

Немного об анализе логов, снятых при общении БК Multitronics'a с Allion' ом. Этот же принцип я реализовал в своем адаптере. Протокол очень напоминает KWP2000, но, видимо, с японским акцентом. По временам и наполнению. Скорость обмена данными в К-линии при установившейся сессии диагностики - 9600 бод. 12В соответствует единице, 0В – нулю. Стартовый бит – нулевой уровень, стоповый – 12В. Байт передается младшим разрядом вперед. Межбайтный интервал внутри кадра 3ms, время между ответом ECU и новым запросом не менее 12ms.

Инициализация линии, так же как и в протоколе KWP2000 начинается с пробуждения ECU с помощью WakeUP сигнала. В протоколе тойоты, он представляет собой hex байт C0 на скорости примерно 200 бод. Или, если описывать во времени, то: после включения зажигания и установки К-линии в 1 (12В) выжидается пауза не менее 2 сек, затем на 35мс БК роняет линию в 0, потом на 15мс возвращается к 12В до начала стартового бита запроса на установку связи.

Дальше, уже на скорости 9600 бод БК передает на линию последовательность запроса на установку связи: 81-13-F0-81-05. В этой посылке:

первое значение 81 - форматный байт, содержащий количество байт данных в посылке (в данном случае 1);

второй байт - физический адрес приемника посылки (ECU), он в тойоте =13h

третий байт - адрес источника запроса (БК), у меня он F0h

Эти первые три байта являются заголовком в данном запросе

четвертый байт - идентификатор сервиса -SID (в данном случае - запрос на коннект), он равен 81h.

пятый байт - байт контрольной суммы по модулю FF всех байтов посылки, исключая последний байт контрольной суммы (81h+13h+F0h+81h=205h, отбрасываем 2, получаем 05)

Дальше, БК освобождает линию и ждет ответа из ECU.

Через некоторое время (примерно 30-35 мс) ECU отвечает такой последовательностью:

83-F0-13-C1-E9-8F-BF. В этом ответе:

первое значение 83 - форматный байт, содержащий количество байт данных в посылке (в данном случае 3);

второй байт - физический адрес приемника посылки (сейчас это БК), =F0h

третий байт - адрес источника посылки (ECU), =13h

Здесь тоже три байта – заголовочная последовательность. Дальше собственно следуют те три байта, о которых информировал первый (форматный) байт:

Четвертый байт последовательности C1 – код ответа ECU о положительной процедуре приема данного запроса

Пятый и шестой байты – битовая маска режима, в данном случае E9-8F. Здесь я особенно распространяться не буду, ибо много писать не хочется, если интересно, можно посмотреть в описании протокола KWP2000.

Седьмой байт контрольная сумма ответа. Вычисляется аналогично, как в запросе.

Через время около 200мс БК посылает новый запрос в ECU на возможность диагностического режима:

82-13-F0-10-00-95.

Здесь первые три байта так же заголовок (82-13-F0), дальше следуют 2 байта запроса диагностики (10-00), ну и контрольная сумма (95)

Если ECU не прочь ответить диагносту, он выдает подтверждение:

81-F0-13-50-D4. Здесь код подтверждения =50.

Дальше, на линии снова пауза 200мс, а после этого начинается циклический обмен диагностическими данными между БК и ECU.

Форма запроса выглядит примерно так:

82-13-F0-xx-yy-cs. Здесь: первые 3 байта – заголовок, xx – SID (Service ID, или MODE), yy – PID, cs – контрольная сумма.

Ответ ECU, в зависимости от запроса, может выглядеть по-разному.

Например, на запрос 82-13-F0-01 E4-6A (запрос времени открытия форсунки), ECU ответит следующее: 83-F0-13-41-E4-xx-cs. Здесь 41- код подтверждения Service ID (SID+30), E4 – PID запроса, xx – время открытой форсунки, cs – контрольная сумма ответа.

При наличии ошибок, еще БК формирует трехбайтный запрос кодов ошибок: 83-13-F0-13-FF-00-98, ответ ECU может выглядеть следующим: 87-F0-13-53-01-00-01-10-16-56-5B.

Расшифровывается ответ так: 53 – ответ о положительном приеме запроса, и три обнаруженные ошибки: P0100, P0110, P1656. (это я отключал ДМРВ и датчик давления масла).