



ООО "НПП "Призма"

Датчик LS5
Протокол обмена данными на основе Modbus RTU v1.1b
rev. E

Екатеринбург
2019

СОДЕРЖАНИЕ

1. Краткие сведения о протоколе Modbus.....	3
2. Адресное пространство для хранения параметров датчика.....	3
2.1. Формат выдаваемого результата.....	11
3. Используемые команды протокола.....	12
3.1. Запрос с кодом 03h. Чтение нескольких регистров хранения (16-тиразрядных целочисленных переменных).....	12
3.2. Запрос с кодом 05h. Изменение одного регистра флага.....	13
3.3. Запрос с кодом 06h. Изменение одного регистра хранения (16-тиразрядных целочисленных переменных).....	13
3.4. Запрос с кодом 10h. Изменение нескольких регистров хранения (16-тиразрядных целочисленных переменных).....	14
4. Контроль ошибок.....	15
4.1. RTU-фрейм.....	15
4.2. Логические ошибки.....	15
5. Алгоритм генерации контрольной суммы.....	16
5.1. Описание алгоритма.....	16
5.2. Пример подпрограммы вычисления CRC на языке С.....	17

1. КРАТКИЕ СВЕДЕНИЯ О ПРОТОКОЛЕ MODBUS

Протокол Modbus обеспечивает связь двух и более устройств по общей линии связи. Этот протокол предполагает одно ведущее (запрашивающее) устройство в линии, которое может передавать команды одному или нескольким ведомым устройствам, обращаясь к ним по уникальному в линии адресу. Датчики LS5 работают всегда в подчинённом режиме, а ведущим устройством (мастером) выступает компьютер или другое устройство пользователя.

Ведомые устройства прослушивают линию связи. Мастер подаёт запрос (последовательность байтов) в линию и переходит в состояние прослушивания линии связи. Ведомое устройство отвечает на запрос, пришедший в его адрес.

Датчики LS5 используют протокол обмена Modbus RTU (более подробно см. <http://www.modbus.org/specs.php> и http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf).

Кадры запроса и ответа по протоколу Modbus имеют фиксированный формат и имеют следующие поля: поле адреса, поле функции, поле данных, поле контрольной суммы. В протоколе Modbus RTU сообщение начинается и заканчивается интервалом тишины, продолжительностью 3,5 символа. Первым байтом передаётся поле адреса.

Каждому подчинённому устройству присваивается адрес в пределах от 1 до 255 (хотя протокол Modbus RTU ограничивает это значение до 247). Адрес 0 используется для широковещательной передачи.

Поле функции содержит байт кода команды.

Поле данных в сообщении от главного к подчинённому может содержать адреса регистров, их количество, счетчик передаваемых байтов данных. Поле данных может отсутствовать в определенных типах сообщений.

Поле контрольной суммы (CRC) состоит из двух байтов. Контрольная сумма вычисляется передающим устройством и добавляется в конец сообщения. Принимающее устройство также вычисляет контрольную сумму в процессе приема и сравнивает ее с полем CRC принятого сообщения. Если суммы не совпали – то имеет место ошибка. Контрольная сумма передаётся младшим байтом вперёд. Алгоритм генерации CRC приведён в разделе 5.

2. АДРЕСНОЕ ПРОСТРАНСТВО ДЛЯ ХРАНЕНИЯ ПАРАМЕТРОВ ДАТЧИКА

Все параметры датчика, подлежащие передаче по сети, хранятся в его памяти (в «таблице данных»). Причём каждому параметру соответствует свой индивидуальный адрес. Некоторые параметры могут как считываться, так и записываться; другие параметры можно только считать. В соответствии со спецификацией Modbus RTU v1.1b доступ к элементам в каждой таблице осуществляется с помощью 16-битного адреса, первой ячейке соответствует адрес 0. Таким образом, каждая таблица может содержать до 65536 элементов. Спецификация не определяет, что физически должны представлять собой элементы таблиц и по каким внутренним адресам устройства они должны быть доступны. Поэтому допустимо организовать перекрывающиеся таблицы, что и сделано в датчиках LS5. В этом случае команды, работающие с однобитными данными и с 16-битными регистрами, будут фактически обращаться к одним и тем же данным.

Адресное пространство в датчиках распределено так, как показано на рис. 2.1, 2.2. Более подробно все параметры описаны в табл. 2.1–2.4. Здесь и далее все значения приведены в шестнадцатеричном формате. Конфигурации датчиков с интерфейсом Ethernet и без него различаются наличием специальных параметров для Ethernet-сети, поэтому адресные пространства Modbus для этих конфигураций тоже различаются. Интерфейс Ethernet поддерживается в датчиках с версиями программного обеспечения (прошивки) «LS5.12.1» и выше.

