

Скважинный прибор для измерения диэлектрических характеристик пластового флюида.

MODBUS-RTU.

Д.А. Коновалов, н.с. лаб. ФПС КФТИ ФИЦ КазНЦ РАН

1. Команды интерфейса RS-485 (MODBUS-RTU)

1.1. Описание реализации

1.1.1. Интерфейс

Прибор имеет последовательный интерфейс RS-485 и является ведомым (slave) устройством, отвечающим на команды с соответствующим адресом в пакете протокола. Поддерживается скорость передачи 9600 бит/с без контроля четности, 8 бит данных, 1 стоп-бит. По последовательному интерфейсу поддерживается протокол верхнего уровня Modbus с форматом пакета RTU в полном соответствии с документом «Modbus over Serial Line Specification & Implementation guide V1.0».

Протокол Modbus определяет элементарный пакет данных Protocol Data Unit (PDU). Структура PDU не зависит от типа линии связи и включает в себя код функции и поле данных. Код функции кодируется однобайтовым полем и может принимать значения в диапазоне 1...127. Поле данных может быть переменной длины. Размер пакета PDU ограничен 253 байтами. Для передачи пакета по физическим линиям связи PDU помещается в другой пакет, содержащий дополнительные поля. Этот пакет носит название Application Data Unit (ADU). Общая структура ADU следующая:

Application Data Unit (ADU)			
Адрес устройства	Protocol Data Unit (PDU)		CRC
	Код функции	Данные	

1.1.2. Адреса устройств Modbus

Контроллер прибора поддерживает команды Modbus в полном соответствии с синтаксисом запроса и ответа, определённым в документе «Modbus Application Protocol Specification v1.1a». Адрес устройства может быть от 0x01 до 0xF7. Диапазон адресов 0xF8-0xFF зарезервирован в стандарте Modbus. Широковещательный режим не поддерживается. Адрес контроллера прибора: 0x30.

1.1.3. Команды

Контроллер поддерживает следующие команды:

- 0x03 Чтение регистров (Read Holding Registers)
- 0x04 Чтение входных регистров (Read Input Register)
- 0x06 Запись регистра (Write Single Register)
- 0x10 Запись регистров (Write Multiple registers)

1.1.4. Адресация

Адреса запрашиваемых регистров по протоколу Modbus и адреса в памяти устройства имеют однозначное табличное соответствие, но не совпадают. Таблица соответствия адресов задаётся программистом и должна быть отражена в документации к устройству. Основным способом передачи данных по протоколу Modbus является чтение или запись регистров.

1.1.5. Регистры хранения и задания параметров (Holding Register).

Адрес регистра	Значение	Диапазон значений
0x0000	Режим выдачи результатов (Значение по умолчанию: 0)	0 – измерения не производятся; 1 – результаты ϵ и σ ; 2 – результаты в отсчетах АЦП
0x0001	Частота генератора возбуждения (Значение по умолчанию: 0)	0 – выбирается автоматически 1 – фиксированная 1... 65535 кГц.
	<i>80 регистров калибровочных параметров:</i>	0...65535
0x0002	C_1 – емкость верх. плеча	$\times 10^{-14}$ F
0x0003	C_0 – емкость ячейки на воздухе	$\times 10^{-14}$ F
0x0004	$C_{IN} + C_S$ – вх. и монтаж. емкость	$\times 10^{-14}$ F
0x0005	R_{IN} – входное сопр. AD8203	Ом
0x0006	F_{FIX} – частота фикс. генератора	$\times 10^3$ Гц
0x0007	Коэффициент АЦП GAIN	$\times 10^3$
0x0008	Коэффициент АЦП PHASE	$\times 10^3$
0x0009	Сдвиг фазы	Градусы $\times 100$
...	<i>резерв</i>	0...65535
0x0051	<i>резерв</i>	0...65535
0x0052	Команда на запись таблицы параметров в EEPROM	1 – записать таблицу в EEPROM

Чтение регистров производится командой 0x03 (Read Holding Register).

Данная функция позволяет получить двоичное содержимое 16-ти разрядных регистров адресуемого контроллера. Регистры нумеруются с нуля. Широковещательный режим не допускается. Контроллер посылает в ответе код выполненной функции и информационное поле. Информационное поле содержит 1 байт, описывающий количество возвращаемых байт данных и содержимое запрошенных регистров. Длина каждого регистра данных – 2 байта. Первый байт данных в посылке является старшим байтом регистра, второй – младшим.

