфейс программы «MeterTools» для подключения к ВПУ, необходимо указать: 1) протокол, 2) канал связи. Символами «x» омечены поля ввода численных занчений указанных в формуляре на ВПУ.

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. Дополнительно необходимо ознакомиться с отличиями исполнений ВПУ, приведенными в приложении А.

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 <u>приложении Б</u>.

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.

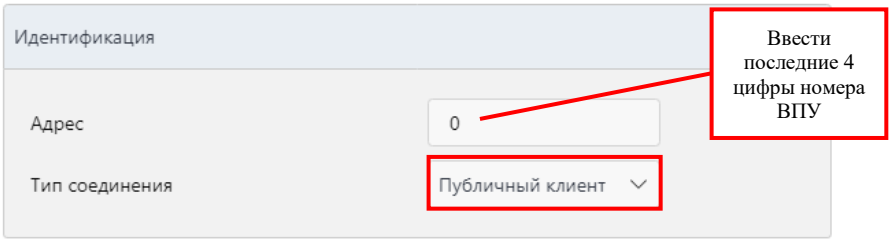


Рисунок 2.1. Пример заполнения подраздела ***Идентификация*** при типе соединения ***Публичный клиент***.

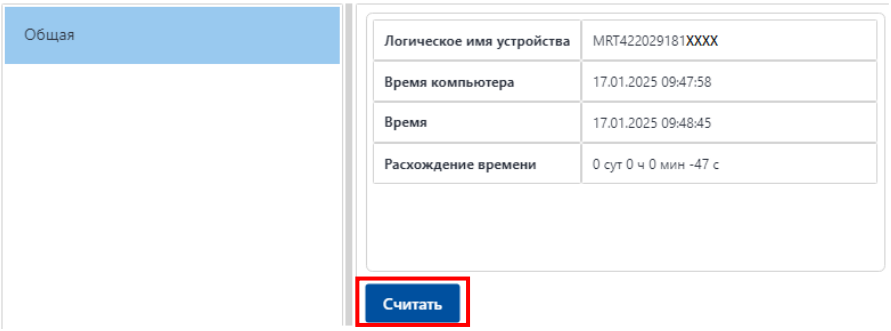


Рисунок 2.2. Вид меню при типе соединения ***Публичный клиент***.

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.

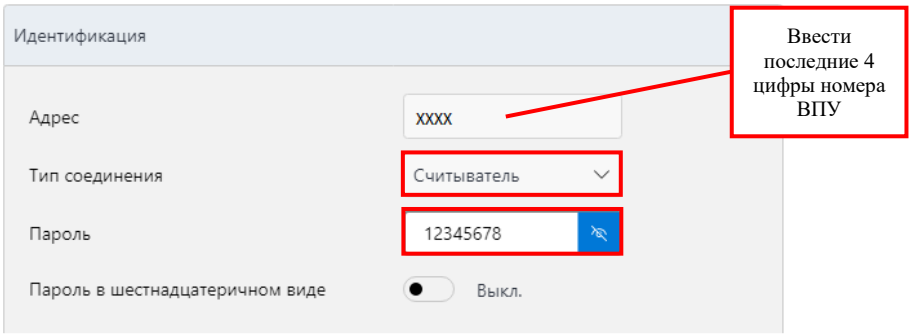


Рисунок 2.3. Пример заполнения подраздела ***Идентификация*** при типе соединения ***Считыватель.***

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).

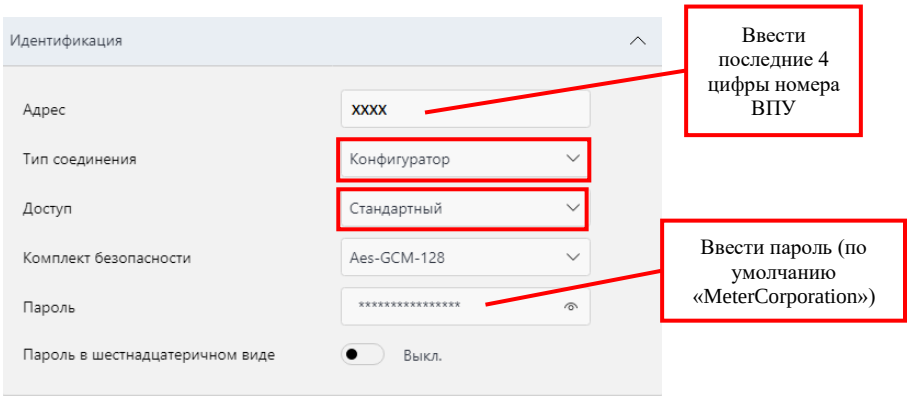


Рисунок 2.4. Пример заполнения подраздела ***Идентификация*** при типе соединения ***Конфигуратор***, вариант доступа ***Стандартный***.

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 – **00000000000000000000000000000001**

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

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.

