

# **Отчёт по лабораторной работе № 10**

**Архитектура компьютера**

**РЫЖОВ Егор**

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
3.1	Реализация подпрограмм в NASM . . . . .	7
3.2	Отладка программ с помощью GDB . . . . .	9
3.3	Добавление точек останова . . . . .	13
3.4	Работа с данными программы в GDB . . . . .	14
3.5	Обработка аргументов командной строки в GDB . . . . .	17
3.6	Задание для самостоятельной работы . . . . .	19
<b>4</b>	<b>Выводы</b>	<b>27</b>

# Список иллюстраций

3.1	7
3.2	8
3.3	8
3.4	9
3.5	9
3.6	9
3.7	10
3.8	10
3.9	10
3.10	11
3.11	11
3.12	12
3.13	12
3.14	13
3.15	13
3.16	13
3.17	14
3.18	14
3.19	15
3.20	15
3.21	15
3.22	15
3.23	16
3.24	16
3.25	16
3.26	17
3.27	17
3.28	17
3.29	17
3.30	17
3.31	18
3.32	18
3.33	18
3.34	19
3.35	19
3.36	19
3.37	20

3.38 . . . . .	20
3.39 . . . . .	20
3.40 . . . . .	20
3.41 . . . . .	21
3.42 . . . . .	21
3.43 . . . . .	21
3.44 . . . . .	21
3.45 . . . . .	22
3.46 . . . . .	22
3.47 . . . . .	23
3.48 . . . . .	23
3.49 . . . . .	24
3.50 . . . . .	24
3.51 . . . . .	25
3.52 . . . . .	25
3.53 . . . . .	26
3.54 . . . . .	26

# 1 Цель работы

Приобретение навыков написания программ с использованием подпрограмм. Знакомство с методами отладки при помощи GDB и его основными возможностями.

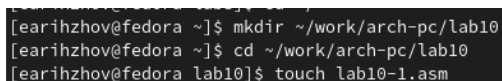
## 2 Задание

1. Реализовать подпрограммы в NASM.
2. Выполнить отладку программ с помощью GDB.
3. Отработать добавление точек останова.
4. Поработа с данными программы в GDB.
5. Отработать обработку аргументов командной строки в GDB.
6. Выполнить задание для самостоятельной работы.

## 3 Выполнение лабораторной работы

### 3.1 Реализация подпрограмм в NASM

1. Создали каталог для выполнения лабораторной работы № 10, перешли в него и создали файл lab10-1.asm: (рис. 3.1)

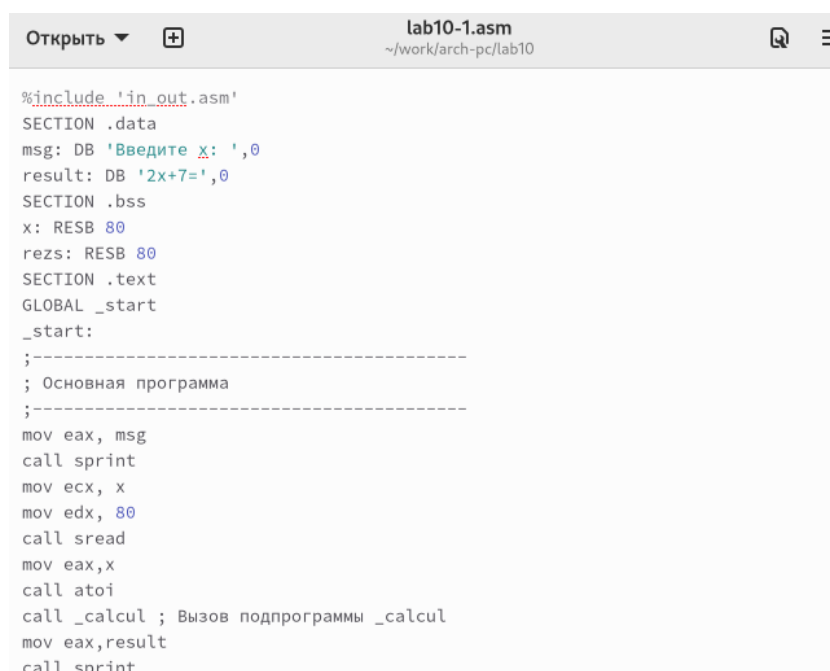


```
[earihzhov@fedora ~]$ mkdir ~/work/arch-pc/lab10  
[earihzhov@fedora ~]$ cd ~/work/arch-pc/lab10  
[earihzhov@fedora lab10]$ touch lab10-1.asm
```

Рис. 3.1: .

2. В качестве примера рассмотрели программу вычисления арифметического выражения  $f(x) = 2x + 7$  с помощью подпрограммы `_calcul`. В данном примере `x` вводится с клавиатуры, а само выражение вычисляется в подпрограмме. Внимательно изучили текст программы (Листинг 10.1).

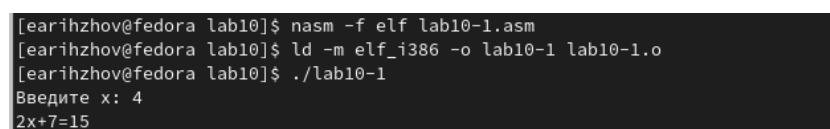
Введите в файл lab10-1.asm текст программы из листинга 10.1. (рис. 3.2) Создайте исполняемый файл и проверьте его работу.(рис. 3.3)



```
Открыть + lab10-1.asm ~/work/arch-pc/lab10

%include 'in_out.asm'
SECTION .data
msg: DB 'Введите x: ',0
result: DB '2x+7=',0
SECTION .bss
x: RESB 80
rezs: RESB 80
SECTION .text
GLOBAL _start
_start:
;-----
; Основная программа
;-----
mov eax, msg
call sprint
mov ecx, x
mov edx, 80
call sread
mov eax, x
call atoi
call _calcul ; Вызов подпрограммы _calcul
mov eax, result
call sprint
```

Рис. 3.2: .

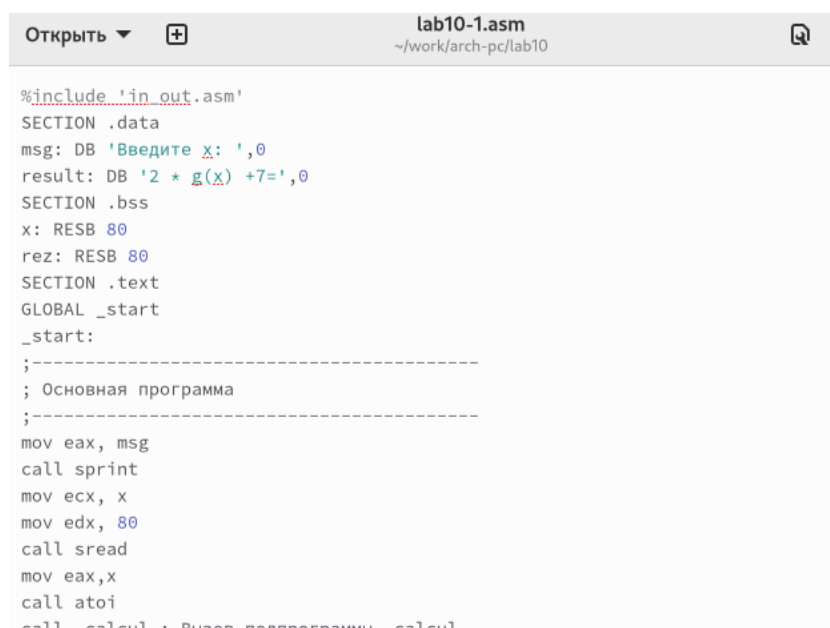


```
[earihzhov@fedora lab10]$ nasm -f elf lab10-1.asm
[earihzhov@fedora lab10]$ ld -m elf_i386 -o lab10-1 lab10-1.o
[earihzhov@fedora lab10]$ ./lab10-1
Введите x: 4
2x+7=15
```

Рис. 3.3: .