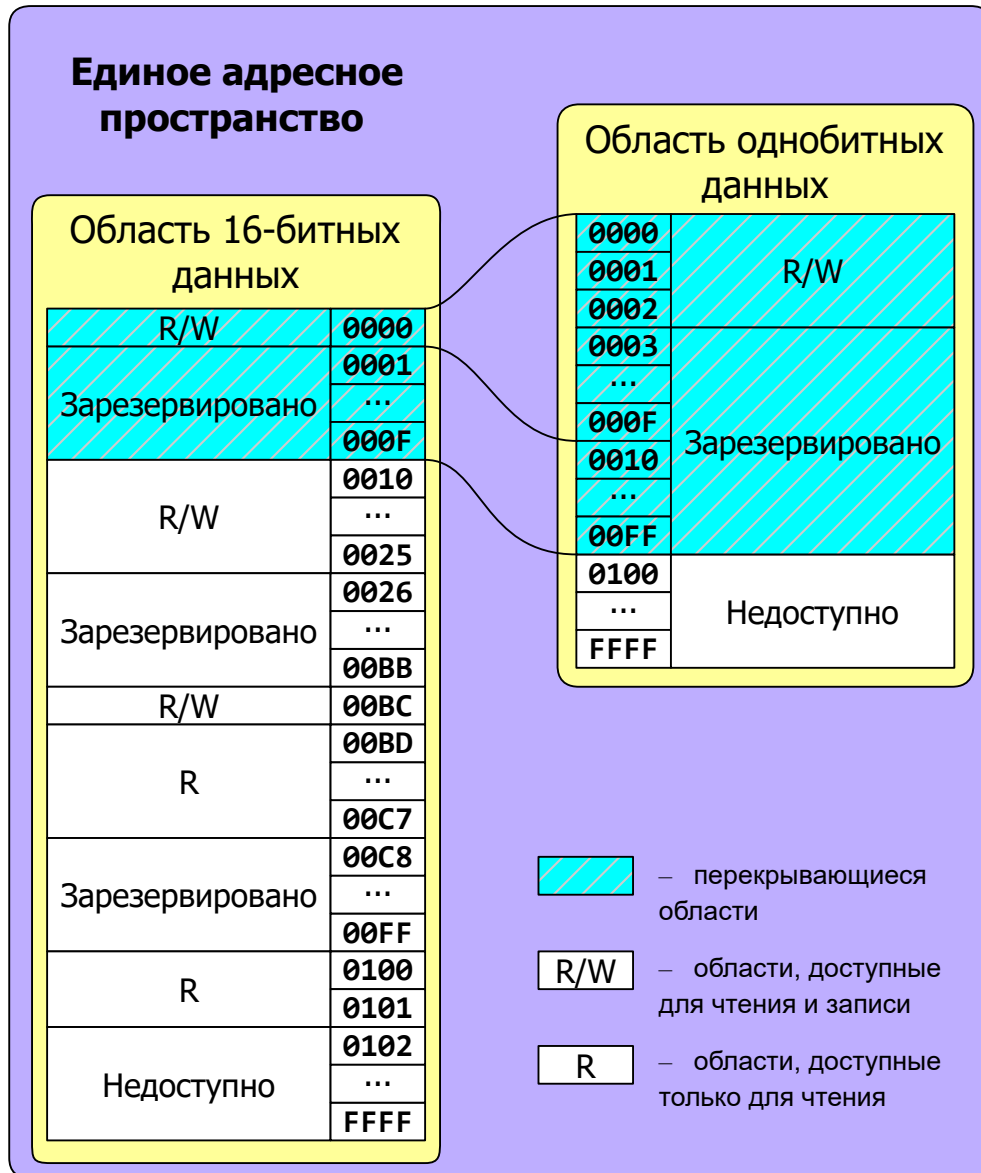


Рисунок 2.1 – Адресное пространство для хранения параметров датчика (для конфигурации без интерфейса Ethernet, т. е. для версий прошивок ниже «LS5.12.1»)