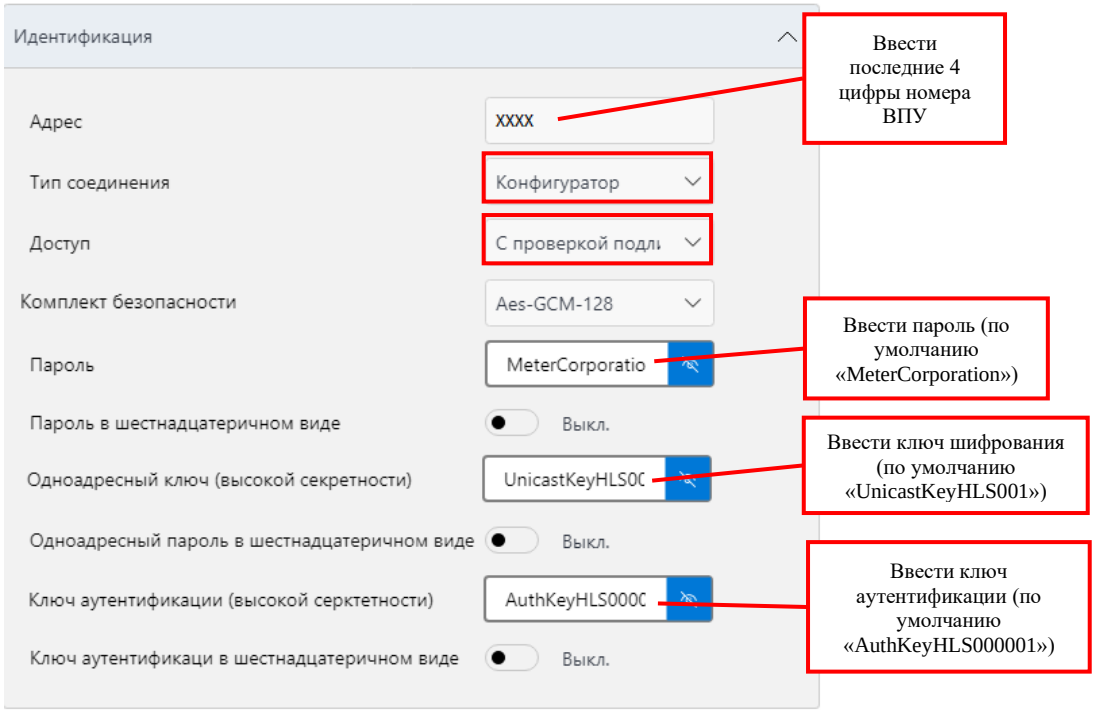
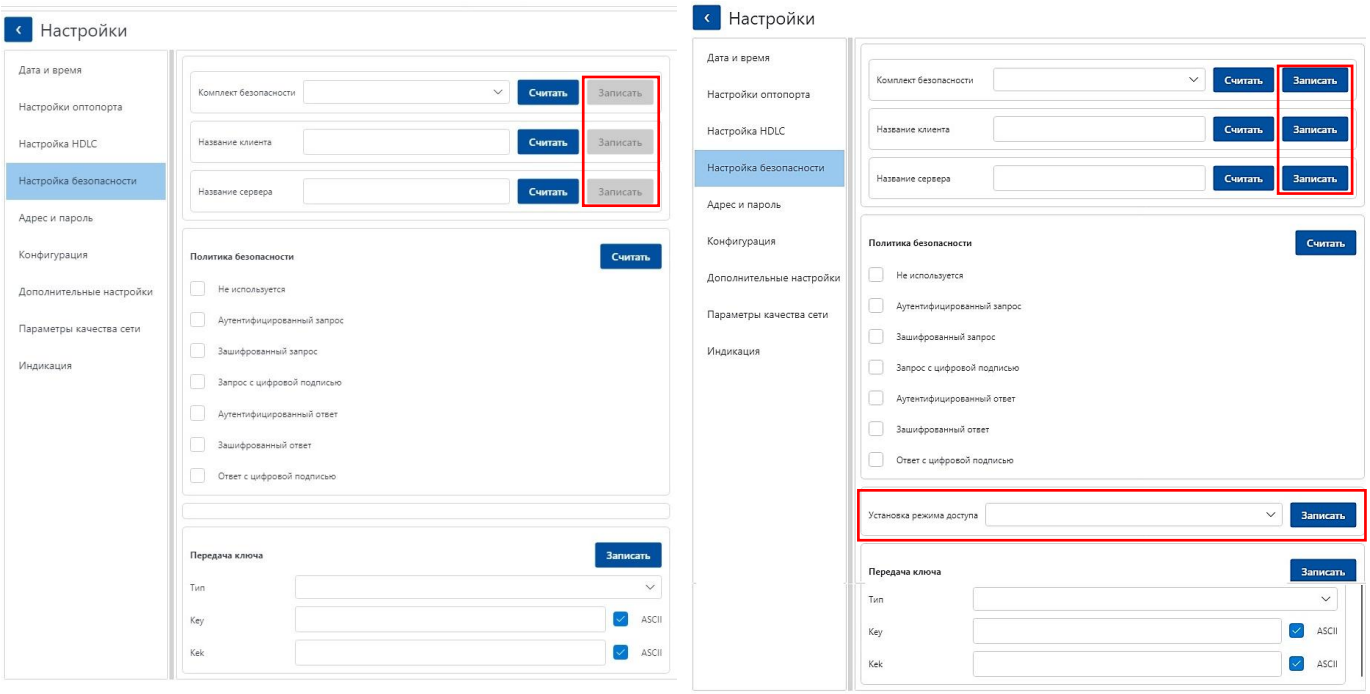


Рисунок 2.5. Пример заполнения подраздела ***Идентификация*** при типе соединения ***Конфигуратор***, и в режимах доступа: ***С проверкой подлинности***, ***С шифрованием, С проверкой подлинности и шифрованием.***



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 численное значения в диапазоне от 900 до 15000 мс.

