

# **Отчёт по лабораторной работе 9**

**Понятие подпрограммы. Отладчик GDB.**

Калашникова Дарья Викторовна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
2.1	Реализация подпрограмм в NASM . . . . .	6
2.2	Отладка программы с помощью GDB . . . . .	9
2.3	Работа с аргументами командной строки . . . . .	18
2.4	Задание для самостоятельной работы . . . . .	19
2.5	Выводы . . . . .	25

## Список иллюстраций

2.1	Исходный код программы lab9-1.asm . . . . .	7
2.2	Результат выполнения программы . . . . .	7
2.3	Модифицированный код программы . . . . .	8
2.4	Результат выполнения модифицированной программы . . . . .	9
2.5	Код программы lab9-2.asm . . . . .	10
2.6	Запуск программы в отладчике . . . . .	11
2.7	Дизассемблированный код . . . . .	12
2.8	Дизассемблированный код в режиме Intel . . . . .	13
2.9	Установка точки останова . . . . .	14
2.10	Изменение значений регистров . . . . .	15
2.11	Отслеживание изменений регистров . . . . .	16
2.12	Изменение переменной . . . . .	17
2.13	Отображение измененного регистра . . . . .	17
2.14	Изменение регистра ebx . . . . .	18
2.15	Просмотр аргументов командной строки . . . . .	19
2.16	Код программы prog-1.asm . . . . .	20
2.17	Результат выполнения программы . . . . .	21
2.18	Код с ошибками . . . . .	22
2.19	Результат отладки . . . . .	23
2.20	Исправленный код программы . . . . .	24
2.21	Результат проверки . . . . .	25

## Список таблиц

# 1 Цель работы

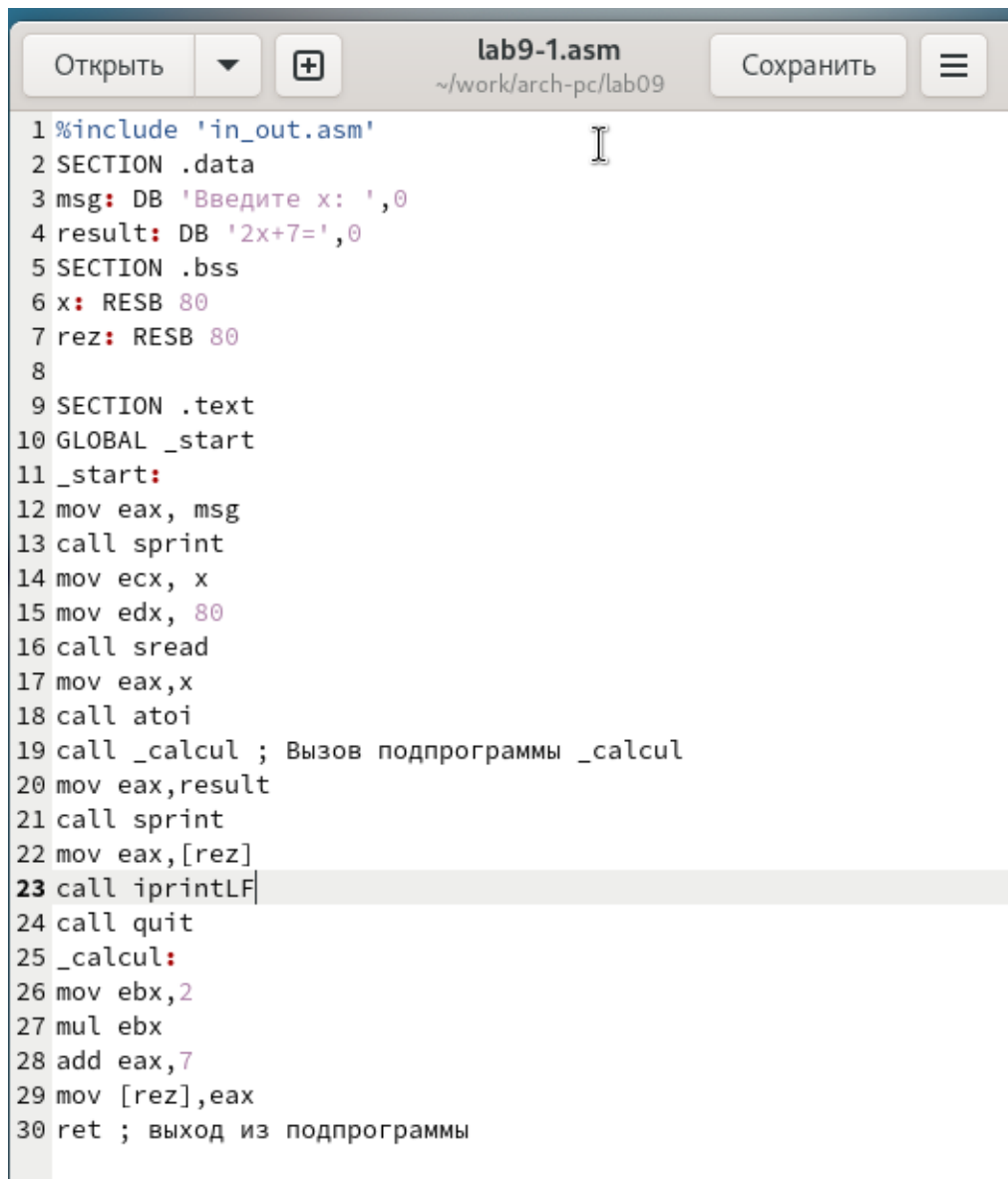
Целью работы является приобретение навыков написания программ с использованием подпрограмм. Знакомство с методами отладки при помощи GDB и его основными возможностями.