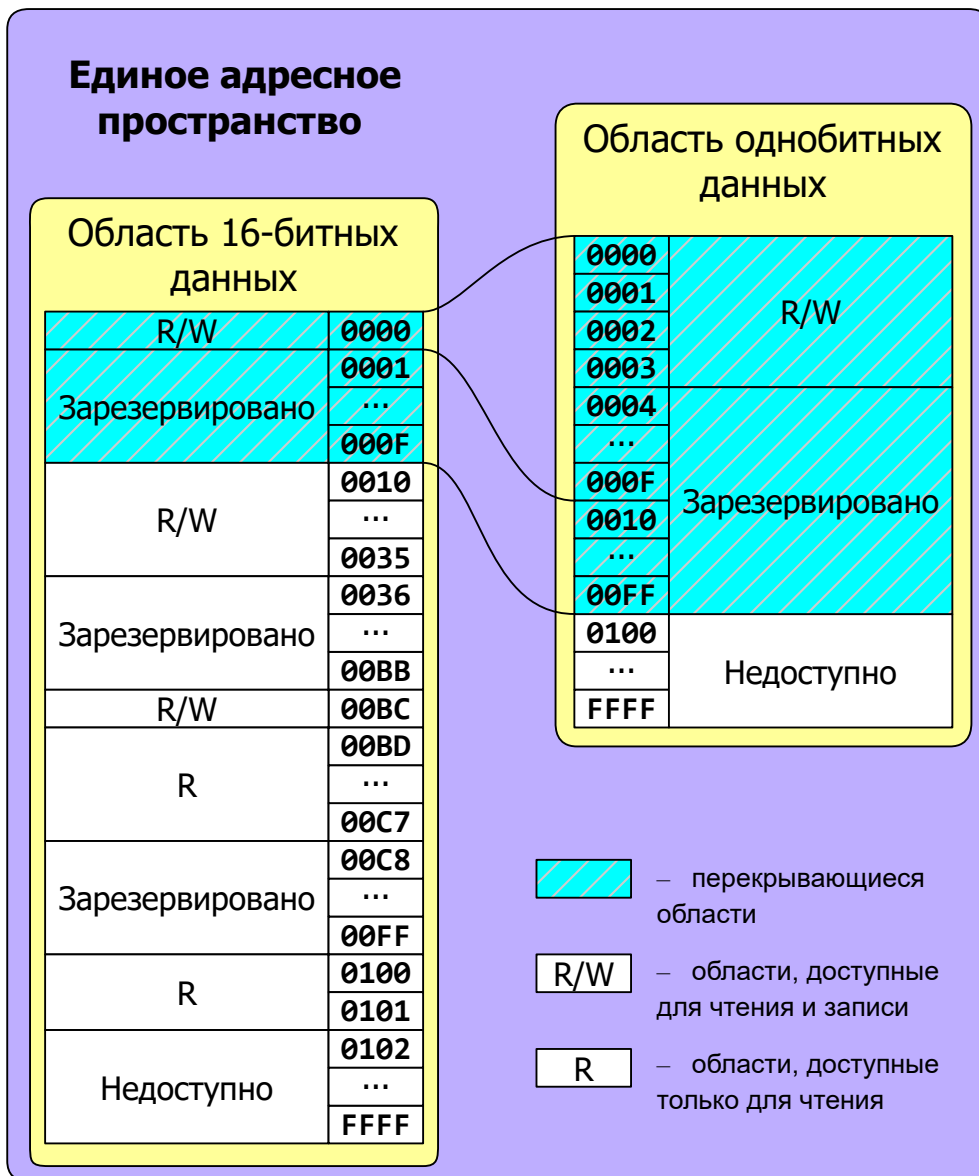


Рисунок 2.2 – Адресное пространство для хранения параметров датчика (для конфигурации с интерфейсом Ethernet, т. е. для версии прошивок «LS5.12.1» и выше)

Таблица 2.1 – Однобитные параметры (флаги) и их адресация (в однобитном адресном пространстве) для конфигурации **без интерфейса Ethernet**, т. е. для версий прошивок ниже «LS5.12.1»

Адрес (hex)	Возможность чтения/записи (R/W)	Параметр	Принимаемые значения (hex)	Значение по умолчанию (hex)
0000	R/W	Датчик включен/выключен при подаче питания	0 – выкл. 1 – вкл.	1
0001	R/W	Аналоговый выход включен/выключен	0 – выкл. 1 – вкл.	1
0002	R/W	Синхронизация	0 – по таймеру 1 – по меандру	0
0003-00FF		Зарезервировано ¹		
0100-FFFF		Недоступно ²		

Таблица 2.2 – Однобитные параметры (флаги) и их адресация (в однобитном адресном пространстве) для конфигурации с интерфейсом Ethernet, т. е. для версии прошивок «LS5.12.1» и выше

Адрес (hex)	Возможность чтения/записи (R/W)	Параметр	Принимаемые значения (hex)	Значение по умолчанию (hex)
0000	R/W	Датчик включен/выключен при подаче питания	0 – выкл. 1 – вкл.	1
0001	R/W	Аналоговый выход включен/выключен	0 – выкл. 1 – вкл.	1
0002	R/W	Синхронизация	0 – по таймеру 1 – по меандру	0
0003	R/W	Автопоток UDP-данных	0 – выкл. 1 – вкл.	1
0004-00FF		Зарезервировано ¹		
0100-FFFF		Недоступно ²		

Примечания:

¹ В случае обращения к зарезервированным регистрам: а) при чтении регистров устройство выдаст нулевые значения зарезервированных регистров; б) при записи в регистры устройство выдаст код ошибки.

² При обращении (чтение или запись) к недоступным регистрам устройство выдаст код ошибки.

Таблица 2.3 – 16-битное адресное пространство датчиков LS5 версии прошивок ниже «LS5.12.1»

Адрес (hex)	Возможность чтения/записи (R/W)	Параметр	Принимаемые значения (hex)	Значение по умолчанию (hex)
0000	R/W	16-битный регистр флагов ¹	0000 - 0007	0003
0001-000F		Зарезервировано ²		
0010	R/W	Сетевой адрес	0000 - 00FF	0001
0011	R/W	Формат байта при работе с последовательными протоколами: 00 – паритета нет, 1 стоп-бит; 01 – контроль четности, 1 стоп-бит; 02 – контроль нечетности, 1 стоп-бит; 03 – паритета нет, 2 стоп-бита; 04 – контроль четности, 2 стоп-бита; 05 – контроль нечетности, 2 стоп-бита.	0000 - 0005	0000
0012	R/W	Скорость последовательного интерфейса: 01 – 9600 бод; 02 – 19200 бод; 03 – 38400 бод; 04 – 57600 бод; 05 – 115200 бод; 06 – 230400 бод; 07 – 460800 бод; 08 – 921600 бод.	0001 - 0008	0005
0013	R/W	Период измерения датчика и заполнения буфера предварительной обработки (дискрет – 0,1 мс; минимальное значение – 0,1 мс): $t = (\text{значение параметра}) * 0,1 [\text{мс}]$. Например: для $t = 1$ мс параметр равен 000A; для $t = 5,2$ мс параметр равен 0034.	0001 - FFFF	0064 (соответствует 10 мс)
0014	R/W	Константа n , задающая период выдачи данных при потоковом режиме: $n = T/t,$ где t – период измерения датчика, T – период выдачи результатов датчиком.	0001 - FFFF	0001
0015	R/W	Допустимое время отсутствия сигнала (дискретность – 1 мс)	0000 - FFFF	000A
0016	R/W	Тип предварительной фильтрации данных: 00 – скользящее усреднение по k значениям; 01 – медианная фильтрация с окном m .	0000, 0001	0000