2.6 Продвинутые настройки подключения

Подраздел ***Продвинутые 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.

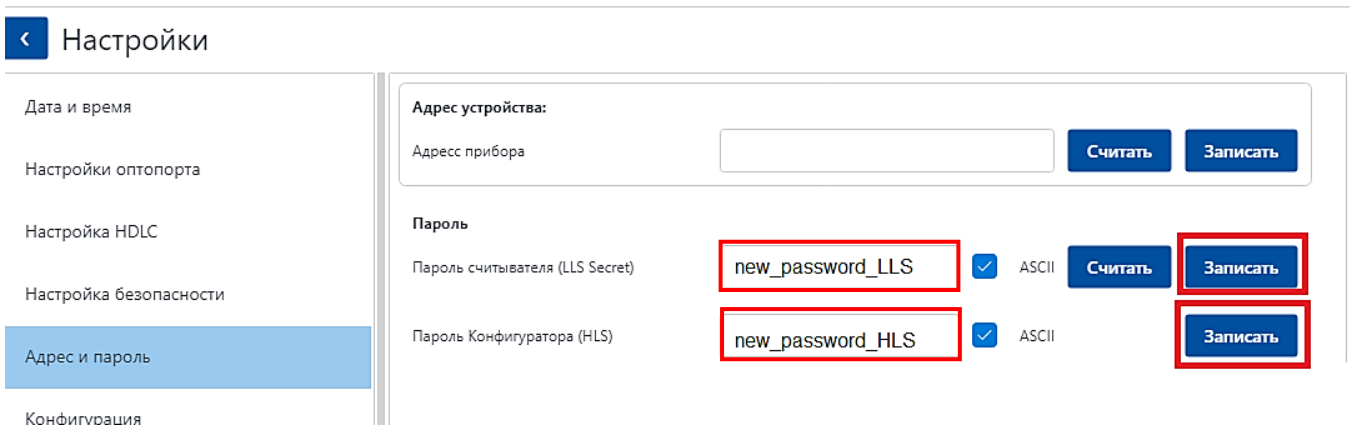


Рисунок 2.7. Задание паролей СПОДЭС.

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.

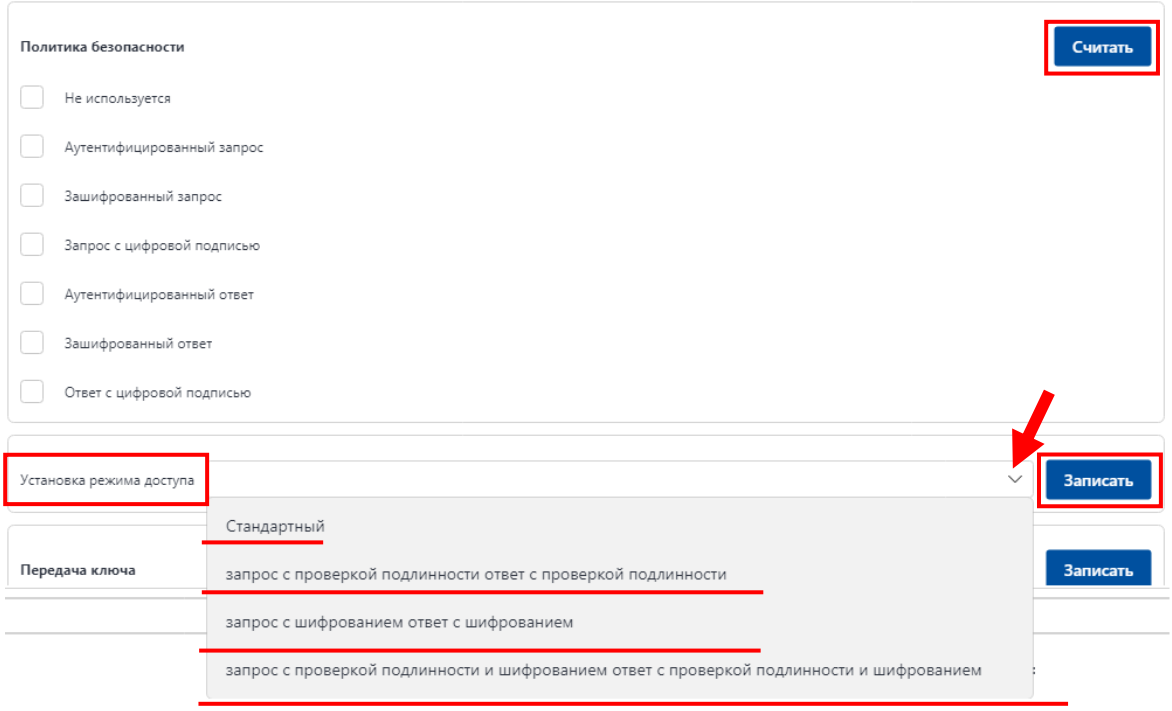


Рисунок 2.8. Настройка режима доступа (политики безопасности).

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).