## 2 Выполнение лабораторной работы

### 2.1 Реализация подпрограмм в NASM

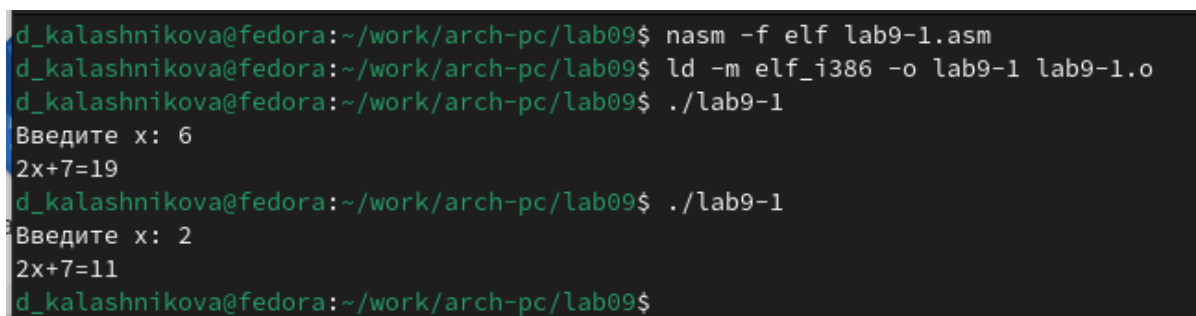
Сначала я создала новую папку для выполнения лабораторной работы №9 и перешла в нее. Затем создала файл с именем lab9-1.asm.

В качестве примера я реализовала программу, вычисляющую арифметическое выражение  $f(x) = 2x + 7$  с использованием подпрограммы calcul. Значение переменной  $x$  вводится с клавиатуры, а само выражение вычисляется в подпрограмме.



```
1 %include 'in_out.asm'
2 SECTION .data
3 msg: DB 'Введите x: ',0
4 result: DB '2x+7=',0
5 SECTION .bss
6 x: RESB 80
7 rez: RESB 80
8
9 SECTION .text
10 GLOBAL _start
11 _start:
12 mov eax, msg
13 call sprint
14 mov ecx, x
15 mov edx, 80
16 call sread
17 mov eax, x
18 call atoi
19 call _calcul ; Вызов подпрограммы _calcul
20 mov eax, result
21 call sprint
22 mov eax, [rez]
23 call iprintLF
24 call quit
25 _calcul:
26 mov ebx, 2
27 mul ebx
28 add eax, 7
29 mov [rez], eax
30 ret ; выход из подпрограммы
```

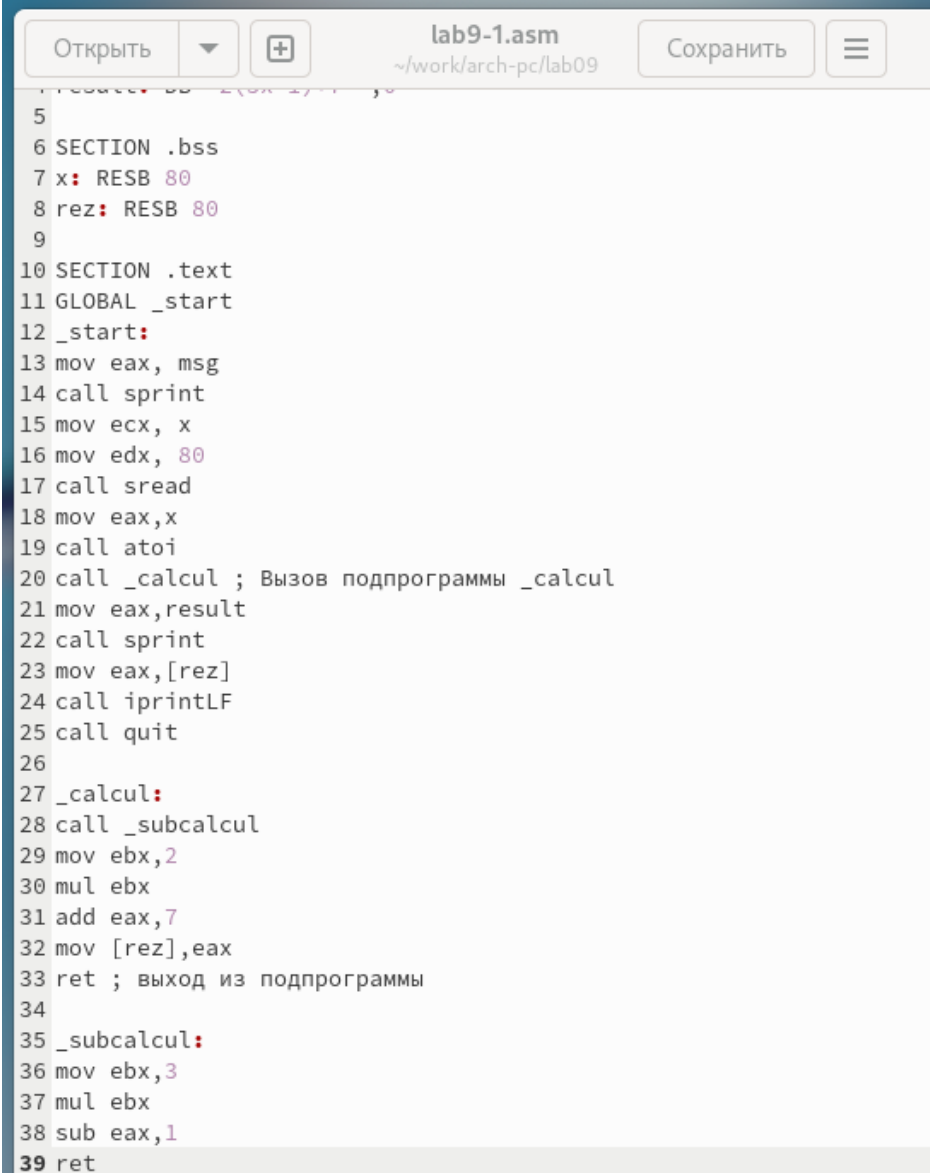
Рис. 2.1: Исходный код программы lab9-1.asm



```
d_kalashnikova@fedora:~/work/arch-pc/lab09$ nasm -f elf lab9-1.asm
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-1 lab9-1.o
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ./lab9-1
Введите x: 6
2x+7=19
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ./lab9-1
Введите x: 2
2x+7=11
d_kalashnikova@fedora:~/work/arch-pc/lab09$
```