Адрес (hex)	Возможность чтения/записи (R/W)	Параметр	Принимаемые значения (hex)	Значение по умолчанию (hex)
0017	R/W	Количество точек усреднения, k	0001 – 00FF	0001
0018	R/W	Количество точек медианного фильтра, m (должно быть нечётным: $m = 2h + 1$, где $h = 0, 1, \dots, 24$)	0001, 0003, 0005, ..., 0031	0005
0019	R/W	Нижняя граница аналогового выхода	0000 – C350	0000
001A	R/W	Верхняя граница аналогового выхода	0000 – C350	C350
001B	R/W	Настройка дискретных выходов: 00XY , где X отвечает за первый выход, Y – за второй. 0 – дискретный выход выключен; 1 – дискретный выход включен (начальное значение – 0); 2 – дискретный выход включен (начальное значение – 1); Пример: 12 – первый выход включен, с начальным значением «0», второй выход включен с начальным значением «1».	0000, 0001, 0002, 0010, 0011, 0012, 0020, 0021, 0022	0012
001C	R/W	Первый перепад первого дискретного выхода	0000 – C350	0000
001D	R/W	Второй перепад первого дискретного выхода	0000 – C350	C350
001E	R/W	Первый перепад второго дискретного выхода	0000 – C350	0000
001F	R/W	Второй перепад второго дискретного выхода	0000 – C350	C350
0020	R/W	Максимальное время экспозиции (в микросекундах)	0001 – FFFF	24B8
0021	R/W	Приоритет частоты измерения/чувствительности 0000 – приоритет частоты 0001 – приоритет чувствительности	0000, 0001	0001
0022	R/W	0000 – выключено; 0001 – включено, только с записью в защёлку; 0002 – включено, кроме записи в защёлку делается пересчёт границ аналогового выхода (с учётом параметра «Фиксируемый диапазон аналогового выхода»); 0003 – то же, что для значения 02 , только значения границ аналогового выхода ещё записываются в ПЗУ; 0004 – включено, кроме записи в защёлку делается пересчёт границ 1-го дискретного выхода (с учётом параметра «Фиксируемый диапазон дискретных выходов»); 0005 – то же, что для значения 04 , только значения границ 1-го дискретного выхода ещё записываются в ПЗУ; 0006 – включено, кроме записи в защёлку делается пересчёт границ 2-го дискретного выхода (с учётом параметра «Фиксируемый диапазон дискретных выходов»); 0007 – то же, что для значения 06 , только значения границ 2-го дискретного выхода ещё записываются в ПЗУ; 0008 – включено, кроме записи в защёлку делается пересчёт нижней границы 1-го и верхней границы 2-го дискретных выходов (с учётом параметра «Фиксируемый диапазон дискретных выходов»); 0009 – то же, что для значения 08 , только значения границ соответствующих дискретных выходов ещё записываются в ПЗУ.	0001 – 0009	0001
0023	R/W	Тип предварительного результата: 00 – в чистом виде; 01 – производная сигнала (разность текущего и предыдущего результата)	0000, 0001	0000
0024	R/W	Фиксируемый диапазон аналогового выхода	0000 – FFFF	2710
0025	R/W	Фиксируемый диапазон дискретных выходов	0000 – FFFF	2710
0026-00BB		Зарезервировано ²		
00BC	R/W	2 байта ASCII-кода	См. табл. 3.7	XXXX ³

Адрес (hex)	Возможность чтения/записи (R/W)	Параметр		Принимаемые значения (hex)	Значение по умолчанию (hex)
00BD	R	1 и 2 байты	Модель устройства (10 символов в ASCII-коде)	0000 - FFFF	-
00BE	R	3 и 4 байты		0000 - FFFF	-
00BF	R	5 и 6 байты		0000 - FFFF	-
00C0	R	7 и 8 байты		0000 - FFFF	-
00C1	R	9 и 10 байты		0000 - FFFF	-
00C2	R	1 и 2 байты	Минимальное расстояние до объекта измерения, H , мм $H = ((1 \text{ байт}) * 16777216 +$	0000 - FFFF	-
00C3	R	3 и 4 байты	$(2 \text{ байт}) * 65536 +$ $(3 \text{ байт}) * 256 +$ $(4 \text{ байт}) / 1000$	0000 - FFFF	-
00C4	R	1 и 2 байты	Диапазон измерения датчика, D , мм $D = ((1 \text{ байт}) * 16777216 +$	0000 - FFFF	-
00C5	R	3 и 4 байты	$(2 \text{ байт}) * 65536 +$ $(3 \text{ байт}) * 256 +$ $(4 \text{ байт}) / 1000$	0000 - FFFF	-
00C6	R	1 и 2 байты	Серийный номер устройства: $sn = (1 \text{ байт}) * 16777216 +$	0000 - FFFF	-
00C7	R	3 и 4 байты	$(2 \text{ байт}) * 65536 +$ $(3 \text{ байт}) * 256 +$ (4 байт)	0000 - FFFF	-
00C8-00FF	Зарезервировано ²				
0100	R	Защёлкнутый результат		0000 - C350, FFFE, FFFF	FFFE ⁴
0101	R	Последнее измеренное значение		0000 - C350, FFFE, FFFF	FFFE ⁴
0102-FFFF	Недоступно ⁵				

Таблица 2.4 – 16-битное адресное пространство датчиков LS5 версий прошивок «LS5.12.1» и выше

Адрес (hex)	Возможность чтения/записи (R/W)	Параметр		Принимаемые значения (hex)	Значение по умолчанию (hex)
0000	R/W	16-битный регистр флагов ¹		0000 - 000F	000B
0001-000F	Зарезервировано ²				
0010	R/W	Сетевой адрес		0000 - 00FF	0001
0011	R/W	Формат байта при работе с последовательными протоколами: 00 – паритета нет, 1 стоп-бит; 01 – контроль четности, 1 стоп-бит; 02 – контроль нечетности, 1 стоп-бит; 03 – паритета нет, 2 стоп-бита; 04 – контроль четности, 2 стоп-бита; 05 – контроль нечетности, 2 стоп-бита.		0000 - 0005	0000
0012	R/W	Скорость последовательного интерфейса: 01 – 9600 бод; 02 – 19200 бод; 03 – 38400 бод; 04 – 57600 бод; 05 – 115200 бод; 06 – 230400 бод; 07 – 460800 бод; 08 – 921600 бод.		0001 - 0008	0005