Изменили текст программы, добавив подпрограмму `_subcalcul` в подпрограмму `_calcul`, для вычисления выражения  $f(g(x))$ , где  $x$  вводится с клавиатуры,  $f(x) = 2x + 7$ ,  $g(x) = 3x - 1$ . Т.е.  $x$  передается в подпрограмму `_calcul` из нее в подпрограмму `_subcalcul`, где вычисляется выражение  $g(x)$ , результат возвращается в `_calcul` и вычисляется выражение  $f(g(x))$ . Результат возвращается в основную программу для вывода результата на экран. (рис. 3.4), (рис. 3.5)

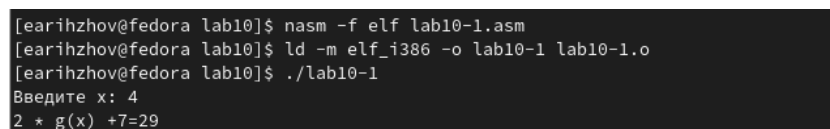




```
Открыть + lab10-1.asm ~/work/arch-pc/lab10

%include 'in_out.asm'
SECTION .data
msg: DB 'Введите x: ',0
result: DB '2 * g(x) +7=',0
SECTION .bss
x: RESB 80
rez: RESB 80
SECTION .text
GLOBAL _start
_start:
;-----
; Основная программа
;-----
mov eax, msg
call sprint
mov ecx, x
mov edx, 80
call sread
mov eax,x
call atoi
call calcul : Вызов подпрограммы calcul
```

Рис. 3.4: .

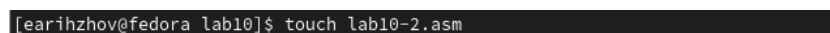


```
[earihzhov@fedora lab10]$ nasm -f elf lab10-1.asm
[earihzhov@fedora lab10]$ ld -m elf_i386 -o lab10-1 lab10-1.o
[earihzhov@fedora lab10]$ ./lab10-1
Введите x: 4
2 * g(x) +7=29
```

Рис. 3.5: .

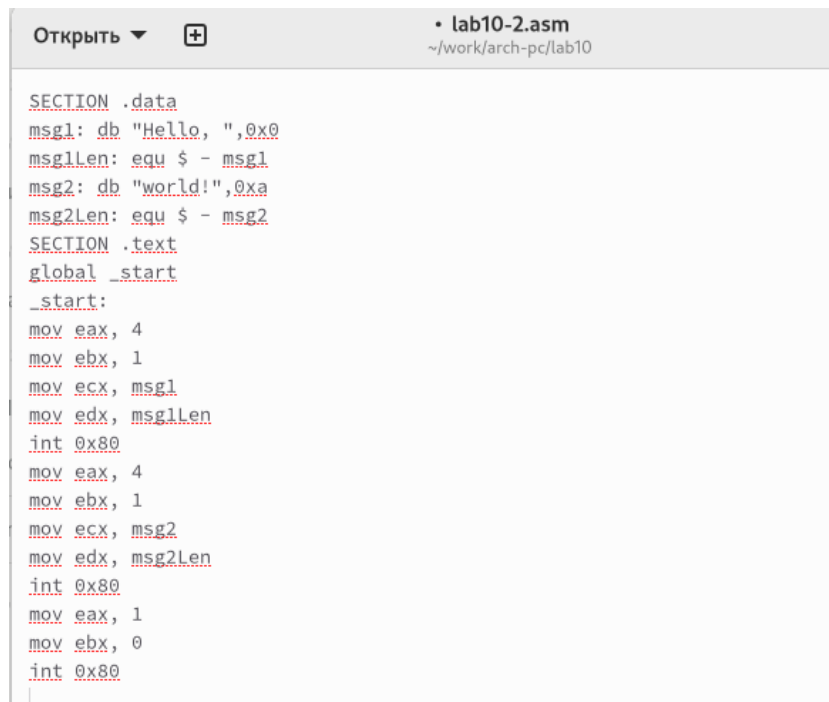
## 3.2 Отладка программ с помощью GDB

Создали файл lab10-2.asm с текстом программы из Листинга 10.2. (Программа печати сообщения Hello world!): (рис. 3.6), (рис. 3.7)



```
[earihzhov@fedora lab10]$ touch lab10-2.asm
```

Рис. 3.6: .

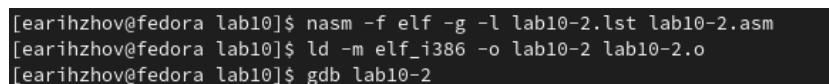


```
Открыть ▾ + lab10-2.asm
~/work/arch-pc/lab10

SECTION .data
msg1: db "Hello, ",0x0
msg1len: equ $ - msg1
msg2: db "world!",0xa
msg2len: equ $ - msg2
SECTION .text
global _start
_start:
mov eax, 4
mov ebx, 1
mov ecx, msg1
mov edx, msg1len
int 0x80
mov eax, 4
mov ebx, 1
mov ecx, msg2
mov edx, msg2len
int 0x80
mov eax, 1
mov ebx, 0
int 0x80
```

Рис. 3.7: .

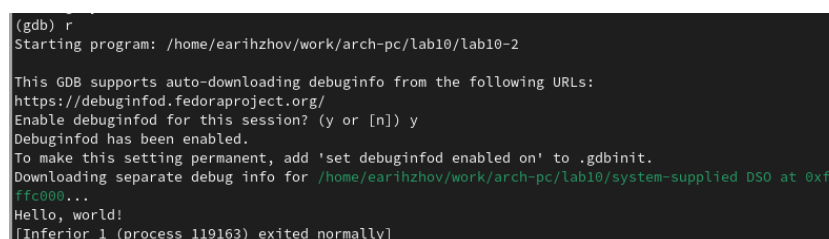
Получили исполняемый файл. Для работы с GDB в исполняемый файл добавили отладочную информацию, для этого трансляцию программ провели с ключом '-g'. Загрузили исполняемый файл в отладчик gdb. (рис. 3.8)



```
[earihzhov@fedora lab10]$ nasm -f elf -g -l lab10-2.lst lab10-2.asm
[earihzhov@fedora lab10]$ ld -m elf_i386 -o lab10-2 lab10-2.o
[earihzhov@fedora lab10]$ gdb lab10-2
```

Рис. 3.8: .