Рис. 2.2: Результат выполнения программы

Затем я изменила текст программы, добавив подпрограмму `subcalcul` внутрь подпрограммы `calcul`. Это позволило вычислять составное выражение  $f(g(x))$ , где  $f(x) = 2x + 7$ ,  $g(x) = 3x - 1$ . Значение  $x$  также вводится с клавиатуры.



```
5
6 SECTION .bss
7 x: RESB 80
8 rez: RESB 80
9
10 SECTION .text
11 GLOBAL _start
12 _start:
13 mov eax, msg
14 call sprint
15 mov ecx, x
16 mov edx, 80
17 call sread
18 mov eax, x
19 call atoi
20 call _calcul ; Вызов подпрограммы _calcul
21 mov eax, result
22 call sprint
23 mov eax, [rez]
24 call iprintLF
25 call quit
26
27 _calcul:
28 call _subcalcul
29 mov ebx, 2
30 mul ebx
31 add eax, 7
32 mov [rez], eax
33 ret ; выход из подпрограммы
34
35 _subcalcul:
36 mov ebx, 3
37 mul ebx
38 sub eax, 1
39 ret
```

Рис. 2.3: Модифицированный код программы

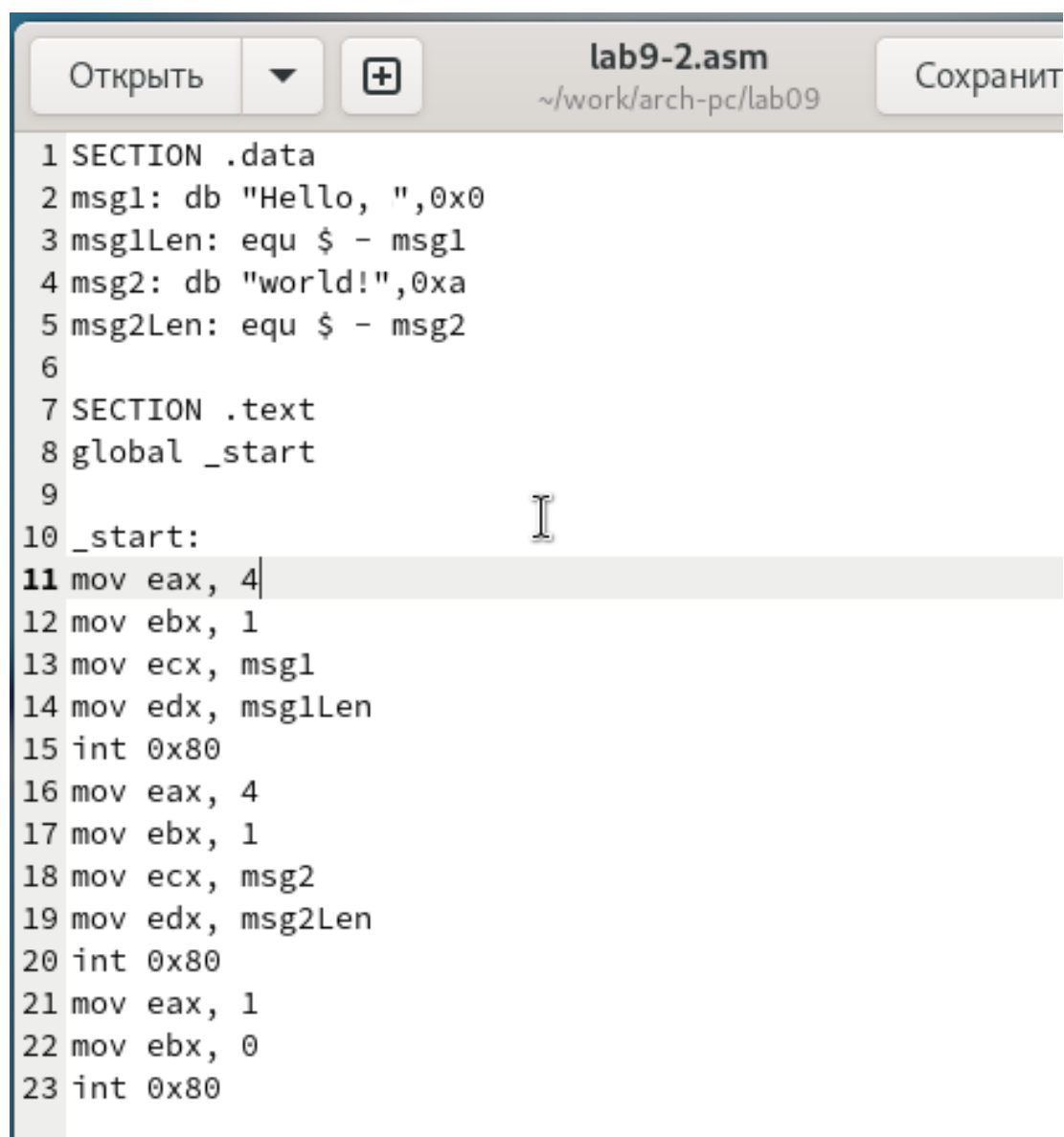


```
d_kalashnikova@fedora:~/work/arch-pc/lab09$  
d_kalashnikova@fedora:~/work/arch-pc/lab09$ nasm -f elf lab9-1.asm  
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-1 lab9-1.o  
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ./lab9-1  
Введите x: 6  
2(3x-1)+7=41  
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ./lab9-1  
Введите x: 2  
2(3x-1)+7=17  
d_kalashnikova@fedora:~/work/arch-pc/lab09$
```