Адрес (hex)	Возможность чтения/записи (R/W)	Параметр	Принимаемые значения (hex)	Значение по умолчанию (hex)
0013	R/W	Период измерения датчика и заполнения буфера предварительной обработки (дискрет – 0,1 мс; минимальное значение – 0,1 мс): $t = (\text{значение параметра}) * 0,1 \text{ [мс]}$. Например: для $t = 1$ мс параметр равен 000A ; для $t = 5,2$ мс параметр равен 0034 .	0001 - FFFF	0064 (соответствует 10 мс)
0014	R/W	Константа n , задающая период выдачи данных при потоковом режиме: $n = T/t$, где t – период измерения датчика, T – период выдачи результатов датчиком.	0001 - FFFF	0001
0015	R/W	Допустимое время отсутствия сигнала (дискретность – 1 мс)	0000 - FFFF	000A
0016	R/W	Тип предварительной фильтрации данных: 00 – скользящее усреднение по k значениям; 01 – медианная фильтрация с окном m .	0000, 0001	0000
0017	R/W	Количество точек усреднения, k	0001 - 00FF	0001
0018	R/W	Количество точек медианного фильтра, m (должно быть нечётным: $m = 2h + 1$, где $h = 0, 1, \dots, 24$)	0001, 0003, 0005, ..., 0031	0005
0019	R/W	Нижняя граница аналогового выхода	0000 - C350	0000
001A	R/W	Верхняя граница аналогового выхода	0000 - C350	C350
001B	R/W	Настройка дискретных выходов: 00XY , где X отвечает за первый выход, Y – за второй. 0 – дискретный выход выключен; 1 – дискретный выход включен (начальное значение – 0); 2 – дискретный выход включен (начальное значение – 1); Пример: 12 – первый выход включен, с начальным значением «0», второй выход включен с начальным значением «1».	0000, 0001, 0002, 0010, 0011, 0012, 0020, 0021, 0022	0012
001C	R/W	Первый перепад первого дискретного выхода	0000 - C350	0000
001D	R/W	Второй перепад первого дискретного выхода	0000 - C350	C350
001E	R/W	Первый перепад второго дискретного выхода	0000 - C350	0000
001F	R/W	Второй перепад второго дискретного выхода	0000 - C350	C350
0020	R/W	Максимальное время экспозиции (в микросекундах)	0001 - FFFF	24B8
0021	R/W	Приоритет частоты измерения/чувствительности 0000 – приоритет частоты 0001 – приоритет чувствительности	0000, 0001	0001

Адрес (hex)	Возможность чтения/записи (R/W)	Параметр	Принимаемые значения (hex)	Значение по умолчанию (hex)
0022	R/W	<p>0000 – выключено;</p> <p>0001 – включено, только с записью в защёлку;</p> <p>0002 – включено, кроме записи в защёлку делается пересчёт границ аналогового выхода (с учётом параметра «Фиксируемый диапазон аналогового выхода»);</p> <p>0003 – то же, что для значения 02, только значения границ аналогового выхода ещё записываются в ПЗУ;</p> <p>0004 – включено, кроме записи в защёлку делается пересчёт границ 1-го дискретного выхода (с учётом параметра «Фиксируемый диапазон дискретных выходов»);</p> <p>0005 – то же, что для значения 04, только значения границ 1-го дискретного выхода ещё записываются в ПЗУ;</p> <p>0006 – включено, кроме записи в защёлку делается пересчёт границ 2-го дискретного выхода (с учётом параметра «Фиксируемый диапазон дискретных выходов»);</p> <p>0007 – то же, что для значения 06, только значения границ 2-го дискретного выхода ещё записываются в ПЗУ;</p> <p>0008 – включено, кроме записи в защёлку делается пересчёт нижней границы 1-го и верхней границы 2-го дискретных выходов (с учётом параметра «Фиксируемый диапазон дискретных выходов»);</p> <p>0009 – то же, что для значения 08, только значения границ соответствующих дискретных выходов ещё записываются в ПЗУ.</p>	0001 - 0009	0001
0023	R/W	<p>Тип предварительного результата:</p> <p>00 – в чистом виде;</p> <p>01 – производная сигнала (разность текущего и предыдущего результата)</p>	0000, 0001	0000
0024	R/W	Фиксируемый диапазон аналогового выхода	0000 - FFFF	2710
0025	R/W	Фиксируемый диапазон дискретных выходов	0000 - FFFF	2710
0026	R/W	IP-адрес датчика: 0-й и 1-й байты	0000 - FFFF	C0A8
0027	R/W	IP-адрес датчика: 2-й и 3-й байты	0000 - FFFF	0003
0028	R/W	IP-адрес шлюза: 0-й и 1-й байты	0000 - FFFF	C0A8
0029	R/W	IP-адрес шлюза: 2-й и 3-й байты	0000 - FFFF	0001
002A	R/W	Маска подсети: 0-й и 1-й байты	0000 - FFFF	FFFF
002B	R/W	Маска подсети: 2-й и 3-й байты	0000 - FFFF	FFFF
002C	R/W	IP-адрес назначения: 0-й и 1-й байты	0000 - FFFF	FFFF
002D	R/W	IP-адрес назначения: 2-й и 3-й байты	0000 - FFFF	FFFF
002E	R/W	MAC-адрес датчика: 0-й и 1-й байты	0000 - FFFF	1E30
002F	R/W	MAC-адрес датчика: 2-й и 3-й байты	0000 - FFFF	6CA2
0030	R/W	MAC-адрес датчика: 4-й и 5-й байты	0000 - FFFF	-
0031	R/W	MAC-адрес назначения: 0-й и 1-й байты	0000 - FFFF	FFFF
0032	R/W	MAC-адрес назначения: 2-й и 3-й байты	0000 - FFFF	FFFF
0033	R/W	MAC-адрес назначения: 4-й и 5-й байты	0000 - FFFF	FFFF
0034	R/W	Номер порта назначения	0001 - FFFF	025B
0035	R/W	Номер порта источника	0001 - FFFF	1388
0036-00BB		Зарезервировано ²		
00BC	R/W	2 байта ASCII-кода	См. табл. 3.7	XXXX ³

