МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ»

Кафедра ИиСП

Отчет
по лабораторной работе № 1

по дисциплине «Машинно-зависимые языки программирования»
Вариант 20

Выполнил: ст. гр. ПС-11
Ложкин С.А.
Проверил: доцент, доцент кафедры ИиСП Баев А.А.

г. Йошкар-Ола
2023

Цель работы: понять работу дизассемблера и самому провести дизассемблирование одного из примеров

Задания на лабораторную работу:

1. Изучить документацию
2. Перевести данные из hex файла в двоичный код, а затем в команды ассемблера по инструкции
3. Записать полученный результат всей программы

1. Теоретические сведения

Есть ассемблерный код, наша задача перевести каждую команду в код на ассемблере.

Возьмём строку и уберём ненужные данные из неё (слева 8 символа и справа 2):

было 100000000C9434000C943E000C943E000C943E0082

стало 0C9434000C943E000C943E000C943E00

Затем отделяем каждые 4 бита, это будет одна команда

0C94 3400 0C94 3E00 0C94 3E00 0C94 3E00

Меняем в паре местами биты

940C 0034 940C 003E 940C 003E 940C 003E

Если байт 94, то это команды либо jmp, либо call. Они четырёхбитные, поэтому рассматриваем их в паре

Переводим в двоичное представление, смотрим по маске аргументы (если есть), пишем команду в виде строки asm.

940C 0034

bin 1001 0100 0000 1100 0000 0000 0011 0100

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 0100

со сдвигом = 00000000000001101000 = 0x68

jmp 0x68

Для jmp, call, breq, brne, rjmp и других команд с адресами в аргументах надо смещать адрес влево на 1. Команды на примере ldi помещают значения в регистры, начиная с 16, поэтому для них надо будет прибавлять 16 к номеру регистра из аргумента команды.

2. Практическая часть

Начальные данные в hex файле

```
:100000000C9434000C943E000C943E000C943E0082
:100010000C943E000C943E000C943E000C943E0068
:100020000C943E000C943E000C943E000C943E0058
:100030000C943E000C943E000C943E000C943E0048
:100040000C943E000C943E000C943E000C943E0038
:100050000C943E000C943E000C943E000C943E0028
:100060000C943E000C943E0011241FBECFEFD8E04C
:10007000DEBFCDBF0E9440000C9451000C940000E4
:100080003D9A81E091E0892711F0459A01C0459899
:1000900020E83AE64DE1215030404040E1F70000D1
:0600A000F2CFF894FFCF3F
:00000001FF
```

Дизассемблирование

:10 0000 00 0C94 3400 0C94 3E00 0C94 3E00 0C94 3E00 82

940C 0034

bin 1001 0100 0000 1100 0000 0000 0011 0100

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 0100

со сдвигом = 00000000000001101000 = 0x68

jmp 0x68

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000001111100 = 0x7C

jmp 0x7C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000001111100 = 0x7C

jmp 0x7C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000001111100 = 0x7C

jmp 0x7C

:10 0010 00 0C94 3E00 0C94 3E00 0C94 3E00 0C94 3E00 68

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000001111100 = 0x7C

jmp 0x7C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000001111100 = 0x7C

jmp 0x7C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000001111100 = 0x7C

jmp 0x7C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000001111100 = 0x7C

jmp 0x7C

:10 0020 00 0C94 3E00 0C94 3E00 0C94 3E00 0C94 3E00 58

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000001111100 = 0x7C

jmp 0x7C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000000111100 = 0x7C

jmp 0x7C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000000111100 = 0x7C

jmp 0x7C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000000111100 = 0x7C

jmp 0x7C

:10 0030 00 0C94 3E00 0C94 3E00 0C94 3E00 0C94 3E00 48

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000000111100 = 0x7C

jmp 0x7C

940C 003E
bin   1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 0000000000000001111100 = 0x7C
jmp 0x7C

940C 003E
bin   1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 0000000000000001111100 = 0x7C
jmp 0x7C

940C 003E
bin   1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 0000000000000001111100 = 0x7C
jmp 0x7C

:10 0040 00 0C94 3E00 0C94 3E00 0C94 3E00 0C94 3E00 38

940C 003E
bin   1001 0100 0000 1100 0000 0000 0011 1110

маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 000000000000001111100 = 0x7C
jmp 0x7C

940C 003E
bin 1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 000000000000001111100 = 0x7C
jmp 0x7C

940C 003E
bin 1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 000000000000001111100 = 0x7C
jmp 0x7C

940C 003E
bin 1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 000000000000001111100 = 0x7C
jmp 0x7C

:10 0050 00 0C94 3E00 0C94 3E00 0C94 3E00 0C94 3E00 28

940C 003E
bin   1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 000000000000001111100 = 0x7C
jmp 0x7C

940C 003E
bin   1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 000000000000001111100 = 0x7C
jmp 0x7C

940C 003E
bin   1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 000000000000001111100 = 0x7C
jmp 0x7C

