

# **Лабораторная работа №9. Понятие подпрограммы. Отладчик GDB.**

**НПМбв-02-21**

Геллер Михаил

# Содержание

Цель работы	5
Задание	6
Выполнение лабораторной работы	7
Выводы	13

## **Список таблиц**

## Список иллюстраций

0.1. Создание и проверка работы файла вычисления арифметического выражения . . . . .	7
0.2. Пример работы файла с двумя подпрограммами вычисления арифметического выражения . . . . .	8
0.3. Создание и проверка работы файла печати сообщения и запуск отладки . . . . .	8
0.4. Создание и проверка работы файла вычисления арифметического выражения . . . . .	9
0.5. Установил точка останова по адресу инструкции в режиме псевдографики . . . . .	9
0.6. Посмотр значение переменной по адресу используя отображения содержимого памяти . . . . .	10
0.7. Посмотр позиции стека и определение размера шага изменения адреса. . . . .	10
0.8. Преобразовали программу из лабораторной работы №8, реализовав вычисление значения функции как подпрограмму . . . . .	11
0.9. Создали файл вычисления арифметического выражения, проверили его работу, обратили внимание на ошибку и запустили отладку. . . . .	11
0.10. Определение ошибки с помощью отладчика GDB . . . . .	12
0.11. Создание и проверка работы исправленного файла вычисления арифметического выражения . . . . .	12

## Цель работы

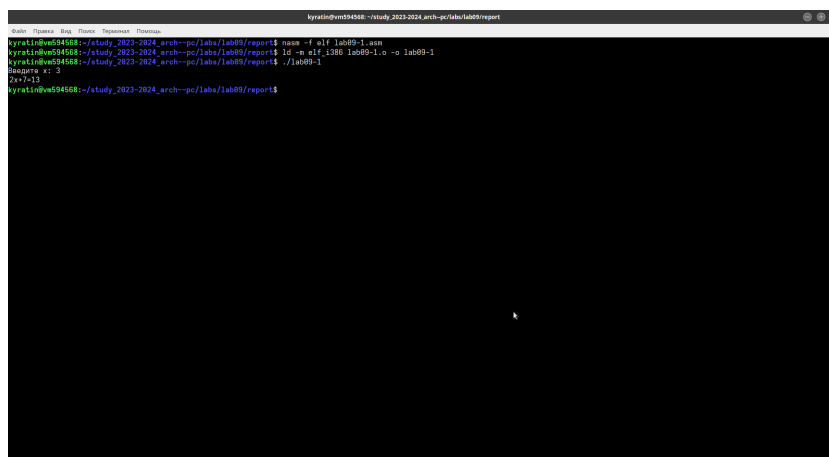
Получить навыки написания программ с использованием подпрограмм. Познакомиться с методами отладки при помощи GDB и его основными возможностями.

# Задание

1. Преобразуйте программу из лабораторной работы №8 (Задание №1 для самостоятельной работы), реализовав вычисление значения функции как подпрограмму.
2. В листинге 9.3 приведена программа вычисления выражения. При запуске данная программа дает неверный результат. Проверьте это. С помощью отладчика GDB, анализируя изменения значений регистров, определите ошибку и исправьте ее

# Выполнение лабораторной работы

Создал каталог для программ лабораторной работы, написал в файл lab09-1.asm текст программы из листинга 9.1. Создал исполняемый файл и проверил его работу. (рис. @fig:001).



```
kyratin@vm594568: ~/study_2023-2024_arch-pc/labs/lab09/report$  
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ nasm -f elf lab09-1.asm  
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ ld -o elf_i386 lab09-1.o -o lab09-1  
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ ./lab09-1  
Введите x: 3  
2*3=13  
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$
```

Рис. 0.1.: Создание и проверка работы файла вычисления арифметического выражения

Изменил текст программы добавив добавив две подпрограммы вычисления арифметического выражения. Создал исполняемый файл и проверил его работу(рис. @fig:002).

```
kyratin@vm594568: ~/study_2023-2024_arch-pc/labs/lab09/report
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ nasm -f elf lab09-1.asm
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ ld -m elf_i386 lab09-1.o -o lab09-1
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ ./lab09-1
f(x) = 2x+7
g(x) = 3x+1
Reporte x: 3
f(g(x))=23
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ 2x+7+13
-bash: 2x+7+13: command not found
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$
```

Рис. 0.2.: Пример работы файла с двумя подпрограммами вычисления арифметического выражения