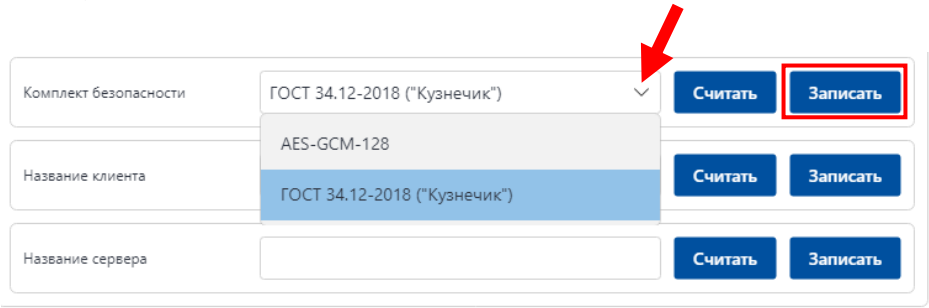


Рисунок 2.9. Изменение комплекта безопасности.

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.411152.136ИМ7 в службу технической поддержки МИРТЕК любым из нижеперечисленных способов:

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

3 ПОДКЛЮЧЕНИЕ ПО ПРОТОКОЛУ «МИРТЕК»

(доступно для ВПУ, имеющих символ «Р2» 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***.

3.5 Параметры ретрансляции

Подраздел ***Ретрансляция*** предназначен главным образом для увеличения дальности канала связи RF433 (п.4.1) путем создания сети ретрансляторов из любых приборов учета МИРТЕК либо специальных ретрансляторов связи МИРТЕК. В строку ***Первая точка*** вводится адрес прибора / ретранслятора расположенного наиболее

близко к мастеру считывания МИРТ-141 (рис. 4.1), в строку ***Вторая точка*** – адрес прибора / ретранслятора наиболее близкорасположенного по отношению к первому и т.д. Последняя вводимая точка ретрансляции должна быть расположена наиболее близко по отношению к ВПУ.

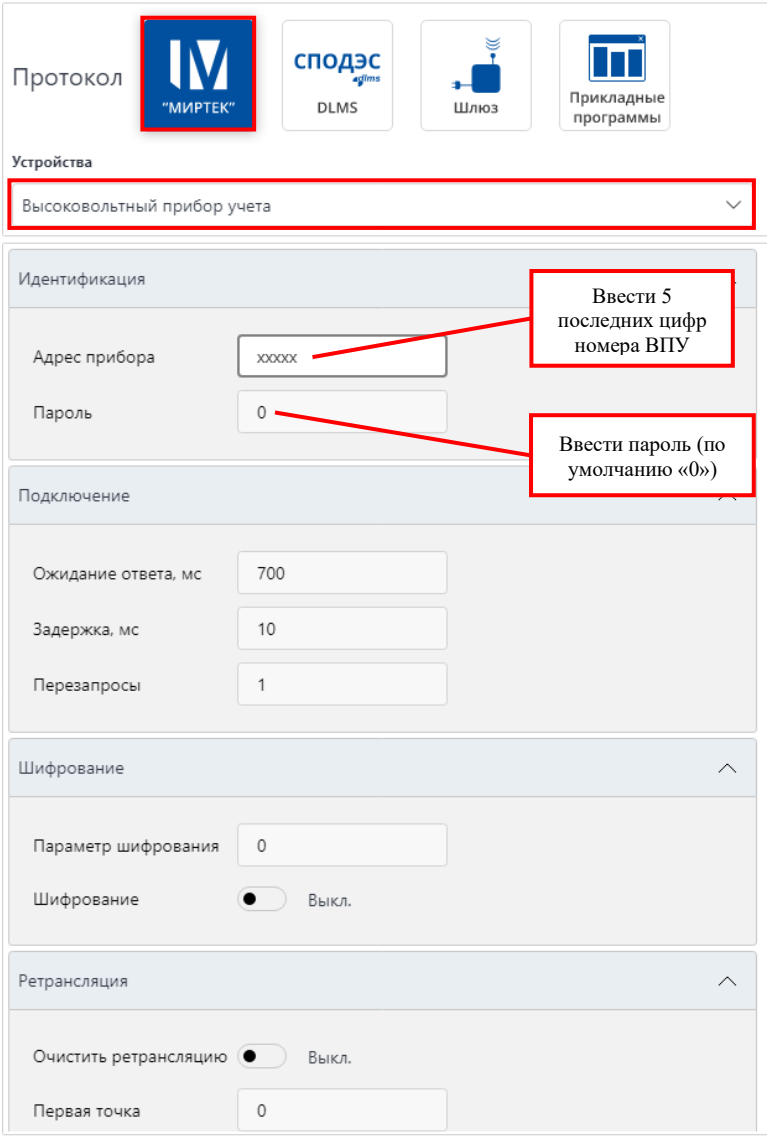


Рисунок 3.1 Параметры подключения по протоколу «МИРТЕК».

3.6 Пример подключения для считывания GSM настроек и изменения пароля

3.6.1 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.

3.6.2 После подключения в меню ***GSM модуль → Параметры сети*** в конце списка нажмите кнопку ***Считать*** (рис. 3.2). Результат считывания IP-адреса SIM-карты отобразится в этом же окне в строке ***IP адрес шлюза GPRS***.

3.6.3 На рис.3.3 показан пример получения данных о GSM модуле прибора.

3.6.4 В списке параметров найти ***Уровень сигнала активной SIM-карты*** и нажать кнопку ***Считать***. При устойчивом соединении значение обычно выше, чем минус 78 дБм.

3.6.5 Если используется 2 SIM-карты, то выбрать номер нужной в раскрывающихся списках ***Активная SIM-карта*** и ***Приоритет SIM-карты***. Подтвердить выбор нажатием кнопки ***Записать***.