940C 003E
bin   1001 0100 0000 1100 0000 0000 0011 1110
маска1001 010k kkkk 110k kkkk kkkk kkkk kkkk
k = 0000 0 0000 0000 0011 1110
со сдвигом = 000000000000001111100 = 0x7C
jmp 0x7C

:10 0060 00 0C94 3E00 0C94 3E00 1124 1FBE CFEF D8E0 4C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000000111100 = 0x7C

jmp 0x7C

940C 003E

bin 1001 0100 0000 1100 0000 0000 0011 1110

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0000 0 0000 0000 0011 1110

со сдвигом = 00000000000000111100 = 0x7C

jmp 0x7C

2411

bin 0010 0100 0001 0001

маска 0010 01rd dddd rrrr

d = 00001 r = 00001

eor r1,r1

BE1F

bin 1011 1110 0001 1111

маска 1011 1PPr rrrr PPPP

P = 111111 = 0x3F r = 0001

out 0x3F,r1

EFCF

bin 1110 1111 1100 1111

маска 1110 KKKK dddd KKKK

K = 11111111 = 0xFF d = 1100 = 0x0C = 12

прибавляем 16 => d = 28

ldi r28,0xFF

E0D8

bin 1110 0000 1101 1000

маска 1110 KKKK dddd KKKK

K = 00001000 = 0x08 d = 1101 = 13

прибавляем 16 => d = 29

ldi r29,0x08

:10 0070 00 DEBF CDBF 0E94 4000 0C94 5100 0C94 0000 E4

BFDE

bin 1011 1111 1101 1110

маска 1011 1PPr rrrr PPPP

P = 111110 = 0x3E

r = 11101 = 29

out 0x3E,r29

BFCD

bin 1011 1111 1100 1101

маска 1011 1PPr rrrr PPPP

P = 111101 = 0x3D

r = 11100 = 28

out 0x3D,r28

940E 0040

bin 1001 0100 0000 1110 0000 0000 0100 0000

маска 1001 010k kkkk 111k kkkk kkkk kkkk kkkk

k = 0100 0000

со сдвигом = 1000 0000 = 0x80

call 0x80

940C 0051

bin 1001 0100 0000 1100 0000 0000 0101 0001

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0 0000 0 0000 0000 0101 0001