Рис. 2.4: Результат выполнения модифицированной программы

## 2.2 Отладка программы с помощью GDB

Я создала файл lab9-2.asm, содержащий программу для вывода сообщения “Hello, world!” (Листинг 9.2).



```
1 SECTION .data
2 msg1: db "Hello, ",0x0
3 msg1Len: equ $ - msg1
4 msg2: db "world!",0xa
5 msg2Len: equ $ - msg2
6
7 SECTION .text
8 global _start
9
10 _start:
11 mov eax, 4
12 mov ebx, 1
13 mov ecx, msg1
14 mov edx, msg1Len
15 int 0x80
16 mov eax, 4
17 mov ebx, 1
18 mov ecx, msg2
19 mov edx, msg2Len
20 int 0x80
21 mov eax, 1
22 mov ebx, 0
23 int 0x80
```

Рис. 2.5: Код программы lab9-2.asm

Скомпилировала файл с ключом -g для добавления отладочной информации и загрузила его в GDB. Затем запустила программу командой run.

```

d_kalashnikova@fedora:~/work/arch-pc/lab09$
d_kalashnikova@fedora:~/work/arch-pc/lab09$ nasm -f elf -g -l lab9-2.lst lab9-2.asm
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-2 lab9-2.o
d_kalashnikova@fedora:~/work/arch-pc/lab09$ gdb lab9-2
GNU gdb (Fedora Linux) 15.1-1.fc39
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-redhat-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab9-2...
(gdb) r
Starting program: /home/d_kalashnikova/work/arch-pc/lab09/lab9-2

This GDB supports auto-downloading debuginfo from the following URLs:
    <https://debuginfod.fedoraproject.org/>
Enable debuginfod for this session? (y or [n])
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.
Hello, world!
[Inferior 1 (process 3558) exited normally]
(gdb)

```

Рис. 2.6: Запуск программы в отладчике

Установила точку останова на метке `_start`, запустила программу, а затем просмотрела дизассемблированный код.

```

(gdb) break _start
Breakpoint 1 at 0x8049000: file lab9-2.asm, line 11.
(gdb) run
Starting program: /home/d_kalashnikova/work/arch-pc/lab09/lab9-2

Breakpoint 1, _start () at lab9-2.asm:11
11      mov eax, 4
(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.
(gdb)

```

Рис. 2.7: Дизассемблированный код

```
End of assembler dump.
(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.
(gdb) █
```

Рис. 2.8: Дизассемблированный код в режиме Intel

Установила дополнительные точки останова, используя команды `info breakpoints` и `break`. Например, добавила точку на инструкции `mov ebx, 0x0`.

```
d_kalashnikova@fedora:~/work/arch-pc/lab09 — gdb lab9-2

Register group: general
eax      0x0      0      ecx      0x0      0
edx      0x0      0      ebx      0x0      0
esp      0xffffd0c0  0xffffd0c0  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
fs       0x0      0      gs       0x0      0

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
0x8049025 <_start+37> mov edx,0x7
0x804902a <_start+42> int 0x80
0x804902c <_start+44> mov eax,0x1
b+ 0x8049031 <_start+49> mov ebx,0x0

native process 3563 (asm) In: _start L11 PC: 0x8049000
(gdb) layout regs
(gdb) b *0x8049031
Breakpoint 2 at 0x8049031: file lab9-2.asm, line 22.
(gdb) i b
Num    Type      Disp Enb Address      What
1      breakpoint keep y  0x08049000 lab9-2.asm:11
       breakpoint already hit 1 time
2      breakpoint keep y  0x08049031 lab9-2.asm:22
(gdb) 
```

Рис. 2.9: Установка точки останова

С помощью команды `stepi` (или `si`) я пошагово выполняла инструкции, отслеживая изменения регистров.

```
d_kalashnikova@fedora:~/work/arch-pc/lab09 — gdb lab9-2

Register group: general
eax      0x4      4      ecx      0x0      0
edx      0x0      0      ebx      0x0      0
esp      0xffffd0c0 0xffffd0c0  ebp      0x0      0x0
esi      0x0      0      edi      0x0      0
eip      0x8049005 0x8049005 <_start+5>  eflags    0x202    [ IF ]
cs       0x23     35      ss       0x2b     43
ds       0x2b     43      es       0x2b     43
fs       0x0      0      gs       0x0      0

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
0x8049025 <_start+37>   mov     edx,0x7
0x804902a <_start+42>   int     0x80
0x804902c <_start+44>   mov     eax,0x1
b+ 0x8049031 <_start+49> mov     ebx,0x0

native process 3563 (asm) In: _start L12 PC: 0x8049005
esp      0xffffd0c0 0xffffd0c0
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 <RET> for more, q to quit, c to continue without paging--
fs       0x0      0
gs       0x0      0
(gdb) si
(gdb) 
```

Рис. 2.10: Изменение значений регистров

```
d_kalashnikova@fedora:~/work/arch-pc/lab09 — gdb lab9-2

Register group: general
eax      0x8      8      ecx      0x804a000    134520832
edx      0x8      8      ebx      0x1      1
esp      0xffffd0c0 0xffffd0c0  ebp      0x0      0x0
esi      0x0      0      edi      0x0      0
eip      0x8049016 0x8049016 <_start+2>  eflags   0x202    [ IF ]
cs       0x23     35      ss       0x2b     43
ds       0x2b     43      es       0x2b     43
fs       0x0      0      gs       0x0      0

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
0x8049025 <_start+37>  mov     edx,0x7
0x804902a <_start+42>  int     0x80
0x804902c <_start+44>  mov     eax,0x1
b+ 0x8049031 <_start+49> mov     ebx,0x0

native process 3563 (asm) In: _start L16 PC: 0x8049016
eip      0x8049000    0x8049000 <_start>
eflags   0x202      [ IF ]
cs       0x23       35
ss       0x2b       43
ds       0x2b       43
es       0x2b       43
--Type <RET> for more, q to quit, c to continue without paging--
fs       0x0        0
gs       0x0        0
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
```