Создал файл lab09-2.asm с текстом программы из Листинга 9.2. (Программа печати сообщения Hello world!) и проверил его работу. Начал отладку(рис. @fig:003).

```
kyratin@vm594568: ~/study_2023-2024_arch-pc/labs/lab09/report
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ touch lab09-2.asm
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ nasm -f elf -g -l lab09-2.lst lab09-2.asm
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ ld -m elf_i386 -o lab09-2 lab09-2.o
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09/report$ gdb lab09-2
GNU gdb (Debian 10.1-1.7) 10.1.90.20210103-git
Copyright (C) 2021 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-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 lab09-2...
(gdb) run
Starting program: /home/kyratin/study_2023-2024_arch-pc/labs/lab09/report/lab09-2
Hello, world!
[Inferior 1 (process 121775) exited normally]
(gdb)
```

Рис. 0.3.: Создание и проверка работы файла печати сообщения и запуск отладки

Проверил работу программы, запустив ее в оболочке GDB с помощью команды run. (рис. @fig:004).



```

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab09-2...
(gdb) run
Starting program: /home/kyratin/study_2023-2024_arch--pc/lab3/lab09/report/lab09-2
Hello, world!
[Inferior 1 (process 121775) exited normally]
(gdb) |

```

Рис. 0.4.: Создание и проверка работы файла вычисления арифметического выражения

В режиме псевдографики gdb была установлена точка останова по адресу инструкции. (рис. @fig:005).

```

kyratin@vm542566: ~/study_2023-2024_arch--pc/lab3/lab09
(gdb) info registers eip
eip      0x8040000      0x8040000 <_start>
(gdb) info all-registers
eax      0x0          0
ecx      0x0          0
edx      0x0          0
ebx      0x0          0
esp      0xffffd5f0    0xffffd5f0
ebp      0x0          0
i387_0   0x0          0
edi      0x0          0
esi      0x0400000    0x0400000 <_start>
eip      0x292        [ 1 ]
cs       0x23        35
ds       0x2b        43
ss       0x2b        43
fs       0x0          0
gs       0x0          0
r10      0            (raw 0x0000000000000000)
r11      0            (raw 0x0000000000000000)
r12      0            (raw 0x0000000000000000)
r13      0            (raw 0x0000000000000000)
r14      0            (raw 0x0000000000000000)
r15      0            (raw 0x0000000000000000)
r16      0            (raw 0x0000000000000000)
r17      0            (raw 0x0000000000000000)
r18      0x37f        895
fsat     0x0          0
fsbase   0xffff       65535
fsindex  0x0          0
fsoffset 0x0          0
foword   0x0          0
fcoff     0x0          0
fno      0x0          0
msgsr     0x1f80      [ 1] 0x 0x 0x 0x 0x 0x 0x 0x 0x 0x 0x 0x 0x 0x 0x 0x
msg0      (v10,0,float10 = (0x0 <repeats 10 times>), v8_float = (0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0), v4_double = (0x0, --Type <REI> for more, q to quit, c to continue without paging
--Type <REI> for more, q to quit, c to continue without paging--]

```

Рис. 0.5.: Установил точка останова по адресу инструкции в режиме псевдографики

Посмотрели значение переменной по адресу используя отображения содержимого памяти. Посмотрели инструкцию `mov esx,msg2` которая записывает в регистр `esx` адрес переменной `msg2` (рис. @fig:006).

```
kyratin@vm594568: ~/study_2023-2024_arch-pc/labs/lab09
A debugging session is active.

Inferior 1 [process 140046] will be killed.

Quit anyway? (y or n) y
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ gdb ./lab09-2
GNU gdb (Debian 10.1-1.7) 10.1.90.20210103-git
Copyright (C) 2021 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-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 ./lab09-2...
(gdb) run
Starting program: /home/kyratin/study_2023-2024_arch-pc/labs/lab09/lab09-2
Hello, world!
[Inferior 1 (process 140135) exited normally]
(gdb) set (char)msg1='h'
msg1 has unknown type; cast it to its declared type
(gdb) x/1sb &msg1
0x0040d000: "Hello, "
(gdb) set (char)msg1='h'
msg1 has unknown type; cast it to its declared type
(gdb) x/1sb &msg1
0x0040d000: "Hello, "
(gdb) |
```

Рис. 0.6.: Посмотр значение переменной по адресу используя отображения содержимого памяти

Посмотр позиции стека. Размер переменной - четыре байта и шаг изменения адреса равен размеру переменной (рис. @fig:007).