Адрес (hex)	Возможность чтения/записи (R/W)	Параметр		Принимаемые значения (hex)	Значение по умолчанию (hex)
00BD	R	1 и 2 байты	Модель устройства (10 символов в ASCII-коде)	0000 - FFFF	-
00BE	R	3 и 4 байты		0000 - FFFF	-
00BF	R	5 и 6 байт		0000 - FFFF	-
00C0	R	7 и 8 байты		0000 - FFFF	-
00C1	R	9 и 10 байты		0000 - FFFF	-
00C2	R	1 и 2 байты	Минимальное расстояние до объекта измерения, Н, мм $H = ((1 \text{ байт}) * 16777216 +$	0000 - FFFF	-
00C3	R	3 и 4 байты	$(2 \text{ байт}) * 65536 +$ $(3 \text{ байт}) * 256 +$ $(4 \text{ байт}) / 1000$	0000 - FFFF	-
00C4	R	1 и 2 байты	Диапазон измерения датчика, D, мм $D = ((1 \text{ байт}) * 16777216 +$	0000 - FFFF	-
00C5	R	3 и 4 байты	$(2 \text{ байт}) * 65536 +$ $(3 \text{ байт}) * 256 +$ $(4 \text{ байт}) / 1000$	0000 - FFFF	-
00C6	R	1 и 2 байты	Серийный номер устройства: $sn = (1 \text{ байт}) * 16777216 +$	0000 - FFFF	-
00C7	R	3 и 4 байты	$(2 \text{ байт}) * 65536 +$ $(3 \text{ байт}) * 256 +$ (4 байт)	0000 - FFFF	-
00C8-00FF	Зарезервировано ²				
0100	R	Защёлкнутый результат		0000 - C350, FFFE, FFFF	FFFE ⁴
0101	R	Последнее измеренное значение		0000 - C350, FFFE, FFFF	FFFE ⁴
0102-FFFF	Недоступно ⁵				

Примечания:

¹ При чтении 16-битного регистра флагов считываются также и зарезервированные биты (для дополнения до 16 бит). Считываемые зарезервированные биты всегда сброшены, запись в них какого-либо значения игнорируется датчиком.

² В случае обращения к зарезервированным регистрам: а) при чтении регистров устройство выдаст нулевые значения зарезервированных регистров; б) при записи в регистры устройство выдаст код ошибки.

³ Запись **XXXX** означает, что как такового значения по умолчанию нет. При включении питания устройства это значение равно **0**; при передаче датчику, например, команды «Восстановить параметры по умолчанию» это значение станет равным **“DF” (4446h)**. См. также раздел 3.3.

⁴ Запись **FFFE** означает, что датчик не сделал ещё ни одного измерения и выдавать пока нечего (см. раздел 2.1).

⁵ При обращении (чтение или запись) к недоступным регистрам устройство выдаст код ошибки.

2.1. Формат выдаваемого результата

Результаты измерения датчика выдаются в виде кода в диапазоне от 0 до 50000 (**C350h**). Числу 0 соответствует начальная точка диапазона, числу 50000 – конечная. Для расчета фактического значения дальности (в миллиметрах) относительно начальной точки диапазона нужно использовать следующую формулу:

$$\text{дальность} = \text{диапазон} \cdot \frac{\text{код}}{50000},$$

где *код* – результат, выдаваемый датчиком, *диапазон* – диапазон датчика в миллиметрах (неизменяемое значение, соответствующее данному датчику).

Кроме диапазона 0...50000 ещё используются два специальных значения:

65534 – для указания на то, что датчик не сделал ещё ни одного измерения и выдавать пока нечего;

65535 – для указания на то, что сигнал отсутствует.

3. ИСПОЛЬЗУЕМЫЕ КОМАНДЫ ПРОТОКОЛА

В датчиках LS5 используются стандартные команды протокола Modbus с кодами: **03h** (чтение нескольких регистров хранения), **05h** (изменение одного регистра флага), **06h** (изменение одного регистра хранения), **10h** (изменение нескольких регистров хранения).

3.1. Запрос с кодом **03h**.

Чтение нескольких регистров хранения (16-тиразрядных целочисленных переменных)

Адреса регистров хранения, к которым можно обратиться по этой команде, приведены в табл. 2.3 и на рис. 2.1.

Широковещательный запрос не поддерживается.

Форма запроса и ответ датчика приведены соответственно в таблицах 3.1, 3.2.

Таблица 3.1 – Запрос с кодом **03h**

Сетевой адрес	Код команды	Адрес первого регистра		Количество регистров для чтения (N)		CRC-16	
		ст. байт	мл. байт	ст. байт	мл. байт	мл. байт	ст. байт
01	03						

Таблица 3.2 – Ответ на запрос с кодом **03h**

Сетевой адрес	Код команды	Количество байтов в ответе	Данные (N*2 байт)			CRC-16	
			Значение 1-го регистра	...	Значение N-го регистра	мл. байт	ст. байт
01	03	N*2					

Количество регистров для чтения в запросе должно быть не более 125, в противном случае устройство выдаст код ошибки (см. табл. 4.2).