Рис. 2.11: Отслеживание изменений регистров

Я также изменила значение переменной msg1 и регистров, используя команду set.



```

(gdb) si
(gdb) x/1sb &msg1
0x804a000 <msg1>:      "Hello, "
(gdb) x/1sb 0x804a008
0x804a008 <msg2>:      "world!\n\034"
(gdb) set {char}&msg1='h'
(gdb) x/1sb &msg1
0x804a000 <msg1>:      "hello, "
(gdb) set {char}0x804a008='L'
(gdb) x/1sb 0x804a008
0x804a008 <msg2>:      "Lor!d!\n\034"
(gdb)

```

Рис. 2.12: Изменение переменной

```

native process 3563 (asm) In: _start
(gdb) p/s $eax
$1 = 8
(gdb) p/t $eax
$2 = 1000
(gdb) p/s $ecx
$3 = 134520832
(gdb) p/x $ecx
$4 = 0x804a000
(gdb) p/s $edx
$5 = 8
(gdb) p/t $edx
$6 = 1000
(gdb) p/x $edx
$7 = 0x8
(gdb)

```

Рис. 2.13: Отображение измененного регистра

Используя аналогичные команды, я изменила значение регистра ebx.

```
(gdb) p/t $edx
$6 = 1000
(gdb) p/x $edx
$7 = 0x8
(gdb) set $ebx='2'
(gdb) p/s $ebx
$8 = 50
(gdb) set $ebx=2
(gdb) p/s $ebx
$9 = 2
(gdb) 
```

Рис. 2.14: Изменение регистра ebx

## 2.3 Работа с аргументами командной строки

Для работы с аргументами командной строки я использовала файл lab8-2.asm (из лабораторной работы №8), создав из него исполняемый файл. Затем загрузила программу в GDB с аргументами, используя ключ `-args`.

```
d_kalashnikova@fedora:~/work/arch-pc/lab09 — gdb --args lab9-3 argument 1 argument 2 argument 3
GNU gdb (Fedora Linux) 15.1-1.fc39
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-redhat-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab9-3...
(gdb) b _start
Breakpoint 1 at 0x80490e8: file lab9-3.asm, line 5.
(gdb) r
Starting program: /home/d_kalashnikova/work/arch-pc/lab09/lab9-3 argument 1 argument 2 argument\ 3

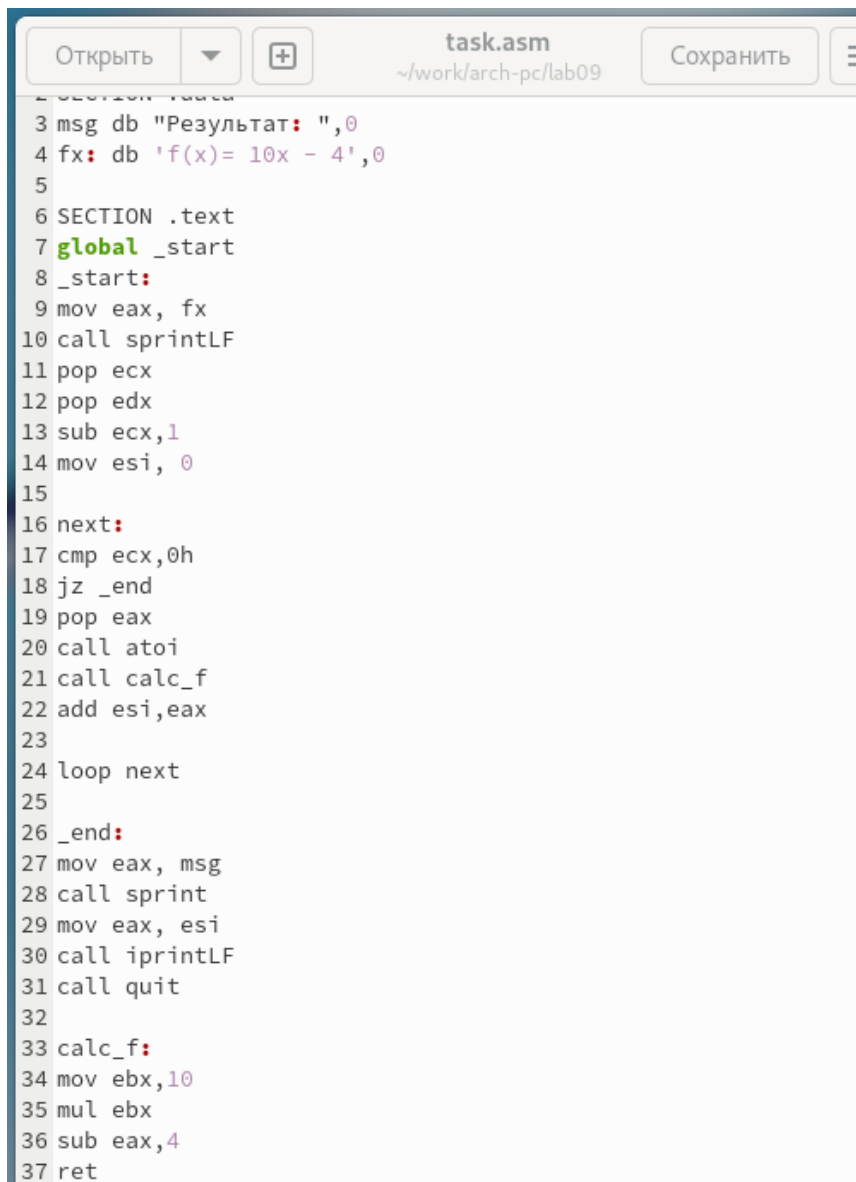
This GDB supports auto-downloading debuginfo from the following URLs:
<https://debuginfod.fedoraproject.org/>
Enable debuginfod for this session? (y or [n])
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.

Breakpoint 1, _start () at lab9-3.asm:5
5      pop ecx ; Извлекаем из стека в `ecx` количество
(gdb) x/x $esp
0xffffd090: 0x00000006
(gdb) x/s *(void**)(esp + 4)
0xffffd25a: "/home/d_kalashnikova/work/arch-pc/lab09/lab9-3"
(gdb) x/s *(void**)(esp + 8)
0xffffd289: "argument"
(gdb) x/s *(void**)(esp + 12)
0xffffd292: "1"
(gdb) x/s *(void**)(esp + 16)
0xffffd294: "argument"
(gdb) x/s *(void**)(esp + 20)
0xffffd29d: "2"
(gdb) x/s *(void**)(esp + 24)
0xffffd29f: "argument 3"
(gdb) 
```