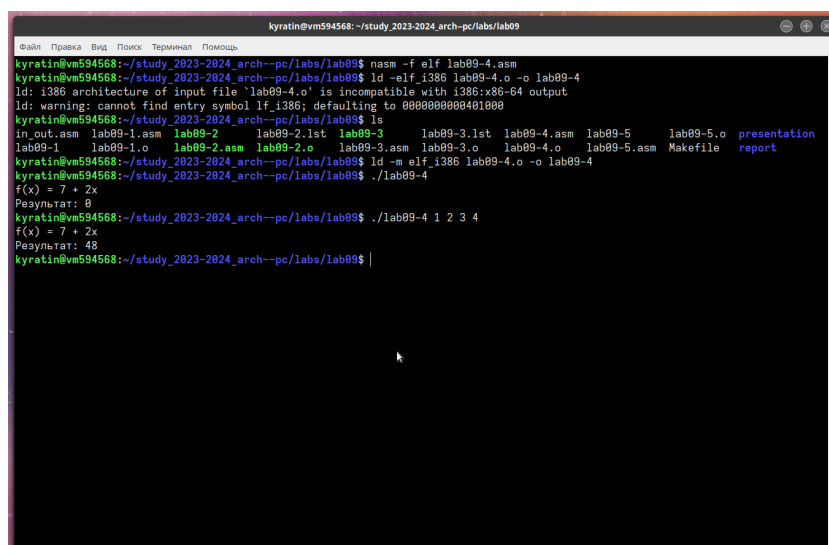
```
kyratin@vm594568: ~/study_2023-2024_arch-pc/labs/lab09
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./lab09-3...
(gdb) b _start
Breakpoint 1 at 0x00400000: file lab09-3.asm, line 5.
(gdb) run
Starting program: /home/kyratin/study_2023-2024_arch-pc/labs/lab09/lab09-3
Breakpoint 1, _start () at lab09-3.asm:5
    pop ecx; Изначем из стека в 'ecx' количество
(gdb) x/x step
No symbol "step" in current context.
(gdb) x/x $esp
0xfffff050: 0x00000001
(gdb) x/s *(void**)(esp + 4)
0xfffff023: "/home/kyratin/study_2023-2024_arch-pc/labs/lab09/lab09-3"
(gdb) x/s *(void**)(esp + 8)
0x0: <error: Cannot access memory at address 0x0>
(gdb) x/s *(void**)(esp + 6)
0xfffff023: <error: Cannot access memory at address 0xfffff>
(gdb) x/s *(void**)(esp + 2)
0x72300000: <error: Cannot access memory at address 0x72300000>
(gdb) x/s *(void**)(esp + 4)
0xfffff023: "/home/kyratin/study_2023-2024_arch-pc/labs/lab09/lab09-3"
(gdb) x/s *(void**)(esp + 16)
0xfffff023: "LANGUAGE=en_US:en"
(gdb) x/s *(void**)(esp + 32)
0xfffff023: "_usr/bin/gdb"
(gdb) |
```

Рис. 0.7.: Посмотр позиции стека и определение размера шага изменения адреса.

Преобразовали программу из лабораторной работы №8 (Задание №1 для са-

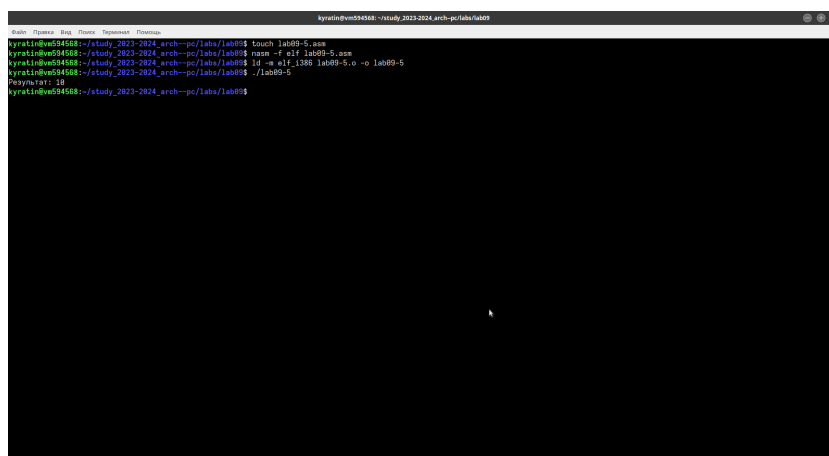
мостоятельной работы), реализовав вычисление значения функции как подпрограмму. (рис. @fig:008).



```
kyratin@vm594568: ~/study_2023-2024_arch-pc/labs/lab09
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ nasm -f elf lab09-4.asm
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ ld -elf_i386 lab09-4.o -o lab09-4
ld: i386 architecture of input file `lab09-4.o' is incompatible with i386:x86-64 output
ld: warning: cannot find entry symbol lf_i386; defaulting to 0000000000401000
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ ls
in out.asm lab09-1.asm lab09-2 lab09-2.lst lab09-3 lab09-3.lst lab09-4.asm lab09-5 lab09-5.o presentation
lab09-1 lab09-1.o lab09-2.asm lab09-2.o lab09-3.asm lab09-3.o lab09-4.o lab09-5.asm Makefile report
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ ld -m elf_i386 lab09-4.o -o lab09-4
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ ./lab09-4
f(x) = 7 + 2x
Результат: 0
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ ./lab09-4 1 2 3 4
f(x) = 7 + 2x
Результат: 48
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ |
```