Загрузили исполняемый файл в отладчик gdb. Проверили работу программы, запустив ее в оболочке GDB с помощью команды run (сокращённо r): (рис. 3.9)



```
(gdb) r
Starting program: /home/earihzhov/work/arch-pc/lab10/lab10-2

This GDB supports auto-downloading debuginfo from the following URLs:
https://debuginfod.fedoraproject.org/
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gdbinit.
Downloading separate debug info for /home/earihzhov/work/arch-pc/lab10/system-supplied DSO at 0xf7ffc000...
Hello, world!
[Inferior 1 (process 119163) exited normally]
```

Рис. 3.9: .

Для более подробного анализа программы установили брейкпоинт на метку `_start`, с которой начинается выполнение любой ассемблерной программы, и запустили её. (рис. 3.10)

```
(gdb) break _start
Breakpoint 1 at 0x8049000: file lab10-2.asm, line 9.
(gdb) run
Starting program: /home/earihzhov/work/arch-pc/lab10/lab10-2

Breakpoint 1, _start () at lab10-2.asm:9
9      mov eax, 4
```

Рис. 3.10: .

Посмотрели дисассимилированный код программы с помощью команды `disassemble` начиная с метки `_start`. (рис. 3.11)

```
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08049000 <+0>:      mov     $0x4,%eax
      0x08049005 <+5>:      mov     $0x1,%ebx
      0x0804900a <+10>:     mov     $0x804a000,%ecx
      0x0804900f <+15>:     mov     $0x8,%edx
      0x08049014 <+20>:     int     $0x80
      0x08049016 <+22>:     mov     $0x4,%eax
      0x0804901b <+27>:     mov     $0x1,%ebx
      0x08049020 <+32>:     mov     $0x804a008,%ecx
      0x08049025 <+37>:     mov     $0x7,%edx
      0x0804902a <+42>:     int     $0x80
      0x0804902c <+44>:     mov     $0x1,%eax
      0x08049031 <+49>:     mov     $0x0,%ebx
      0x08049036 <+54>:     int     $0x80
End of assembler dump.
```

Рис. 3.11: .

Переключились на отображение команд с Intel'овским синтаксисом, введя команду `set disassembly-flavor intel`. (рис. 3.12)

```

(gdb) set disassembly-flavor intel
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08049000 <+0>:      mov     eax,0x4
    0x08049005 <+5>:      mov     ebx,0x1
    0x0804900a <+10>:     mov     ecx,0x804a000
    0x0804900f <+15>:     mov     edx,0x8
    0x08049014 <+20>:     int     0x80
    0x08049016 <+22>:     mov     eax,0x4
    0x0804901b <+27>:     mov     ebx,0x1
    0x08049020 <+32>:     mov     ecx,0x804a008
    0x08049025 <+37>:     mov     edx,0x7
    0x0804902a <+42>:     int     0x80
    0x0804902c <+44>:     mov     eax,0x1
    0x08049031 <+49>:     mov     ebx,0x0
    0x08049036 <+54>:     int     0x80
End of assembler dump.

```

Рис. 3.12: .

Различия отображения синтаксиса машинных команд в режимах АТТ и Intel: в АТТ перед адресом регистра ставится \$, а перед названием регистра %, сначала записывается адрес, а потом - регистр. В Intel сначала регистр, а потом адрес, и перед ними ничего не ставится.

Включили режим псевдографики для более удобного анализа программы.(рис. 3.13)

```

[ Register Values Unavailable ]

B+> 0x8049000 <_start>  mov     eax,0x4
    0x8049005 <_start+5>  mov     ebx,0x1
    0x804900a <_start+10> mov     ecx,0x804a000
    0x804900f <_start+15> mov     edx,0x8
    0x8049014 <_start+20> int     0x80
    0x8049016 <_start+22> mov     eax,0x4
    0x804901b <_start+27> mov     ebx,0x1
    0x8049020 <_start+32> mov     ecx,0x804a008
native process 45229 In: _start L?? PC: 0x8049000
(gdb) layout regs
(gdb)

```

Рис. 3.13: .

### 3.3 Добавление точек останова

Установить точку останова можно командой `break` (кратко `b`). Типичный аргумент этой команды — место установки. Его можно задать или как номер строки программы (имеет смысл, если есть исходный файл, а программа компилировалась с информацией об отладке), или как имя метки, или как адрес. Чтобы не было путаницы с номерами, перед адресом ставится «звёздочка»: На предыдущих шагах была установлена точка останова по имени метки (`_start`). Проверили это с помощью команды `info breakpoints` (кратко `i b`). (рис. 3.14)

```
(gdb) info breakpoints
Num   Type             Disp Enb Address      What
1     breakpoint       keep y   0x08049000  <_start>
      breakpoint already hit 1 time
```

Рис. 3.14: .

Установили еще одну точку останова по адресу инструкции. Адрес инструкции увидели в средней части экрана в левом столбце соответствующей инструкции. Определили адрес предпоследней инструкции (`mov ebx,0x0`) и установили точку останова. (рис. 3.15)

```
b+ 0x8049031 <_start+49>  mov    ebx,0x0
0x8049036 <_start+54>  int     0x80
0x8049038                add     BYTE PTR [eax],al

native process 45229 In: _start L?? PC: 0x80490
(gdb) break *0x8049031
Breakpoint 2 at 0x8049031
```

Рис. 3.15: .

Посмотрели информацию о всех установленных точках останова: (рис. 3.16)

```
(gdb) i b
Num   Type             Disp Enb Address      What
1     breakpoint       keep y   0x08049000  <_start>
      breakpoint already hit 1 time
2     breakpoint       keep y   0x08049031  <_start+49>
(gdb)
```

Рис. 3.16: .