Рис. 2.15: Просмотр аргументов командной строки

## 2.4 Задание для самостоятельной работы

В рамках задания я модифицировала программу из лабораторной работы №8, добавив подпрограмму для вычисления функции  $f(x)$ .



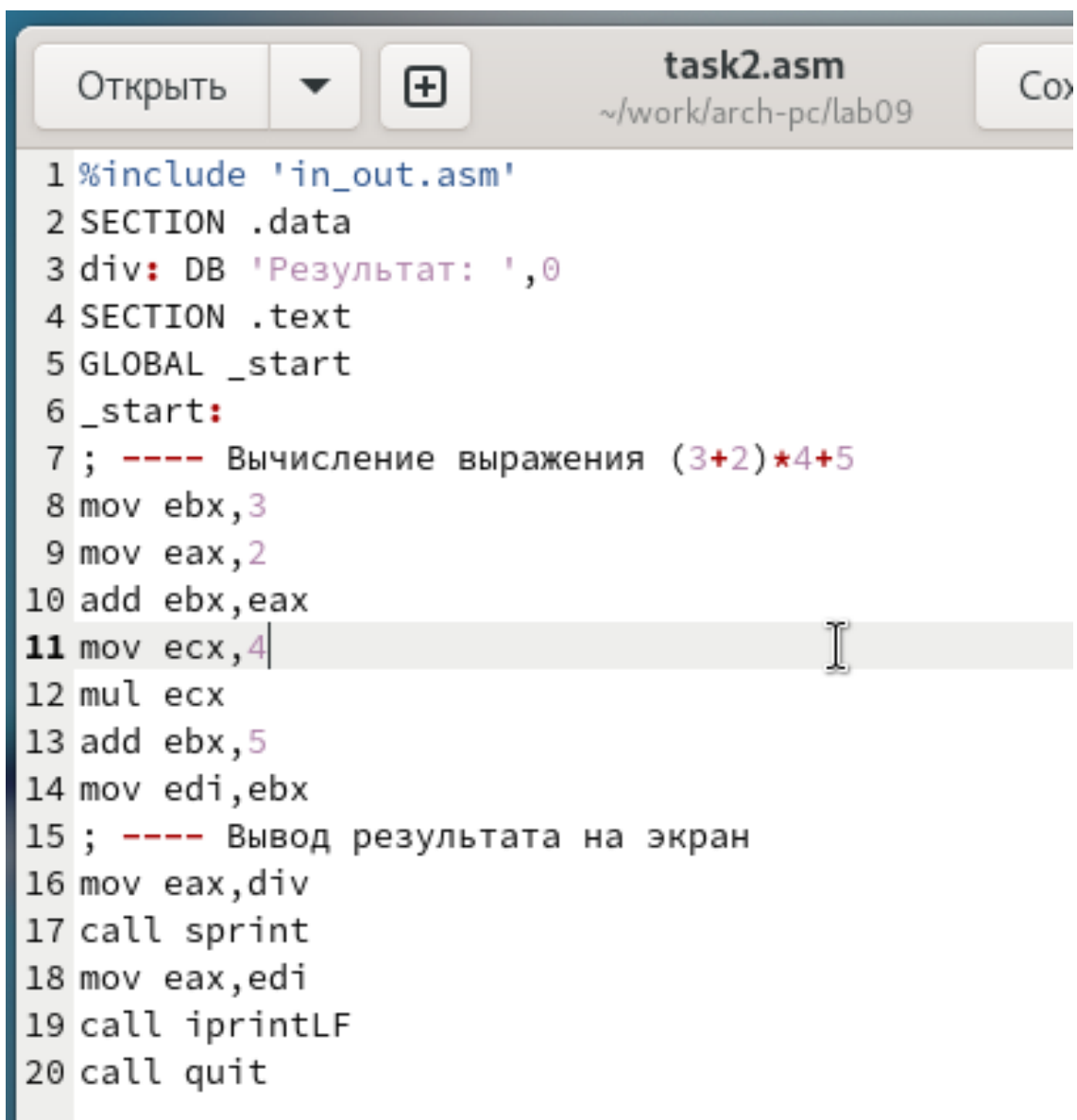
```
1 SECTION .data
2
3 msg db "Результат: ",0
4 fx: db 'f(x)= 10x - 4',0
5
6 SECTION .text
7 global _start
8 _start:
9 mov eax, fx
10 call sprintf
11 pop ecx
12 pop edx
13 sub ecx,1
14 mov esi, 0
15
16 next:
17 cmp ecx,0h
18 jz _end
19 pop eax
20 call atoi
21 call calc_f
22 add esi,eax
23
24 loop next
25
26 _end:
27 mov eax, msg
28 call sprintf
29 mov eax, esi
30 call iprintLF
31 call quit
32
33 calc_f:
34 mov ebx,10
35 mul ebx
36 sub eax,4
37 ret
```