PDU запроса:

Команда (Функция)	1 байт	0x03
Начальный адрес	2 байта	0x0000 .. 0xFFFF
Кол-во регистров*	2 байта	1 .. 125 (0x7D)

* Если значение поля «Кол-во регистров» равно 0 (ноль), то в ответ возвращаются значения всех регистров хранения.

PDU ответа:

Команда (Функция)	1 байт	0x03
Кол-во байт	1 байт	2 x N*
Значения регистров	N* x 2 байта	значение

* N – количество регистров.

Запись в один регистр производится командой 0x06 (Write Single Register).

В случае успешного выполнения функции ответное сообщение идентично запросу.

PDU запроса:

Команда (Функция)	1 байт	0x06
Адрес регистра	2 байта	0x0000 .. 0xFFFF
Значение регистра	2 байта	0x0000 .. 0xFFFF

PDU ответа:

Команда (Функция)	1 байт	0x06
Адрес регистра	2 байта	0x0000 .. 0xFFFF
Значение регистра	2 байта	0x0000 .. 0xFFFF

Запись в несколько регистров производится командой 0x10 (Write Multiple registers).

В случае успешного выполнения функции ответное сообщение содержит код функции, начальный адрес и количество записанных регистров.

PDU запроса:

Команда (Функция)	1 байт	0x10
Начальный адрес	2 байта	0x0000 .. 0xFFFF
Кол-во регистров	2 байта	1 .. 123 (0x7B)
Кол-во байт	1 байт	2 x N*
Значения регистров	N* x 2 байта	значение

* N – количество регистров.

PDU ответа:

Команда (Функция)	1 байт	0x10
Начальный адрес	2 байта	0x0000 .. 0xFFFF
Кол-во регистров	2 байта	0x0000 .. 0xFFFF

1.1.6. Регистры данных (Input Register).

Нач. адрес регистра	Содержание регистра
00	Режим 1 - ϵ Режим 2 - GAIN (отсчёты АЦП)
01	Режим 1 - σ (x10000) Режим 2 - PHASE (отсчёты АЦП)
02	Температура корпуса MCU (град. по Цельсию)
03	GAIN A/B(x100)
04	PHASE сдвиг фаз°(x100)
05	Температура корпуса MCU (отсчёты АЦП)
06	Vref (отсчёты АЦП)
07	VCC/2 (отсчёты АЦП)
08	VCC (В/100)
09..16	8 регистров необработанных GAIN АЦП
17..24	8 регистров необработанных PHASE АЦП

В регистрах 00..02 содержатся обработанные данные.

Регистры 03..40 содержат отладочную информацию и промежуточные данные.

Чтение регистров производится командой 0x04 (Read Input Register).

Данная функция позволяет получить двоичное содержимое 16-ти разрядных регистров адресуемого контроллера. Регистры нумеруются с нуля. Широковещательный режим не допускается. Контроллер посылает в ответе код выполненной функции и информационное поле. Информационное поле содержит 1 байт, описывающий количество возвращаемых байт данных и содержимое запрошенных регистров. Длина каждого регистра данных – 2 байта. Первый байт данных в посылке является старшим байтом регистра, второй – младшим.

PDU запроса:

Команда (Функция)	1 байт	0x04
Начальный адрес	2 байта	0x0000 .. 0xFFFF
Кол-во регистров*	2 байта	1 .. 125 (0x7D)

* Если значение поля «Кол-во регистров» равно 0 (ноль), то в ответ возвращаются значения всех регистров хранения.

PDU ответа:

Команда (Функция)	1 байт	0x04
Кол-во байт	1 байт	2 x N*
Значения регистров	N* x 2 байта	значение

* N – количество регистров.

1.1.7. Исключительные ситуации

Контроллер поддерживает сообщения информирования клиента (мастера) Modbus об исключительных ситуациях (Exception). Формат возвращаемых пакетов полностью соответствует документу «Modbus Application Protocol Specification v1.1a». Сообщения об

исключительных ситуациях возникают только на запросы, адресованные данному устройству с правильным значением CRC пакета.

Код ошибки	Название	Описание
01	Неподдерживаемая команда	Возникает только при запросе с номером команды, которую не поддерживает контроллер.
02	Неподдерживаемый адрес данных	Возникает только при запросе с адресом данных, которых нет в таблицах соответствия между адресами Modbus и внутренней памятью контроллера.
03	Неверное количество данных	Возникает при запросе количества регистров больше допустимого для заданного начального адреса.

Когда контроллер обнаруживает одну из этих ошибок, он посылает ответное сообщение, содержащее адрес, код функции, код ошибки и контрольную сумму. Для указания на то, что ответное сообщение – это уведомление об ошибке, старший бит поля кода функции устанавливается в 1.