### 3.4 Работа с данными программы в GDB

Отладчик может показывать содержимое ячеек памяти и регистров, а при необходимости позволяет вручную изменять значения регистров и переменных. Выполнили 5 инструкций с помощью команды `stepi` (или `si`) и проследили за изменением значений регистров. (рис. 3.17), (рис. 3.18)

```
eax      0x0      0
ecx      0x0      0
edx      0x0      0
ebx      0x0      0
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049000 0x8049000 <_start>
eflags   0x202    [ IF ]
cs       0x23     35
ss       0x2b     43
ds       0x2b     43
es       0x2b     43
Type: PPT, 64-bit, 32-bit, 16-bit, 8-bit, 4-bit, 2-bit, 1-bit, 0-bit, 0.5-bit, 0.25-bit, 0.125-bit, 0.0625-bit, 0.03125-bit, 0.015625-bit, 0.0078125-bit, 0.00390625-bit, 0.001953125-bit, 0.0009765625-bit, 0.00048828125-bit, 0.000244140625-bit, 0.0001220703125-bit, 0.00006103515625-bit, 0.000030517578125-bit, 0.0000152587890625-bit, 0.00000762939453125-bit, 0.000003814697265625-bit, 0.0000019073486328125-bit, 0.00000095367431640625-bit, 0.000000476837158203125-bit, 0.0000002384185791015625-bit, 0.00000011920928955078125-bit, 0.000000059604644775390625-bit, 0.0000000298023223876953125-bit, 0.00000001490116119384765625-bit, 0.000000007450580596923828125-bit, 0.0000000037252902984619140625-bit, 0.00000000186264514923095703125-bit, 0.000000000931322574615478515625-bit, 0.0000000004656612873077392578125-bit, 0.00000000023283064365386962890625-bit, 0.000000000116415321826934814453125-bit, 0.0000000000582076609134674072265625-bit, 0.00000000002910383045673370361328125-bit, 0.000000000014551915228366851806640625-bit, 0.0000000000072759576141834259033203125-bit, 0.00000000000363797880709171295166015625-bit, 0.000000000001818989403545856475830078125-bit, 0.0000000000009094947017729282379150390625-bit, 0.00000000000045474735088646411895751953125-bit, 0.000000000000227373675443232059478759765625-bit, 0.0000000000001136868377216160297393798828125-bit, 0.00000000000005684341886080801486968994140625-bit, 0.000000000000028421709430404007434844970703125-bit, 0.0000000000000142108547152020037174224853515625-bit, 0.00000000000000710542735760100185871124267578125-bit, 0.000000000000003552713678800500929355621337890625-bit, 0.0000000000000017763568394002504646778106689453125-bit, 0.00000000000000088817841970012523233890533447265625-bit, 0.000000000000000444089209850062616169452667236328125-bit, 0.0000000000000002220446049250313080847263336181640625-bit, 0.00000000000000011102230246251565404236316680908203125-bit, 0.000000000000000055511151231257827021181583404541015625-bit, 0.0000000000000000277555756156289135105907917022705078125-bit, 0.00000000000000001387778780781445675529539585113525390625-bit, 0.000000000000000006938893903907228377647697925567626953125-bit, 0.0000000000000000034694469519536141888238489627838134765625-bit, 0.00000000000000000173472347597680709441192448139190673828125-bit, 0.000000000000000000867361737988403547205962240695953369140625-bit, 0.0000000000000000004336808689942017736029811203479766846875-bit, 0.00000000000000000021684043449710088680149056017398834234375-bit, 0.000000000000000000108420217248550443400745280086994171171875-bit, 0.0000000000000000000542101086242752217003726400434970855859375-bit, 0.00000000000000000002710505431213761085018632002174854279296875-bit, 0.000000000000000000013552527156068805425093160010874271396484375-bit, 0.0000000000000000000067762635780344027125465800054371359822421875-bit, 0.00000000000000000000338813178901720135627329000271856799112109375-bit, 0.000000000000000000001694065894508600678136645001359283995560546875-bit, 0.0000000000000000000008470329472543003390683225006796419977802734375-bit, 0.00000000000000000000042351647362715016953416125033982099889013671875-bit, 0.000000000000000000000211758236813575084767080625169910499445068359375-bit, 0.0000000000000000000001058791184067875423835403125849552497225341796875-bit, 0.00000000000000000000005293955920339377119177015629247762486126708984375-bit, 0.000000000000000000000026469779601696885595885078146238812430633544921875-bit, 0.0000000000000000000000132348898008484427979425390731169062153167724609375-bit, 0.00000000000000000000000661744490042422139897126953655845310765838623046875-bit, 0.000000000000000000000003308722450212110699485634768279226538294193115234375-bit, 0.0000000000000000000000016543612251060553497428173841396132691470965576171875-bit, 0.00000000000000000000000082718061255302767487140869206980663457354827880859375-bit, 0.000000000000000000000000413590306276513837435704346034903317286774139404296875-bit, 0.0000000000000000000000002067951531382569187178521730174516586433870697021484375-bit, 0.00000000000000000000000010339757656912845935892608650872582932169353485107421875-bit, 0.000000000000000000000000051698788284564229679463043254362914660846767425537109375-bit, 0.0000000000000000000000000258493941422821148397315216271814573304233837127685546875-bit, 0.00000000000000000000000001292469707114105741986576081359072866521169185638427734375-bit, 0.000000000000000000000000006462348535570528709932880406795364332605845928172138671875-bit, 0.000000000000000000000000003231174267785264354966440203397682166522922902892964359375-bit, 0.0000000000000000000000000016155871338926321774832201016988410832614614514464821796875-bit, 0.000000000000000000000000000807793566946316088741610050849420541630730725723241089375-bit, 0.0000000000000000000000000004038967834731580443708050254247102708153653628616205446875-bit, 0.00000000000000000000000000020194839173657902218540251271235513540768268143081027234375-bit, 0.000000000000000000000000000100974195868289511092701256356177567703841340715405136171875-bit, 0.00000000000000000000000000005048709793414475554635062817808878385192067035770258959375-bit, 0.000000000000000000000000000025243548967072377773175314089044391925960335178851294796875-bit, 0.0000000000000000000000000000126217744835361888865876570445221959629801675894256473984375-bit, 0.00000000000000000000000000000631088724176809444329378252226110979649008379471282369921875-bit, 0.000000000000000000000000000003155443620884047221646891261130549898245041897356411849609375-bit, 0.0000000000000000000000000000015777218104420236108234456305652749491225209486782059248046875-bit, 0.00000000000000000000000000000078886090522101180541172281528263747456126047433910296240234375-bit, 0.000000000000000000000000000000394430452610505902705861407641318737280630237169551481201171875-bit, 0.000000000000000000000000000000197215226305252951352930703820659368640315118584775740600589375-bit, 0.0000000000000000000000000000000986076131526264756764653519103296843201575592923878703002946875-bit, 0.00000000000000000000000000000004930380657631323783823267595516484216007877964619393515014734375-bit, 0.000000000000000000000000000000024651903288156618919116337977582421080039389823096967575073671875-bit, 0.0000000000000000000000000000000123259516440783094595581689887912105400196949115484837875368359375-bit, 0.00000000000000000000000000000000616297582203915472977908449439560527000984745577424189376841796875-bit, 0.0000000000000000000000000000000030814879110195773648895422471978026350049237278871209468842089375-bit, 0.00000000000000000000000000000000154074395550978868244477112359890131750246186394356047344210446875-bit, 0.000000000000000000000000000000000770371977754894341222385561799450658751230931971780236721052234375-bit, 0.0000000000000000000000000000000003851859888774471706111927808997253293756154659858901183605261171875-bit, 0.00000000000000000000000000000000019259299443872358530559639044986266468780773299294505918026305859375-bit, 0.00000000000000000000000000000000009629649721936179265279819522493133234390386649647252959013152921875-bit, 0.000000000000000000000000000000000048148248609680896326399097612465666171951933248236264795065764609375-bit, 0.0000000000000000000000000000000000240741243048404481631995488062328330859759666241181323975328823046875-bit, 0.00000000000000000000000000000000001203706215242022408159977440311641654298798331205906619876644115234375-bit, 0.000000000000000000000000000000000006018531076210112040799887201558208271493991656029533099383220576171875-bit, 0.0000000000000000000000000000000000030092655381050560203999436007791041357469958280147665496916102880859375-bit, 0.00000000000000000000000000000000000150463276905252801019997180038955206787349791400738327484580514404296875-bit, 0.000000000000000000000000000000000000752316384526264005099985900194776033936748957000366637422902572021484375-bit, 0.00000000000000000000000000000000000037615819226313200254999295009738801696837447850001831871145012860107421875-bit, 0.000000000000000000000000000000000000188079096131566001274996475048694008484187239250009159355725064300537109375-bit, 0.0000000000000000000000000000000000000940395480657830006374982375243470042420936196250004579677875032150175546875-bit, 0.00000000000000000000000000000000000004701977403289150031874911876217350212104680981250022898389375160750877734375-bit, 0.000000000000000000000000000000000000023509887016445750159374559381086751060523404906250011446946875753754388671875-bit, 0.0000000000000000000000000000000000000117549435082228750796872796905433755302617024531250005724734386768771943359375-bit, 0.00000000000000000000000000000000000000587747175411143753984363984527168776513085122656250002862367193393859716796875-bit, 0.000000000000000000000000000000000000002938735877055718769921819922635843882565425613281250001431183466969298583984375-bit, 0.0000000000000000000000000000000000000014693679385278593849609099613179219412827128066406250000715591734846492941921875-bit, 0.00000000000000000000000000000000000000073468396926392969248045498065896097064135640332031250000357795869732464709609375-bit, 0.000000000000000000000000000000000000000367341984631964846240227490329480485320678201666015625000017889793498673548046875-bit, 0.0000000000000000000000000000000000000001836709923159824231201137451647402426603391008330078125000008944896993367740234375-bit, 0.000000000000000000000000000000000000000091835496157991211560056872582370121330169550416503906250000044724484966838701171875-bit, 0.000000000000000000000000000000000000000045917748078995605780028436291185060665084775208251953125000002236224248343505859375-bit, 0.0000000000000000000000000000000000000000229588740394978028900142181455925303325423876041259765625000001118112124171752796875-bit, 0.00000000000000000000000000000000000000001147943701974890144500710907279626516627119380206298828125000000559056062085863984375-bit, 0.00000000000000000000000000000000000000000573971850987445072250355453639813258313559690103149414062500000027952803104429319921875-bit, 0.0000000000000000000000000000000000000000028698592549372253612517772681990662915677984505157470703125000000139764015522146599909375-bit, 0.00000000000000000000000000000000000000000143492962746861268062588863409953314578389922525787353515625000000069882007761073299996875-bit, 0.0000000000000000000000000000000000000000007174648137343063403129443170499765728919496126289367675781250000000349440038805366499984375-bit, 0.000000000000000000000000000000000000000000358732406867153170156472158524988286445974806314468383789062500000001747200194026824999921875-bit, 0.000000000000000000000000000000000000000000179366203433576585078236079262494143222987403157234191894531250000000087360009701341249999609375-bit, 0.000000000000000000000000000000000000000000089683101716788292539118039631247071611493720157617070947265625000000004368000485067062499998046875-bit, 0.00000000000000000000000000000000000000000004484155085839414626955901981562353580574686007880853547363281250000000218400024253353124999940234375-bit, 0.000000000000000000000000000000000000000000022420775429197073134779509907811767902873430039404267736816406250000001092000121266765624999701171875-bit, 0.00000000000000000000000000000000000000000001121038771459853656738975495390588395143671501970213386840820312500000005460000606333781249998505859375-bit, 0.000000000000000000000000000000000000000000005605193857299268283694877476952941975718357509851066934204410156250000000273000030316689062499992529296875-bit, 0.00000000000000000000000000000000000000000000280259692864963414184743873847647098785917875492553346710220507812500000013650001515834453124999962646484375-bit, 0.00000000000000000000000000000000000000000000140129846432481707092371936923823549392958937746276673355110253906250000000682500075791722656249999813232421875-bit, 0.00000000000000000000000000000000000000000000070064923216240853546185968461911774696479468873138336677555126953125000000034125003789586132812499999066112109375-bit, 0.000000000000000000000000000000000000000000000350324616081204267730929842309558873482397344365691683387775634765625000000017062501894793066406249999953305560546875-bit, 0.000000000000000000000000000000000000000000000175162308040602133865464921154779436741198672182845841693887817382812500000000853125094739653320312499999766527802734375-bit, 0.000000000000000000000000000000000000000000000087581154020301066932732460577389718370599336091422292096943908691406250000000042656254
```