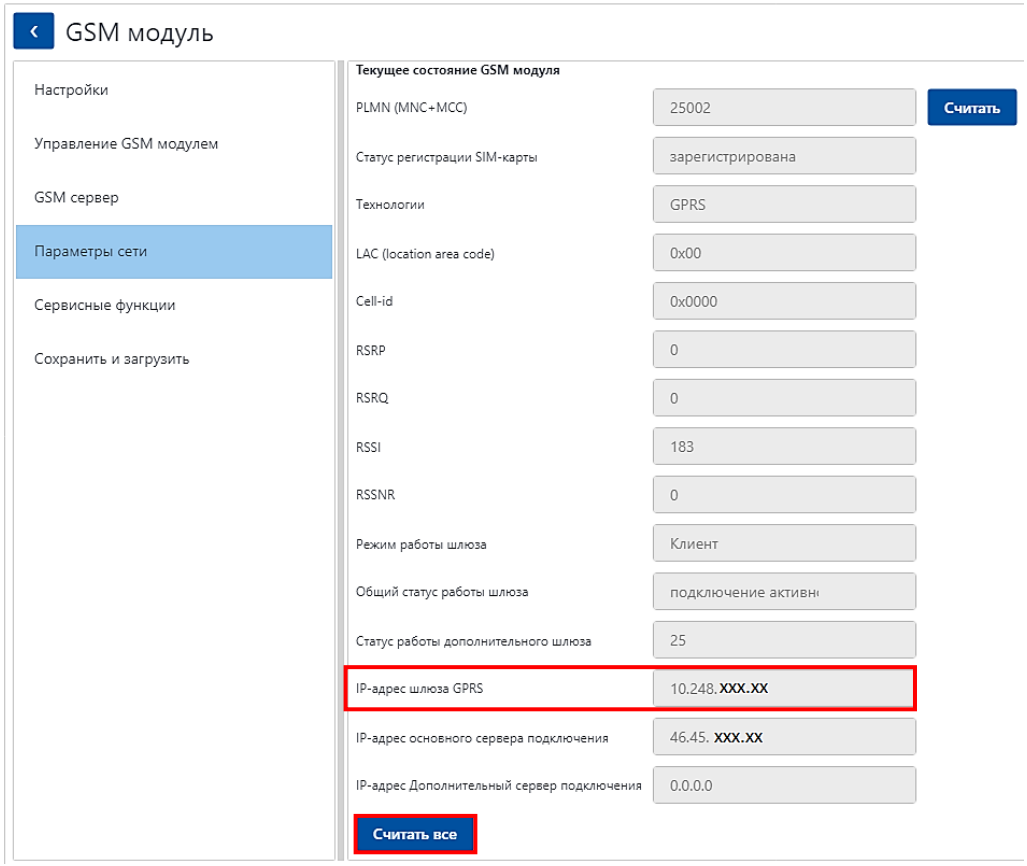


Рисунок 3.2 – Считывание IP-адреса.

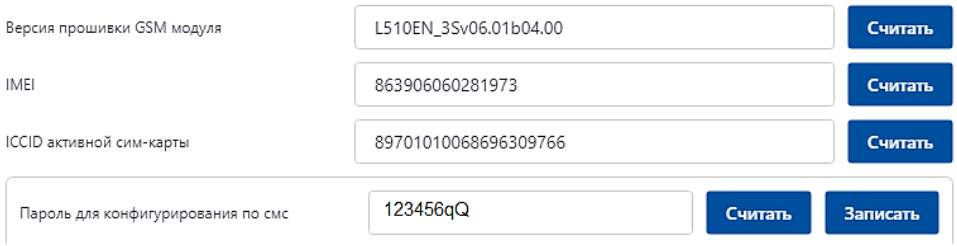


Рисунок 3.3 – Считывание данных о GSM модуле прибора.

3.6.6 Задание нового пароля для подключения к ВПУ производится на вкладке ***Адрес и пароль***, рис. 3.4.

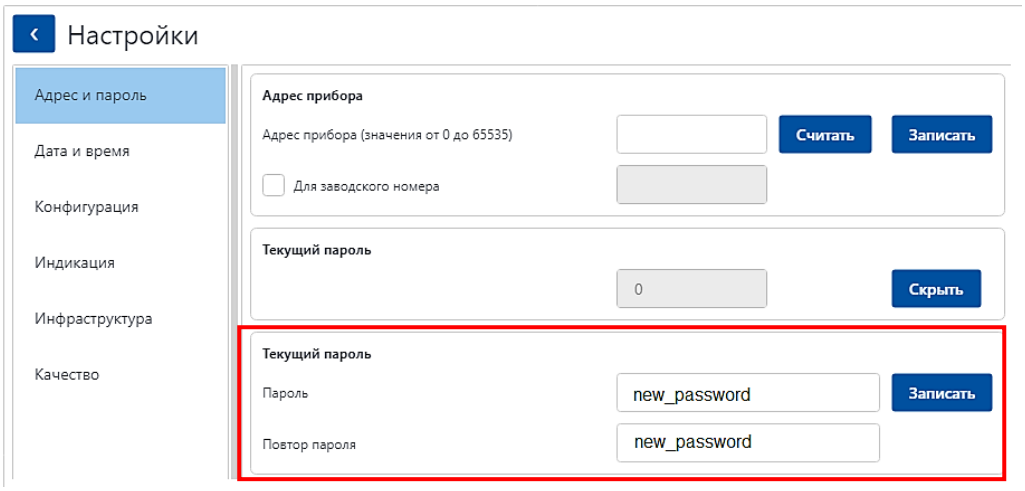


Рисунок 3.4 – Задание нового пароля.