Рис. 2.16: Код программы prog-1.asm

```
d_kalashnikova@fedora:~/work/arch-pc/lab09$  
d_kalashnikova@fedora:~/work/arch-pc/lab09$ nasm -f elf task.asm  
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 task.o -o task  
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ./task 4  
f(x)= 10x - 4  
Результат: 36  
d_kalashnikova@fedora:~/work/arch-pc/lab09$ ./task 4 5 6 3 1  
f(x)= 10x - 4  
Результат: 170  
d_kalashnikova@fedora:~/work/arch-pc/lab09$
```

Рис. 2.17: Результат выполнения программы

В процессе выполнения программы я обнаружила ошибку: порядок аргументов в инструкции `add` был перепутан, а регистр `ebx` вместо `eax` отправлялся в `edi`.



```
1 %include 'in_out.asm'
2 SECTION .data
3 div: DB 'Результат: ',0
4 SECTION .text
5 GLOBAL _start
6 _start:
7 ; ---- Вычисление выражения (3+2)*4+5
8 mov ebx,3
9 mov eax,2
10 add ebx,eax
11 mov ecx,4
12 mul ecx
13 add ebx,5
14 mov edi,ebx
15 ; ---- Вывод результата на экран
16 mov eax,div
17 call sprint
18 mov eax,edi
19 call iprintLF
20 call quit
```

Рис. 2.18: Код с ошибками

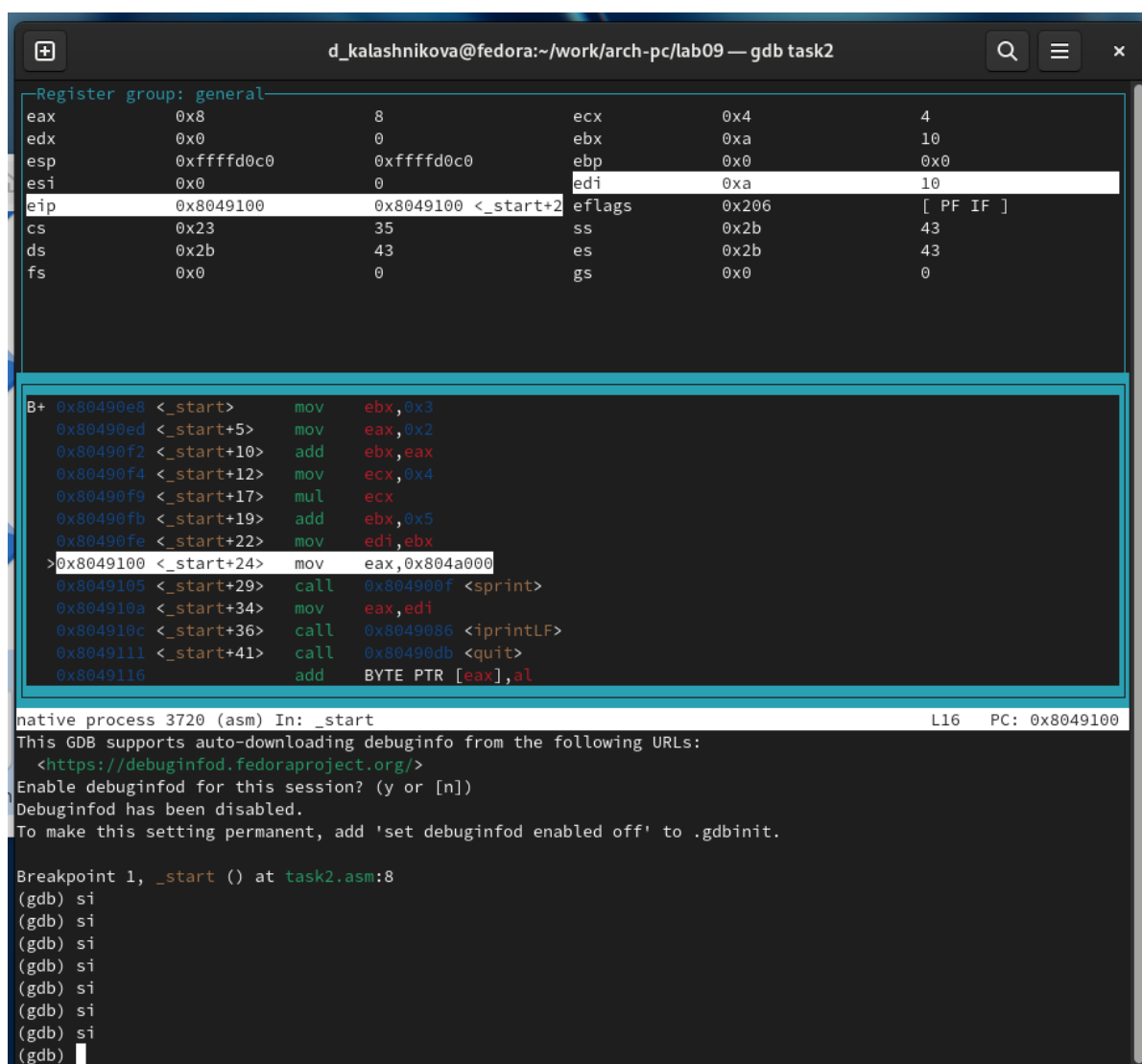
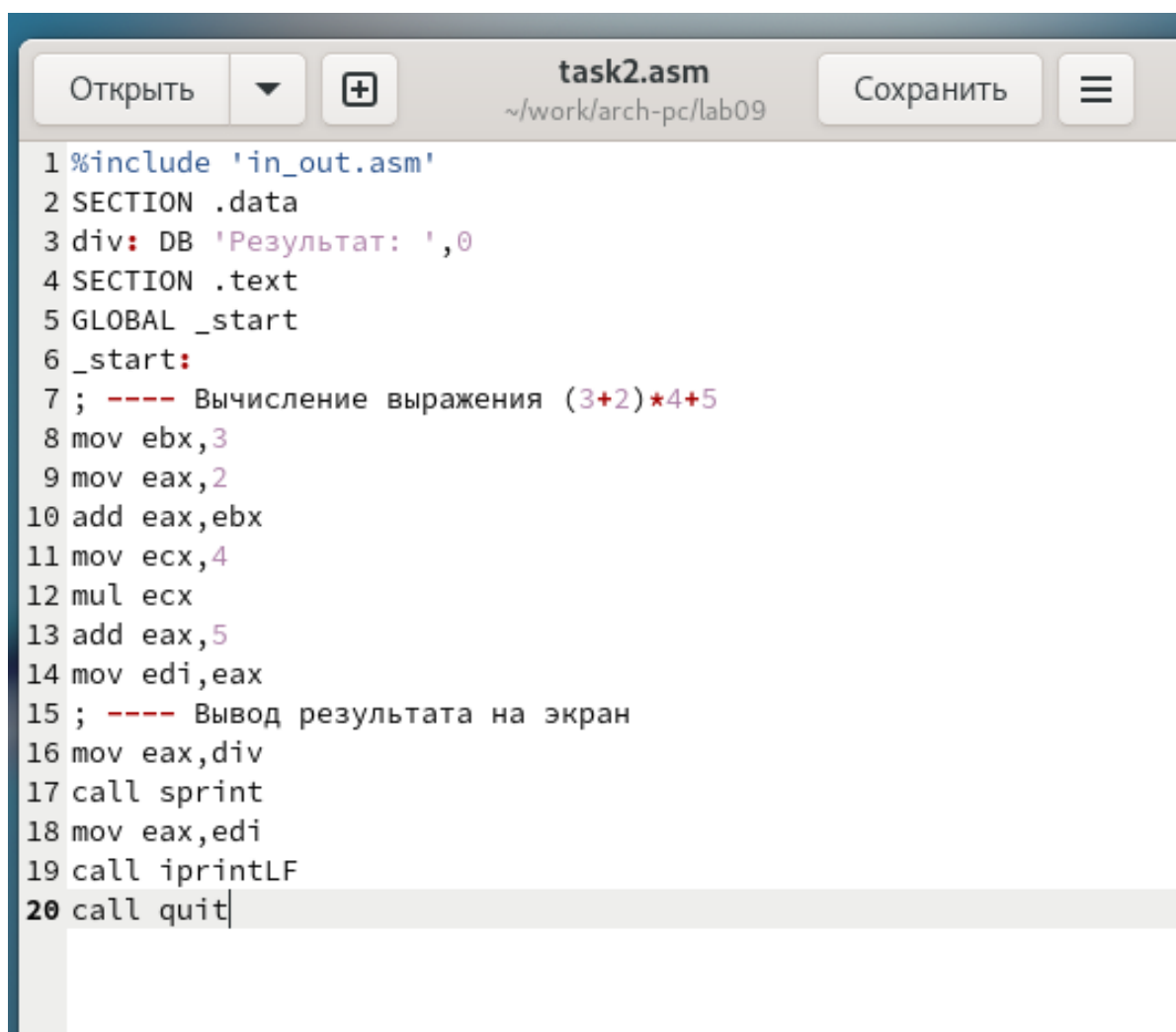