eax	0x8	8
ecx	0x804a000	134520832
edx	0x8	8
ebx	0x1	1
esp	0xffffd1d0	0xffffd1d0
ebp	0x0	0x0
esi	0x0	0
edi	0x0	0
eip	0x8049016	0x8049016 <_start+22>
eflags	0x202	[ IF ]
cs	0x23	35
ss	0x2b	43
ds	0x2b	43
es	0x2b	43

Рис. 3.19: .

Для отображения содержимого памяти можно использовать команду `x`, которая выдаёт содержимое ячейки памяти по указанному адресу. Формат, в котором выводятся данные, можно задать после имени команды через косую черту: `x/NFU`. С помощью команды `x &` также можно посмотреть содержимое переменной. Посмотрели значение переменной `msg1` по имени. (рис. 3.20)

```
(gdb) x/1sb &msg1
0x804a000: "Hello, "
```

Рис. 3.20: .

Посмотрели значение переменной `msg2` по адресу. Адрес переменной определили по дизассемблированной инструкции. Посмотрели инструкцию `mov ecx,msg2` которая записывает в регистр `ecx` адрес переменной `msg2`. (рис. 3.21)

```
(gdb) x /1sb 0x804a008
0x804a008: "world!\n"
```

Рис. 3.21: .

Изменить значение для регистра или ячейки памяти можно с помощью команды `set`, задав ей в качестве аргумента имя регистра или адрес. При этом перед именем регистра ставится префикс `$`, а перед адресом нужно указать в фигурных скобках тип данных. Изменили первый символ переменной `msg1`. (рис. 3.22)

```
(gdb) set {char}0x804a000='h'
(gdb) x /1sb &msg1
0x804a000 <msg1>: "hello, "
```

Рис. 3.22: .

Замените первый символ во второй переменной msg2. (рис. 3.23)

```
(gdb) set {char}0x804a008='f'
(gdb) x /1sb &msg2
0x804a008 <msg2>: "for1d!\n\034"
```

Рис. 3.23: .

Чтобы посмотреть значения регистров используется команда print /F . Вывели в различных форматах (в шестнадцатеричном формате, в двоичном формате и в символьном виде) значение регистра edx. (рис. 3.24)

```
(gdb) p/s $edx
$5 = 0
(gdb) p/x $edx
$6 = 0x0
(gdb) p/t $edx
$7 = 0
(gdb) p/s $edx
$8 = 0
```

Рис. 3.24: .

С помощью команды set измените значение регистра ebx: (рис. 3.25)

```
(gdb) set $ebx='2'
(gdb) p/s $ebx
$3 = 50
(gdb) set $ebx=2
(gdb) p/s $ebx
$4 = 2
```

Рис. 3.25: .

Разница вывода команд p/s \$ebx:

Завершили выполнение программы с помощью команды continue (сокращенно c) и вышли из GDB с помощью команды quit (сокращенно q). (рис. 3.26), (рис. 3.27)



```
(gdb) c
Continuing.
hello, world!

Breakpoint 2, _start () at lab10-2.asm:20
20      mov ebx, 0
(gdb) c
Continuing.
[Inferior 1 (process 119368) exited normally]
```

Рис. 3.26: .

```
(gdb) q
[Inferior 1 (process 119368) exited normally]
```

Рис. 3.27: .

### 3.5 Обработка аргументов командной строки в GDB

Скопировали файл lab9-2.asm, созданный при выполнении лабораторной работы №9, с программой выводящей на экран аргументы командной строки (Листинг 9.2) в файл с именем lab10-3.asm: (рис. 3.28)

```
[earihzhov@fedora lab10]$ cp ~/work/arch-pc/lab09/lab9-2.asm ~/work/arch-pc/lab10/lab10-3.asm
```

Рис. 3.28: .