4 КАНАЛЫ СВЯЗИ

Для подключения к ВПУ указывается доступный канал связи. ВПУ поддерживает 4 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.

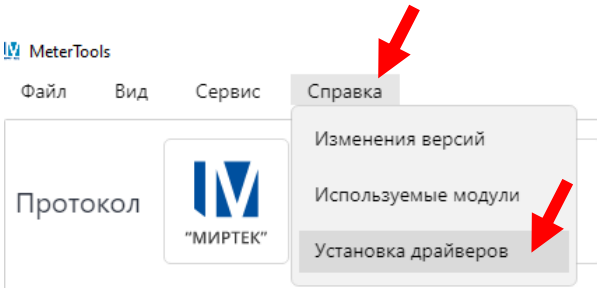


Рисунок 4.2 – Установка драйвера МИРТ-141.

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 COM-порт, который определила операционная система для МИРТ-141.

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

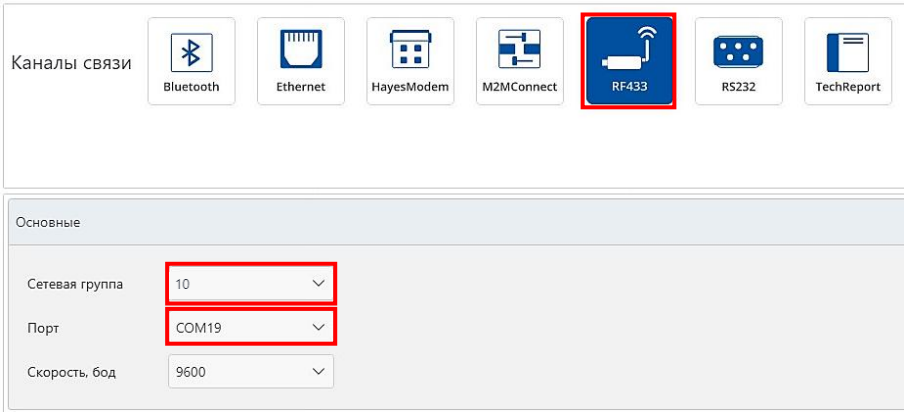


Рисунок 4.3. Пример ввода основных параметров для канала связи RF433.

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 измерительного блока (рис. 1.2б).

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 (указан в формуляре), канал шлюза – первый, рис. 4.4.

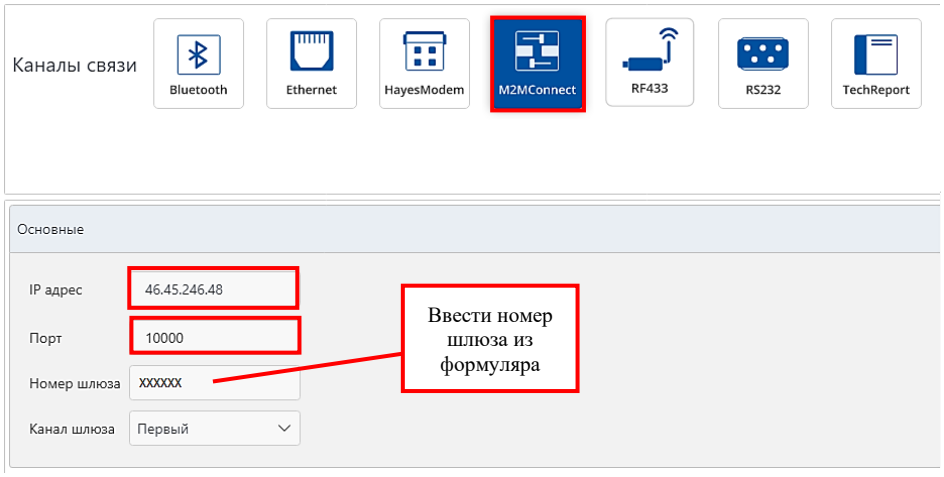


Рисунок 4.4. Пример ввода основных параметров для канала связи ***M2MConnect***.

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 первый слот измерительного блока.

4.3.2 Необходимо узнать у оператора фактический IP-адрес своей SIM-карты, либо определить его с помощью «Meter tools» путем подключения по другому каналу связи и считывания данных GSM (рис. 3.2).

4.3.3 Запустить приложение «Meter Tools», открыв программу в новом окне.

4.3.4 В разделе «Каналы связи» нажать кнопку с условным обозначением ***Ethernet***, которая отвечает за подключение по GSM со статическим IP-адресом.

4.3.5 В подразделе ***Основные***, ввести статический ***IP-адрес*** SIM-карты и ***Порт подключения*** - по умолчанию 10000, рис. 4.5.