Пример:

Для считывания модели, минимального расстояния, диапазона и серийного номера датчика можно воспользоваться командой:

Запрос:

01 03 00 0D 00 0B 94 29

Ответ:

01 03 16 20 20 20 4C 53 35 2E 36 2E 30 00 00 C3 50 00 01 86 A0 00 00 01 52 86 B4,

где

20 20 20 4C 53 35 2E 36 2E 30 – модель датчика (« LS5.6.0» – в ASCII коде);

00 00 C3 50 – минимальное расстояние до объекта измерения (50 мм при переводе в десятичный формат (см. табл. 2.3));

00 01 86 A0 – диапазон (100 мм при переводе в десятичный формат (см. табл. 2.3));

00 00 01 52 – шестнадцатеричный серийный номер датчика (338 в десятичном формате (см. табл. 2.3)).

3.2. Запрос с кодом 05h.

Изменение одного регистра флага

Исходя из особенностей адресного пространства однобитных данных для датчика LS5, для этого запроса доступны регистры с адресами: **0000-0002** (см. табл. 2.1). В случае широковещательного запроса ответа нет.

Таблица 3.3 – Запрос с кодом 05h

Сетевой адрес	Код команды	Адрес регистра флага		Значение флага		CRC-16	
		ст. байт	мл. байт	ст. байт (FFh или 00h)	мл. байт (00h)	мл. байт	ст. байт
01	05						

Таблица 3.4 – Ответ на запрос с кодом 05h (повторяет запрос)

Сетевой адрес	Код команды	Адрес регистра флага		Значение флага		CRC-16	
		ст. байт	мл. байт	ст. байт (FFh или 00h)	мл. байт (00h)	мл. байт	ст. байт
01	05						

Значение флага **FF00h** означает, что флаг установлен, значение **0000h** – флаг сброшен.

Чтобы изменить несколько настроечных параметров одной командой, воспользуйтесь запросом с кодом **06h** с доступом к регистру хранения **0000** (см. раздел 3.3).

Пример:

Запрос:

01 05 00 00 FF 00 8C 3A

Эта команда послана датчику с сетевым адресом 1 для установки параметра «Включение при подаче питания».

Ответное сообщение:

01 05 00 00 FF 00 8C 3A

3.3. Запрос с кодом 06h.

Изменение одного регистра хранения (16-тиразрядных целочисленных переменных)

Этот запрос доступен для регистров с адресами **0000h**, **0010h-0025h**, **00BCh** (см. табл. 2.3). При записи в регистры для чтения устройство выдаст код ошибки (см. табл. 4.2).

В случае широковещательного запроса ответа нет.

Таблица 3.5 – Запрос с кодом 06h

Сетевой адрес	Код команды	Адрес регистра		Новое значение регистра		CRC-16	
		ст. байт	мл. байт	ст. байт	мл. байт	мл. байт	ст. байт
01	06						

Таблица 3.6 – Ответ на запрос с кодом 06h (повторяет принятый запрос)

Сетевой адрес	Код команды	Номер регистра		Новое значение регистра		CRC-16	
		ст. байт	мл. байт	ст. байт	мл. байт	мл. байт	ст. байт
01	06						

Регистр с адресом **00BCh** служит приёмником специальных управляющих датчиком параметров (перечисленных в табл. 3.7). Эти параметры посылаются внутри запросов с кодами **06h** и **10h** в виде слова (в поле «Новое значение регистра»), а именно двух байтов ASCII-кода. Регистр с ад-

ресом **00BCh** всегда можно прочитать, чтобы узнать последнюю принятую устройством по протоколу Modbus специальную команду.

Таблица 3.7 – Параметры специальных команд, посылаемых в запросе с кодом функции **06h** по адресу регистра **00BCh**

Назначение команды	Параметр (2 байта в ASCII-коде)
Запись параметров в энергонезависимую память	FL (46h 4Ch)
Включить датчик	ON (4Fh 4Eh)
Выключить датчик	OF (4Fh 46h)
Защелкнуть результат	FX (46h 58h)
Восстановить параметры по умолчанию	DF (44h 46h)

Пример:

Запрос:

01 06 00 BC 46 58 7B B4

Это команда «Защелкнуть результат» для датчика с сетевым адресом 1.

Ответ:

01 06 00 BC 46 58 7B B4

После получения команды «Защелкнуть результат», датчик сделает измерение и сохранит измеренное значение в регистре по адресу **0100h**.

3.4. Запрос с кодом **10h**.

Изменение нескольких регистров хранения (16-тиразрядных целочисленных переменных)

Этот запрос доступен для регистров с адресами **0000h**, **0010h–0025h**, **00BCh** (см. табл. 2.3 и рис. 2.1). При записи в регистры для чтения устройство выдаст код ошибки (см. табл. 4.2).

В случае широковещательного запроса ответа нет.

Таблица 3.8 – Запрос с кодом **10h**

Сетевой адрес	Код команды	Адрес первого регистра		Число регистров для записи (N)		Количество записываемых байт (2*N)	...			
		ст. байт	мл. байт	ст. байт	мл. байт		XX	...		
01	10	Записываемые данные (N*2 байт)						CRC-16		
		...		Значение 1-го регистра		...	Значение N-го регистра		мл. байт	ст. байт
		ст. байт	мл. байт	ст. байт	мл. байт	ст. байт	мл. байт			

Таблица 3.9 – Ответ на запрос с кодом **10h**

Сетевой адрес	Код команды	Адрес первого регистра		Количество записанных регистров (N байт)		CRC-16	
		ст. байт	мл. байт	ст. байт	мл. байт	мл. байт	ст. байт
01	10	ст. байт	мл. байт	ст. байт	мл. байт	мл. байт	ст. байт

Количество записываемых регистров в запросе должно быть не более 125, в противном слу-

чае устройство выдаст код ошибки (см. табл. 4.2).