Создали исполняемый файл. (рис. 3.29)

```
[earihzhov@fedora lab10]$ nasm -f elf -g -l lab10-3.lst lab10-3.asm
[earihzhov@fedora lab10]$ ld -m elf_i386 -o lab10-3 lab10-3.o
```

Рис. 3.29: .

Для загрузки в gdb программы с аргументами необходимо использовать ключ `--args`. Загрузили исполняемый файл в отладчик, указав аргументы: (рис. 3.30)

```
[earihzhov@fedora lab10]$ gdb --args lab10-3 аргумент1 аргумент2 'аргумент 3'
```

Рис. 3.30: .

Как отмечалось в предыдущей лабораторной работе, при запуске программы аргументы командной строки загружаются в стек. Исследовали расположение

аргументов командной строки в стеке после запуска программы с помощью gdb. Для начала установили точку останова перед первой инструкцией в программе и запустили ее. (рис. 3.31)

```
(gdb) b _start
Breakpoint 1 at 0x80490e8: file lab10-3.asm, line 5.
(gdb) r
Starting program: /home/earihzhov/work/arch-pc/lab10/lab10-3 аргумент1 аргумент 2
аргумент\ 3

This GDB supports auto-downloading debuginfo from the following URLs:
https://debuginfod.fedoraproject.org/
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gdbinit.

Breakpoint 1, _start () at lab10-3.asm:5
5      pop ecx ; Извлекаем из стека в `ecx` количество
(gdb)
```

Рис. 3.31: .

Адрес вершины стека храниться в регистре esp и по этому адресу располагается число равное количеству аргументов командной строки (включая имя программы): (рис. 3.32)

```
(gdb) x/x $esp
0xfffffd180: 0x00000005
(gdb)
```

Рис. 3.32: .

Как видно, число аргументов равно 5 – это имя программы lab10-3 и непосредственно аргументы: аргумент1, аргумент, 2 и ‘аргумент 3’. Посмотрели остальные позиции стека – по адресу [esp+4] располагается адрес в памяти где находится имя программы, по адресу [esp+8] храниться адрес первого аргумента, по адресу [esp+12] – второго и т.д. (рис. 3.33)

```
(gdb) x/s *(void**)($esp + 4)
0xfffffd34b: "/home/earihzhov/work/arch-pc/lab10/lab10-3"
(gdb) x/s *(void**)($esp + 8)
0xfffffd37e: "аргумент1"
(gdb) x/s *(void**)($esp + 12)
0xfffffd388: "аргумент"
(gdb) x/s *(void**)($esp + 16)
0xfffffd399: "2"
(gdb) x/s *(void**)($esp + 20)
0xfffffd39b: "аргумент 3"
(gdb) x/s *(void**)($esp + 24)
0x0: <error: Cannot access memory at address 0x0>
(gdb)
```

Рис. 3.33: .

Шаг изменения адреса равен 4 ([esp+4], [esp+8], [esp+12] и т.д.), потому что в теле цикла 4 строки кода.

## 3.6 Задание для самостоятельной работы

1. Преобразовали программу из лабораторной работы №9 (Задание №1 для самостоятельной работы), реализовав вычисление значения функции  $f(x)$  как подпрограмму. (рис. 3.34), (рис. 3.35), (рис. 3.36)

```
[earihzhov@fedora lab10]$ cp ~/work/arch-pc/lab09/lab9-4.asm ~/work/arch-pc/lab10/lab10-4.asm
```

Рис. 3.34: .

```
Открыть ▾ + lab10-4.asm
~/work/arch-pc/lab10

por eax ; иначе извлекаем следующий аргумент из стека
call atoi ; преобразуем символ в число

call _func

add esi, eax ; добавляем к промежуточной сумме
; след. аргумент `esi=esi+eax`
loop next ; переход к обработке следующего аргумента
_end:
mov eax, msg ; вывод сообщения "Результат: "
call sprint
mov eax, esi ; записываем сумму в регистр `eax`
call iprintLF ; печать результата
call quit ; завершение программы

_func:
    mov ebx, 2
    add eax, ebx
    mov eax, eax
    mov ebx, 3
    mul ebx
    ret
```

Рис. 3.35: .

```
[earihzhov@fedora lab10]$ nasm -f elf lab10-4.asm
[earihzhov@fedora lab10]$ ld -m elf_i386 -o lab10-4 lab10-4.o
[earihzhov@fedora lab10]$ ./lab10-4 1 2 3
f(x) = 3(x + 2)
Результат: 36
```

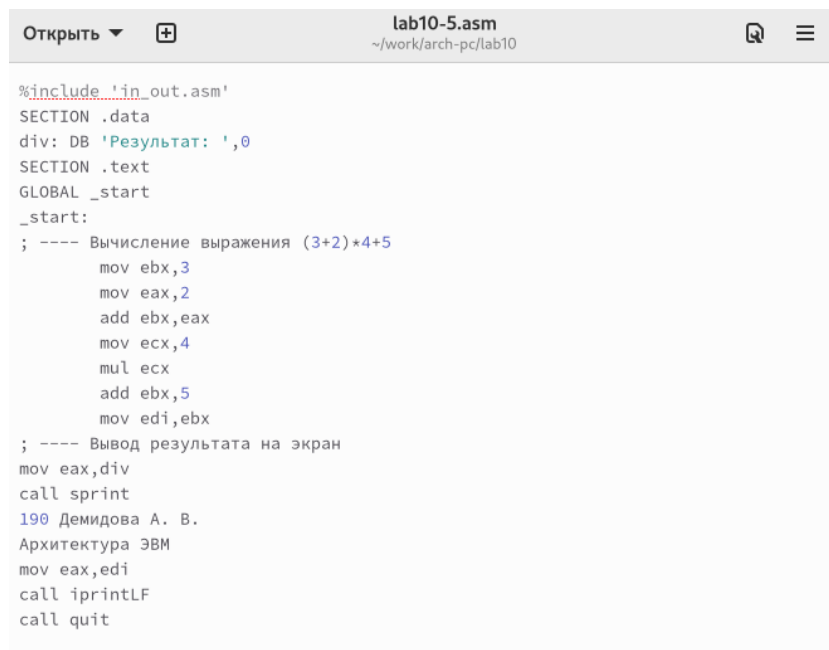
Рис. 3.36: .

2. В листинге 10.3 приведена программа вычисления выражения  $(3 + 2) \times 4 + 5$ .

Создали файл (рис. 3.37), записали туда код листинга (рис. 3.38), создали исполняющий файл (рис. 3.39), при запуске обнаружили вывод неверного результата (рис. 3.40).

```
[earihzhov@fedora lab10]$ touch lab10-5.asm
```

Рис. 3.37: .



```
Открыть  lab10-5.asm
~/work/arch-pc/lab10

%include 'in_out.asm'
SECTION .data
div: DB 'Результат: ',0
SECTION .text
GLOBAL _start
_start:
; ---- Вычисление выражения (3+2)*4+5
    mov ebx,3
    mov eax,2
    add ebx,eax
    mov ecx,4
    mul ecx
    add ebx,5
    mov edi,ebx
; ---- Вывод результата на экран
    mov eax,div
    call sprint
190 Демидова А. В.
Архитектура ЭВМ
    mov eax,edi
    call iprintLF
    call quit
```

Рис. 3.38: .

```
[earihzhov@fedora lab10]$ nasm -f elf -g -l lab10-5.lst lab10-5.asm
[earihzhov@fedora lab10]$ ld -m elf_i386 -o lab10-5 lab10-5.o
```

Рис. 3.39: .

```
[earihzhov@fedora lab10]$ ./lab10-5
Результат: 10
```

Рис. 3.40: .