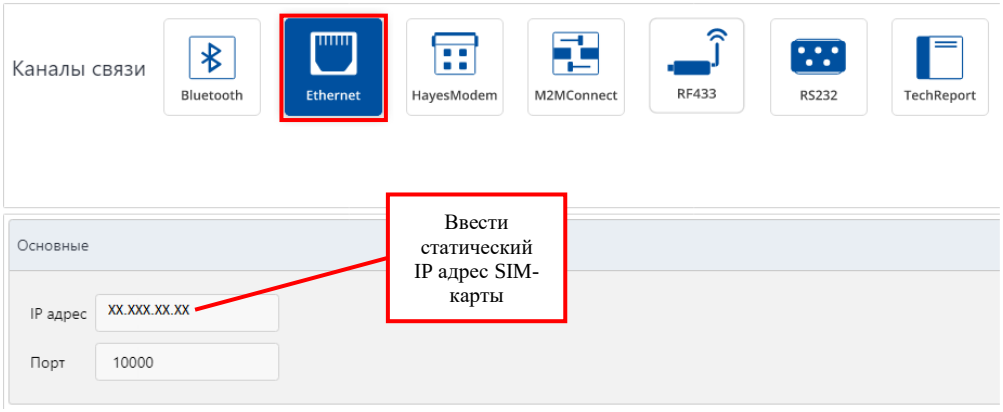


Рисунок 4.5 – Пример ввода параметров канала для подключения по GSM со статическим IP-адресом.

4.4 Bluetooth

4.4.1 Функционал для подключения по **Bluetooth** имеется в ВПУ со сменным модулем связи (приложение А). 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. 4.6. Выберите команду ***Добавление устройства Bluetooth***.

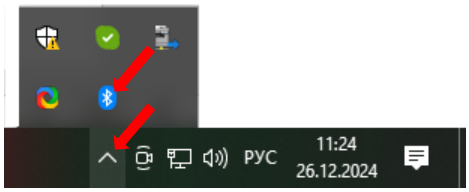


Рисунок 4.6. Панель Windows.

На панели ***Параметры*** нажмите ***Добавление Bluetooth или другого устройства.*** В открывшемся окне нажмите ***Bluetooth.*** Запустится поиск устройств Bluetooth, где должно появится имя устройства ВПУ в указанном формате (рис. 4.7).

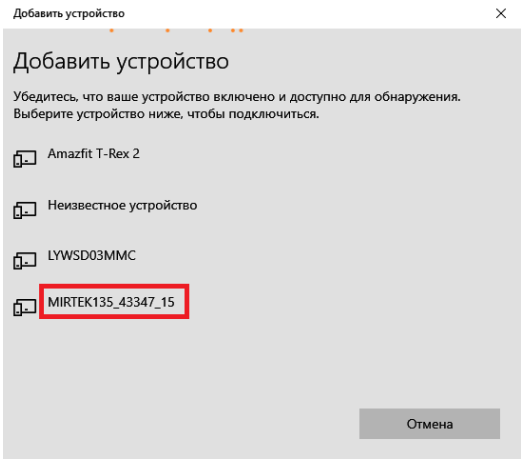


Рисунок 4.7. Поиск устройств Bluetooth.

Введите это имя в строку ***Имя устройства***, как показано на рис. 4.3.

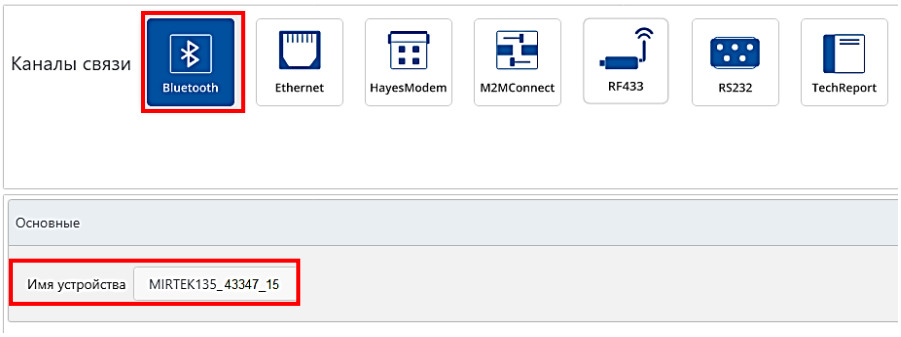


Рисунок 4.8. Пример ввода имени устройства канала связи Bluetooth.

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. Проверьте, подано ли питание к ВПУ (см п. 2).

5.2 Для первого подключения на смартфоне с ОС Android нужно запустить браузер, например ***Google Chrome,*** и ввести в строке поиска ***Rustore для андройд***. 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.

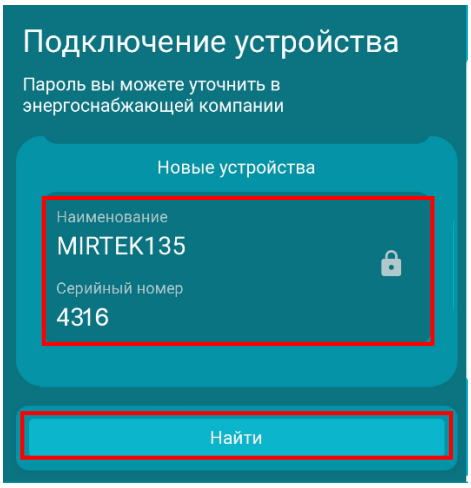


Рисунок 5.1. Пример поиска устройств в ***МИРТЕК: мобильный учет***.

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 понадобиться указать пароль для считывания данных, по умолчанию – ***12345678***, а таже адрес (по умолчанию это последние **4 цифры** номера ВПУ, например 4316). Внизу диалогового окна нажать кнопку ***Подключить***, рис. 5.2.