со свдигом = 00000000000000010100010 = 0xA2

jmp 0xA2

940C 0000

bin 1001 0100 0000 1100 0000 0000 0000 0000

маска 1001 010k kkkk 110k kkkk kkkk kkkk kkkk

k = 0

jmp 0

:10 0080 00 3D9A 81E0 91E0 8927 11F0 459A 01C0 4598 99

9A3D

bin 1001 1010 0011 1101

маска 1001 1010 PPPP Pbbb

P = 00111 = 0x07 b = 101 = 5

sbi 0x07,5

E081

bin 1110 0000 1000 0001

маска 1110 KKKK dddd KKKK

K = 1 = 0x1 d = 0000 1000 = 8

прибавляем 16 => d = 24

ldi r24, 0x01

E091

bin 1110 0000 1001 0001

маска 1110 KKKK dddd KKKK

K = 1 = 0x1 d = 1001 = 9

прибавляем 16 => d = 25

ldi r25, 0x01

2789

bin 0010 0111 1000 1001

маска 0010 01rd dddd rrrr

r = 11001 = 25 d = 11000 = 24

eor r24,r25

F011

bin 1111 0000 0001 0001

маска 1111 00kk kkkk k001

k = 0000010

со сдвигом = 0000100 = 4

breq .+4

9A45

bin 1001 1010 0100 0101

маска 1001 1010 PPPP Pbbb

P = 01000 = 0x08 b = 101 = 5

sbi 0x08,5

C001

bin 1100 0000 0000 0001

маска 1100 kkkk kkkk kkkk

k = 0000 0000 0001

со сдвигом = 000000000010 = 2

rjmp .+2

9845

bin 1001 1000 0100 0101

маска 1001 1000 PPPP Pbbb

P = 01000 = 0x08 b = 101 = 5

cbi 0x08,5

:10 0090 00 20E8 3AE6 4DE1 2150 3040 4040 E1F7 0000 D1

E820

bin 1110 1000 0010 0000

маска 1110 KKKK dddd KKKK

K = 10000000 = 0x80 d = 0010 = 2

прибавляем 16 => d = 18

ldi r18,0x80

E63A

bin 1110 0110 0011 1010

маска 1110 KKKK dddd KKKK

K = 01101010 = 0x6A d = 0011 = 3

прибавляем 16 => d = 19

ldi r19,0x6A

E14D

bin 1110 0001 0100 1101

маска 1110 KKKK dddd KKKK

K = 00011101 = 0x1D d = 0100 = 4

прибавляем 16 => d = 20

ldi r20,0x1D

5021

bin 101 0000 0010 0001

маска 1010 KKKK dddd KKKK

K = 1 = 0x01 d = 0010 = 2

прибавляем 16 => d = 18

subi r18,0x01

4030

bin 0100 0000 0011 0000

маска0100 KKKK dddd KKKK

K = 0 = 0x00 d = 0011 = 3

прибавляем 16 => d = 19

sbci r19,0x00

4040

bin 0100 0000 0100 0000

маска0100 KKKK dddd KKKK

K = 0 = 0x00

d = 0100 = 4

прибавляем 16 => d = 20

sbci r20,0x00

F7E1

bin 1111 0111 1110 0001

маска1111 01kk kkkk k001

k = 1111 1100

со сдвигом = 11111000 = -8

brne .-8

0000

bin 0000 0000 0000 0000

nop

:06 00A0 00 F2CF F894 FFCF 3F

CFF2

bin 1100 1111 1111 0010

маска 1100 kkkk kkkk kkkk

k = 1111 1111 0010

со сдвигом = 111111100100 = -28

rjmp .-28

94F8

1001 0100 1111 1000

cli

CFFF

bin 1100 1111 1111 1111

маска 1100 kkkk kkkk kkkk

k = 111111111111

со сдвигом = 111111111110 = -2

rjmp .-2

:00 0000 01 FF

Конечный вариант

```
00: 0c 94 34 00         jmp 0x68        ; 0x68
04: 0c 94 3e 00         jmp 0x7c        ; 0x7c
08: 0c 94 3e 00         jmp 0x7c        ; 0x7c
0c: 0c 94 3e 00         jmp 0x7c        ; 0x7c
10: 0c 94 3e 00         jmp 0x7c        ; 0x7c
14: 0c 94 3e 00         jmp 0x7c        ; 0x7c
18: 0c 94 3e 00         jmp 0x7c        ; 0x7c
```

```
1c: 0c 94 3e 00      jmp 0x7c        ; 0x7c
20: 0c 94 3e 00      jmp 0x7c        ; 0x7c
24: 0c 94 3e 00      jmp 0x7c        ; 0x7c
28: 0c 94 3e 00      jmp 0x7c        ; 0x7c
2c: 0c 94 3e 00      jmp 0x7c        ; 0x7c
30: 0c 94 3e 00      jmp 0x7c        ; 0x7c
34: 0c 94 3e 00      jmp 0x7c        ; 0x7c
38: 0c 94 3e 00      jmp 0x7c        ; 0x7c
3c: 0c 94 3e 00      jmp 0x7c        ; 0x7c
40: 0c 94 3e 00      jmp 0x7c        ; 0x7c
44: 0c 94 3e 00      jmp 0x7c        ; 0x7c
48: 0c 94 3e 00      jmp 0x7c        ; 0x7c
4c: 0c 94 3e 00      jmp 0x7c        ; 0x7c
50: 0c 94 3e 00      jmp 0x7c        ; 0x7c
54: 0c 94 3e 00      jmp 0x7c        ; 0x7c
58: 0c 94 3e 00      jmp 0x7c        ; 0x7c
5c: 0c 94 3e 00      jmp 0x7c        ; 0x7c
60: 0c 94 3e 00      jmp 0x7c        ; 0x7c
64: 0c 94 3e 00      jmp 0x7c        ; 0x7c
68: 11 24            eor r1,r1
6a: 1F BE            out 0x3F,r1     ; 63
6c: CF EF            ldi r28,0xFF    ; 255
6e: D8 E0            ldi r29,0x08    ; 8
70: DE BF            out 0x3E,r29    ; 62
72: CD BF            out 0x3D,r28    ; 61
74: 0e 94 40 00      call 0x80       ; 0x80
78: 0C 94 51 00      jmp 0xA2        ; 0xA2
7c: 0C 94 00 00      jmp 0           ; 0x0
```

```
80: 3D 9A       sbi 0x07,5          ; 7
82: 81 E0       ldi r24,0x01        ; 1
84: 91 E0       ldi r25,0x01        ; 1
86: 89 27       eor r24,r25
88: 11 F0       breq .+4            ; 0x8e
8a: 45 9A       sbi 0x08,5          ; 8
8c: 01 C0       rjmp .+2            ; 0x90
8e: 45 98       cbi 0x08,5          ; 8
90: 20 E8       ldi r18,0x80 ; 128
92: 3A E6       ldi r19,0x6A        ; 106
94: 4D E1       ldi r20,0x1D        ; 29
96: 21 50       subi r18, 0x01      ; 1
98: 30 40       sbci r19, 0x00      ; 0
9a: 40 40       sbci r20, 0x00      ; 0
9c: E1 F7       brne .-8            ; 0x96
9e: 00 00       nop
a0: F2 CF       rjmp .-28           ; 0x86
a2: F8 94       cli
a4: FF CF       rjmp .-2            ; 0xA4
```

Выводы

В ходе выполнения данной лабораторной работы я на конкретном примере отлично понял работу ассемблера и дизассемблера, структуру hex файлов, работу с масками и теперь могу применять эти знания на практике.