Запустили файл в отладчике GDB (рис. 3.41), установили точку останова (рис. 3.42), запустили код (рис. 3.43), включили режим псевдографики (рис. 3.44), пошагово прошли все строчки кода (рис. 3.45), (рис. 3.46), (рис. 3.47), (рис. 3.48), (рис. 3.49), (рис. 3.50), (рис. 3.51), (рис. 3.52), обнаружили ошибку: вместо регистра ebx на 4 умножался eax, а 5 прибавлялась не к произведению, а только к ebx, исправили её (рис. 3.53), проверили результат работы программы (рис. 3.54).

```
[earihzhov@fedora lab10]$ gdb lab10-5
```

Рис. 3.41: .

```
(gdb) b _start
Breakpoint 1 at 0x80490e8: file lab10-5.asm, line 8.
```

Рис. 3.42: .

```
(gdb) r
Starting program: /home/earihzhov/work/arch-pc/lab10/lab10-5
```

Рис. 3.43: .

```

[ Register Values Unavailable ]

B+> 0x80490e8 <_start>    mov     $0x3,%ebx
      0x80490ed <_start+5> mov     $0x2,%eax
      0x80490f2 <_start+10> add     %eax,%ebx
      0x80490f4 <_start+12> mov     $0x4,%ecx
      0x80490f9 <_start+17> mul     %ecx
      0x80490fb <_start+19> add     $0x5,%ebx
      0x80490fe <_start+22> mov     %ebx,%edi
      0x8049100 <_start+24> mov     $0x804a000,%eax
      0x8049105 <_start+29> call    0x804900f <sprint>
      0x804910a <_start+34> mov     %edi,%eax
      0x804910c <_start+36> call    0x8049086 <iprintf>
      0x8049111 <_start+41> call    0x80490db <quit>

native process 47532 In: _start          L8    PC: 0x80490e8
(gdb) layout regs
(gdb)

```

Рис. 3.44: .

```

--Register group: general--
eax      0x0      0
ecx      0x0      0
edx      0x0      0
ebx      0x3      3
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x80490ed 0x80490ed <_start+5>
eflags   0x202    [ IF ]
cs       0x23     35

B+ 0x80490e8 <_start>    mov    $0x3,%ebx
> 0x80490ed <_start+5>  mov    $0x2,%eax
0x80490f2 <_start+10>   add    %eax,%ebx
0x80490f4 <_start+12>   mov    $0x4,%ecx
0x80490f9 <_start+17>   mul    %ecx
0x80490fb <_start+19>   add    $0x5,%ebx
0x80490fe <_start+22>   mov    %ebx,%edi
0x8049100 <_start+24>   mov    $0x804a000,%eax
0x8049105 <_start+29>   call   0x804900f <sprint>
0x804910a <_start+34>   mov    %edi,%eax
0x804910c <_start+36>   call   0x8049086 <iprintLF>
0x8049111 <_start+41>   call   0x80490db <quit>

native process 47532 In: _start L9 PC: 0x80490ed
(gdb) layout regs
(gdb) stepi
(gdb)

```

Рис. 3.45: .

```

--Register group: general--
eax      0x2      2
ecx      0x0      0
edx      0x0      0
ebx      0x3      3
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x80490f2 0x80490f2 <_start+10>
eflags   0x202    [ IF ]
cs       0x23     35

B+ 0x80490e8 <_start>    mov    $0x3,%ebx
0x80490ed <_start+5>    mov    $0x2,%eax
> 0x80490f2 <_start+10>  add    %eax,%ebx
0x80490f4 <_start+12>   mov    $0x4,%ecx
0x80490f9 <_start+17>   mul    %ecx
0x80490fb <_start+19>   add    $0x5,%ebx
0x80490fe <_start+22>   mov    %ebx,%edi
0x8049100 <_start+24>   mov    $0x804a000,%eax
0x8049105 <_start+29>   call   0x804900f <sprint>
0x804910a <_start+34>   mov    %edi,%eax
0x804910c <_start+36>   call   0x8049086 <iprintLF>
0x8049111 <_start+41>   call   0x80490db <quit>

native process 47532 In: _start L10 PC: 0x80490f2
(gdb) layout regs
(gdb) stepi
(gdb) stepi
(gdb)

```

Рис. 3.46: .

```

--Register group: general
eax      0x2      2
ecx      0x0      0
edx      0x0      0
ebx      0x5      5
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x80490f4 0x80490f4 <_start+12>
eflags   0x206    [ PF IF ]
cs       0x23     35

B+ 0x80490e8 <_start>    mov    $0x3,%ebx
0x80490ed <_start+5>    mov    $0x2,%eax
0x80490f2 <_start+10>   add    %eax,%ebx
> 0x80490f4 <_start+12> mov    $0x4,%ecx
0x80490f9 <_start+17>   mul    %ecx
0x80490fb <_start+19>   add    $0x5,%ebx
0x80490fe <_start+22>   mov    %ebx,%edi
0x8049100 <_start+24>   mov    $0x804a000,%eax
0x8049105 <_start+29>   call   0x804900f <sprint>
0x804910a <_start+34>   mov    %edi,%eax
0x804910c <_start+36>   call   0x8049086 <iprintLF>
0x8049111 <_start+41>   call   0x80490db <quit>

native process 47532 In: _start L11 PC: 0x80490f4
(gdb) layout regs
(gdb) stepi
(gdb) stepi
(gdb) stepi

```

Рис. 3.47: .

```

--Register group: general
eax      0x2      2
ecx      0x4      4
edx      0x0      0
ebx      0x5      5
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x80490f9 0x80490f9 <_start+17>
eflags   0x206    [ PF IF ]
cs       0x23     35

B+ 0x80490e8 <_start>    mov    $0x3,%ebx
0x80490ed <_start+5>    mov    $0x2,%eax
0x80490f2 <_start+10>   add    %eax,%ebx
0x80490f4 <_start+12>   mov    $0x4,%ecx
> 0x80490f9 <_start+17> mul    %ecx
0x80490fb <_start+19>   add    $0x5,%ebx
0x80490fe <_start+22>   mov    %ebx,%edi
0x8049100 <_start+24>   mov    $0x804a000,%eax
0x8049105 <_start+29>   call   0x804900f <sprint>
0x804910a <_start+34>   mov    %edi,%eax
0x804910c <_start+36>   call   0x8049086 <iprintLF>
0x8049111 <_start+41>   call   0x80490db <quit>

```

Рис. 3.48: .