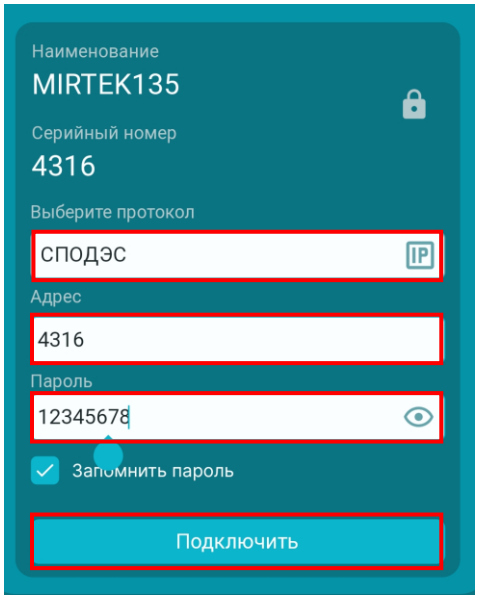
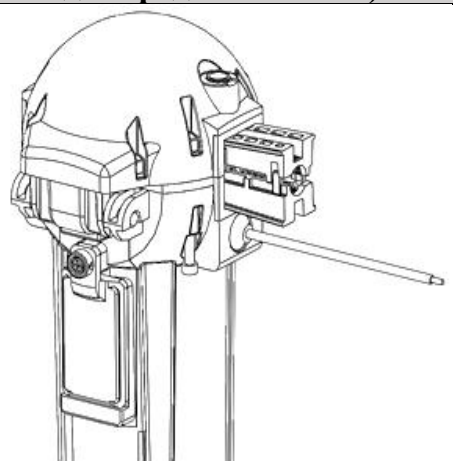
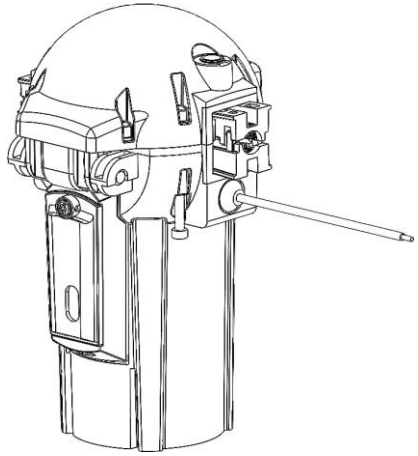


Рисунок 5.2. Пример ввода параметров подключения.

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. Отличия исполнений ВПУ при подключении по СПОДЭС

	Исполнения со встроенным модулем связи (выпускались до середины 2024 г.)	Исполнения со сменным модулем связи (выпускаются с середины 2024 г.)
		
1. При первом подключении к ВПУ	Режим доступа (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 режим доступа, и он сразу же будет функционировать в полном объёме.
2. Режимы безопасности при типе соединения «Считыватель»	Имеется 4 варианта режима доступа: 1. Стандартный 2. С проверкой подлинности 3. С шифрованием 4. С проверкой подлинности и шифрованием.	Имеется только режим доступа «Стандартный» (согласно версии 4 стандарта СТО 34.01-5.1-006-2023).
3. Выбор политики безопасности	Можно выбрать любой режим доступа: «Стандартный» (включен по умолчанию), «С проверкой подлинности», «С шифрованием», «С проверкой подлинности и шифрованием». После выбора режима безопасности на вкладке «Настройка безопасности» и нажатия кнопки «Записать» подключение к ВПУ будет происходить только в выбранном варианте политики безопасности независимо от пользовательских	Каждый режим доступа может быть заменен на следующий, т.е. если в ВПУ установлен режим «Стандартный», то к прибору можно подключиться, используя любой из 4 режимов. Если прибор настроен на режим доступа «с проверкой подлинности», то к нему можно подключиться с использованием одноименного режима, а также двух последующих: «с

	Исполнения со встроенным модулем связи (выпускались до середины 2024 г.)	Исполнения со сменным модулем связи (выпускаются с середины 2024 г.)
	установок в графе «Параметры подключения → Доступ» при подключении.	шифрованием» и «с проверкой подлинности и шифрованием»
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	Bluetooth, RF433, GSM

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

	Исполнения ВПУ «Р1»	Исполнения ВПУ «Р2»
Поддерживаемые протоколы	1. СПОДЭС (DLMS / COSEM)	1. СПОДЭС (DLMS / COSEM), 2. МИРТЕК
Поддержка SMS команд	нет	есть

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.

ПРИЛОЖЕНИЕ В. Ключи шифрования в «СПОДЭС»

Ключи \ Комплект безопасности		AES-GCM-128	ГОСТ 34.12-2018 «Кузнечик»
Аутентификации	низкой секретности*	AuthKeyLLS000001	00000000000000000000000000000001
	высокой секретности	AuthKeyHLS000001	00000000000000000000000000000001
Одноадресный	низкой секретности*	UnicastKeyLLS001	UnicastKeyLLS0000000000000000000
	высокой секретности	UnicastKeyHLS001	UnicastKeyHLS0000000000000000000
Мастер ключ		MeterMasterKey01	MeterMasterKey00000000000000000000 00000000000000000000000000000001

* в СПОДЭС 4 (ВПУ со сменным модулем связи) LLS ключи не используются.