Рис. 2.19: Результат отладки

После исправления ошибок программа заработала корректно.



```
1 %include 'in_out.asm'
2 SECTION .data
3 div: DB 'Результат: ',0
4 SECTION .text
5 GLOBAL _start
6 _start:
7 ; ---- Вычисление выражения (3+2)*4+5
8 mov ebx,3
9 mov eax,2
10 add eax,ebx
11 mov ecx,4
12 mul ecx
13 add eax,5
14 mov edi,eax
15 ; ---- Вывод результата на экран
16 mov eax,div
17 call sprint
18 mov eax,edi
19 call iprintLF
20 call quit
```

Рис. 2.20: Исправленный код программы



The screenshot shows a GDB terminal window with the title bar "d\_kalashnikova@fedora:~/work/arch-pc/lab09 — gdb task2". The window is divided into three main sections. The top section displays register values: `eax` is `s` (value 25), `ecx` is `0x4` (value 4), and `edx` is `0x0` (value 0). Below these, a memory dump shows values `ffffd0c0`, `xxxxffd0c0`, and `x8049100 <_start+2`. The middle section shows assembly code with addresses and instructions: `0x8049100 <_start+24> mov eax,0x804a000`, `0x8049105 <_start+29> call 0x804900f <sprint>`, `0x804910a <_start+34> mov ecx,0di`, `0x804910c <_start+36> call 0x8049086 <iprintLF>`, and `0x8049111 <_start+41> call 0x80490db <quit>`. The bottom section shows the GDB prompt `>` and the output of the `rint>` command, which is `86 <iprintLF>`. The bottom status bar shows "native process 3761 (asm) In: \_start" and "PC: 0x8049100".

```
native process 3761 (asm) In: _start L16 PC: 0x8049100
Enable No process (asm) In: (y or [n]) L?? PC: ??
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.

Breakpoint 1, _start () at task2.asm:8
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) c
Continuing.
Результат: 25
[Inferior 1 (process 3761) exited normally]
(gdb)
```

Рис. 2.21: Результат проверки

## 2.5 Выводы

В ходе лабораторной работы я научилась работать с подпрограммами и отладчиком GDB, а также диагностировать и исправлять ошибки в ассемблерных программах.