Register group: general		
eax	0x8	8
ecx	0x4	4
edx	0x0	0
ebx	0x5	5
esp	0xffffd1d0	0xffffd1d0
ebp	0x0	0x0
esi	0x0	0
edi	0x0	0
eip	0x80490fb	0x80490fb <_start+19>
eflags	0x202	[ IF ]
cs	0x23	35

B+	0x80490e8 <_start>	mov	\$0x3,%ebx
	0x80490ed <_start+5>	mov	\$0x2,%eax
	0x80490f2 <_start+10>	add	%eax,%ebx
	0x80490f4 <_start+12>	mov	\$0x4,%ecx
	0x80490f9 <_start+17>	mul	%ecx
>	0x80490fb <_start+19>	add	\$0x5,%ebx
	0x80490fe <_start+22>	mov	%ebx,%edi
	0x8049100 <_start+24>	mov	\$0x804a000,%eax
	0x8049105 <_start+29>	call	0x804900f <sprint>
	0x804910a <_start+34>	mov	%edi,%eax
	0x804910c <_start+36>	call	0x8049086 <iprintLF>
	0x8049111 <_start+41>	call	0x80490db <quit>

Рис. 3.49: .

Register group: general		
eax	0x8	8
ecx	0x4	4
edx	0x0	0
ebx	0xa	10
esp	0xffffd1d0	0xffffd1d0
ebp	0x0	0x0
esi	0x0	0
edi	0x0	0
eip	0x80490fe	0x80490fe <_start+22>
eflags	0x206	[ PF IF ]
cs	0x23	35

B+	0x80490e8 <_start>	mov	\$0x3,%ebx
	0x80490ed <_start+5>	mov	\$0x2,%eax
	0x80490f2 <_start+10>	add	%eax,%ebx
	0x80490f4 <_start+12>	mov	\$0x4,%ecx
	0x80490f9 <_start+17>	mul	%ecx
	0x80490fb <_start+19>	add	\$0x5,%ebx
>	0x80490fe <_start+22>	mov	%ebx,%edi
	0x8049100 <_start+24>	mov	\$0x804a000,%eax
	0x8049105 <_start+29>	call	0x804900f <sprint>
	0x804910a <_start+34>	mov	%edi,%eax
	0x804910c <_start+36>	call	0x8049086 <iprintLF>
	0x8049111 <_start+41>	call	0x80490db <quit>

Рис. 3.50: .



```

Register group: general
eax      0x8      8
ecx      0x4      4
edx      0x0      0
ebx      0xa      10
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0xa      10
eip      0x8049100 0x8049100 <_start+24>
eflags   0x206    [ PF IF ]
cs       0x23     35

B+ 0x80490e8 <_start>    mov    $0x3,%ebx
    0x80490ed <_start+5> mov    $0x2,%eax
    0x80490f2 <_start+10> add    %eax,%ebx
    0x80490f4 <_start+12> mov    $0x4,%ecx
    0x80490f9 <_start+17> mul    %ecx
    0x80490fb <_start+19> add    $0x5,%ebx
    0x80490fe <_start+22> mov    %ebx,%edi
> 0x8049100 <_start+24> mov    $0x804a000,%eax
    0x8049105 <_start+29> call   0x804900f <sprint>
    0x804910a <_start+34> mov    %edi,%eax
    0x804910c <_start+36> call   0x8049086 <iprintLF>
    0x8049111 <_start+41> call   0x80490db <quit>

```

Рис. 3.51: .

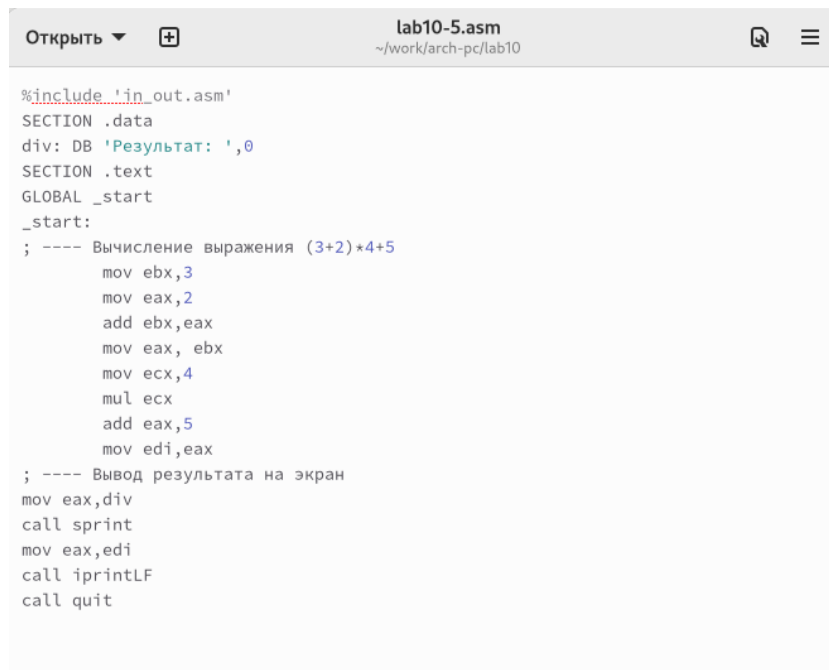
```

Register group: general
eax      0x804a000 134520832
ecx      0x4      4
edx      0x0      0
ebx      0xa      10
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0xa      10
eip      0x8049105 0x8049105 <_start+29>
eflags   0x206    [ PF IF ]
cs       0x23     35

B+ 0x80490e8 <_start>    mov    $0x3,%ebx
    0x80490ed <_start+5> mov    $0x2,%eax
    0x80490f2 <_start+10> add    %eax,%ebx
    0x80490f4 <_start+12> mov    $0x4,%ecx
    0x80490f9 <_start+17> mul    %ecx
    0x80490fb <_start+19> add    $0x5,%ebx
    0x80490fe <_start+22> mov    %ebx,%edi
    0x8049100 <_start+24> mov    $0x804a000,%eax
> 0x8049105 <_start+29> call   0x804900f <sprint>
    0x804910a <_start+34> mov    %edi,%eax
    0x804910c <_start+36> call   0x8049086 <iprintLF>
    0x8049111 <_start+41> call   0x80490db <quit>

```

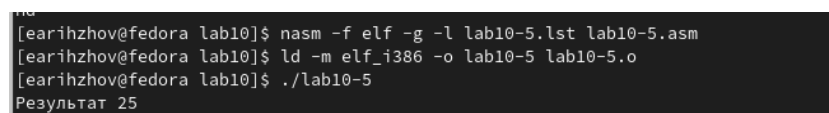
Рис. 3.52: .



```
Открыть ▾ + lab10-5.asm
~/work/arch-pc/lab10

%include 'in_out.asm'
SECTION .data
div: DB 'Результат: ',0
SECTION .text
GLOBAL _start
_start:
; ---- Вычисление выражения (3+2)*4+5
    mov ebx,3
    mov eax,2
    add ebx,eax
    mov eax, ebx
    mov ecx,4
    mul ecx
    add eax,5
    mov edi,eax
; ---- Вывод результата на экран
mov eax,div
call sprint
mov eax,edi
call iprintLF
call quit
```

Рис. 3.53: .



```
earihzhov@fedora lab10]$ nasm -f elf -g -l lab10-5.lst lab10-5.asm
earihzhov@fedora lab10]$ ld -m elf_i386 -o lab10-5 lab10-5.o
earihzhov@fedora lab10]$ ./lab10-5
Результат 25
```

Рис. 3.54: .

## 4 Выводы

В ходе выполнения лабораторной работы были приобретены навыки написания программ с использованием подпрограмм, ознакомились с методами отладки при помощи GDB и его основными возможностями.