Пример:

Запрос:

01 10 00 19 00 02 04 C3 50 00 00 0E 9C

Этой командой устанавливаются новые значения нижней границы аналогового выхода (**C3 50**) и верхней границы аналогового выхода (**00 00**).

Ответ:

01 10 00 19 00 02 90 0F

4. КОНТРОЛЬ ОШИБОК

Во время обмена данными могут возникать ошибки двух типов:

- ошибки, связанные с искажениями при передаче данных;
- логические ошибки.

Ошибки первого типа обнаруживаются при помощи фреймов символов, контроля чётности и циклической контрольной суммы CRC-16 (используется число-полином **A001h**).

4.1. RTU-фрейм

В RTU режиме сообщение должно начинаться и заканчиваться интервалом тишины – временем не менее 3,5 символов при данной скорости в сети. Новое сообщение может начинаться после этого интервала.

Фрейм сообщения передаётся непрерывно. Если интервал тишины продолжительностью 1,5 возник во время передачи фрейма, принимающее устройство должно игнорировать этот фрейм как неполный.

При скорости 9600 и 11 битах в кадре (стартовый бит + 8 бит данных + бит контроля чётности + стоп-бит) интервал тишины продолжительностью 3,5 символа равен $3,5 \cdot 11 / 9600 = 0,00401041(6)$, то есть более 4 мс; интервал тишины продолжительностью 1,5 символа равен $1,5 \cdot 11 / 9600 = 0,00171875$, то есть более 1 мс. Для скоростей более 19200 бод допускается использовать интервалы 1,75 и 0,75 мс соответственно.

4.2. Логические ошибки

Для сообщений об ошибках второго типа протокол Modbus RTU предусматривает, что устройства могут отсылать ответы, свидетельствующие об ошибочной ситуации. Признаком того, что ответ содержит сообщение об ошибке, является установленный старший бит кода команды. Пример кадра при выявлении ошибки ведомым устройством (датчиком), в ответ на запрос приведён в табл. 4.1.

Поведение при наличии/отсутствии логических ошибок:

- 1) Если датчик принимает корректный запрос и может его нормально обработать, то возвращает нормальный ответ;
- 2) Если датчик не принимает какого-либо значения, никакого ответа не отправляется. Управляющее устройство диагностирует ошибку по таймауту;
- 3) Если датчик принимает запрос, но обнаруживает ошибку при подсчёте контрольной суммы, никакого ответа не отправляется. Управляющее устройство диагностирует ошибку по таймауту;
- 4) Если датчик принимает запрос, но не может его обработать (обращение к недоступному

регистру и т. д.), отправляется ответ, содержащий в себе данные об ошибке (см. раздел 4.2).

Таблица 4.1 – Кадр ответа при возникновении ошибки Modbus RTU

Направление передачи	Сетевой адрес	Код команды	Данные (или код ошибки)	CRC
Запрос	01	04	01 01 00 01	61 F6
Ответ	01	84	01	82 C0

В этом примере датчик нашёл ошибку в запросе – код команды **04h** не поддерживается датчиками LS5.

Таблица 4.2 – Коды ошибок, применяемые в датчиках LS5

Код	Расшифровка
01	Не поддерживаемый код команды
02	Адрес данных, указанный в запросе, недоступен
03	Величина, содержащаяся в поле данных запроса, является недопустимой величиной
04	Ошибка записи во Flash
05	Недопустимое количество запрашиваемых регистров
06	Недопустимая операция: запись в регистры, предназначенные только для чтения
07	Недопустимая операция: запись в зарезервированные регистры

5. АЛГОРИТМ ГЕНЕРАЦИИ КОНТРОЛЬНОЙ СУММЫ

5.1. Описание алгоритма

- 16-ти битовый регистр загружается числом **FFFFh**, и используется далее как регистр CRC.
- Первый байт сообщения складывается по ИСКЛЮЧАЮЩЕМУ ИЛИ с содержимым регистра CRC. Результат помещается в регистр CRC.
- Регистр CRC сдвигается вправо (в направлении младшего бита) на 1 бит, старший бит обнуляется.
- (Если младший бит **0**): Повторяется шаг 3 (сдвиг)
(Если младший бит **1**): Делается операция ИСКЛЮЧАЮЩЕЕ ИЛИ регистра CRC и полиномиального числа **A001h**.
- Шаги 3 и 4 повторяются восемь раз.
- Повторяются шаги со 2 по 5 для следующего сообщения. Это повторяется до тех пор, пока все байты сообщения не будут обработаны.
- Финальное содержание регистра CRC и есть контрольная сумма.

5.2. Пример подпрограммы вычисления CRC на языке C

```
// Подпрограмма вычисления контрольной суммы
int CRC_control(char *mas, char len)
{
    int i,j,c,result;

    result = 0xffff;

    for (j=0; j<len; j++)
    {
        c = mas[j];
        result = result^c;
        for (i=0; i!=8; i++)
        {
            c = result & 1;
            result >>= 1;
            if (c == 1)
            {
                result ^= 0xa001;
            }
        }
    }
    // контрольная сумма выдается младшим байтом вперед, поэтому меняем байты местами
    c = ((result & 0xff)<<8) | ((result & 0xff00)>>8);
    return (c);
}
```