Рис. 0.8.: Преобразовали программу из лабораторной работы №8, реализовав вычисление значения функции как подпрограмму

Создали файл вычисления арифметического выражения, проверили его работу, обратили внимание на ошибку и запустили отладку. (рис. @fig:009).

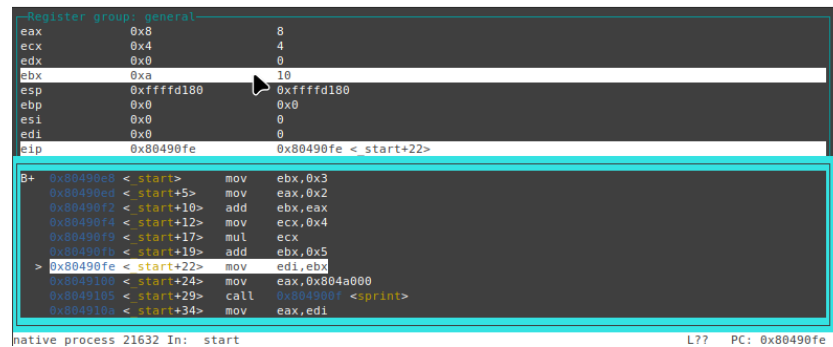


```
kyratin@vm594568: ~/study_2023-2024_arch-pc/labs/lab09
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ touch lab09-5.asm
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ nasm -f elf lab09-5.asm
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ ld -m elf_i386 lab09-5.o -o lab09-5
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$ ./lab09-5
Результат: 10
kyratin@vm594568:~/study_2023-2024_arch-pc/labs/lab09$
```

Рис. 0.9.: Создали файл вычисления арифметического выражения, проверили его работу, обратили внимание на ошибку и запустили отладку.

С помощью отладчика GDB, анализируя изменения значений реги-

стров,определил ошибку и исправил(рис. @fig:0010).



The screenshot shows the GDB interface. The top panel displays the 'Register group: general' with values for eax (0x8), ecx (0x4), edx (0x0), ebx (0xa), esp (0xffffd180), ebp (0x0), esi (0x0), edi (0x0), and eip (0x80490fe). The bottom panel shows the disassembly of the current instruction at address 0x80490fe, which is a 'mov edi,ebx' instruction. The instruction is highlighted with a red box. The status bar at the bottom indicates 'native process 21632 In: start' and 'L?? PC: 0x80490fe'.

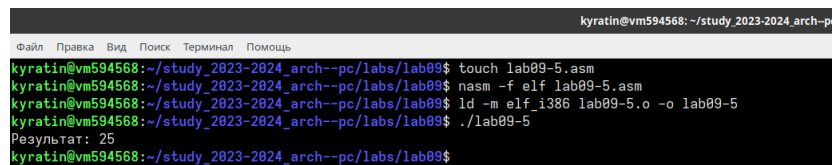
```
--Register group: general--
eax      0x8      8
ecx      0x4      4
edx      0x0      0
ebx      0xa     10
esp      0xffffd180 0xffffd180
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x80490fe 0x80490fe < start+22>

0x80490e8 < start+> mov     ebx,0x3
0x80490ed < start+5> mov     eax,0x2
0x80490f2 < start+10> add     ebx,eax
0x80490f4 < start+12> mov     ecx,0x4
0x80490f9 < start+17> mul     ecx
0x80490fb < start+19> add     ebx,0x5
> 0x80490fe < start+22> mov     edi,ebx
0x8049100 < start+24> mov     eax,0x804a000
0x8049105 < start+29> call    0x8049007 <sprint>
0x804910a < start+34> mov     eax,edi

native process 21632 In: start                                L??  PC: 0x80490fe
```

Рис. 0.10.: Определение ошибки с помощью отладчика GDB

Создал исполняемый исправленный файл, проверил его работу и убедился, что работает скрипт корректно. (рис. @fig:0011).



The screenshot shows a terminal window with the following commands and output:

```
kyratin@vm594568: ~/study_2023-2024_arch-pc/
Файл  Правка  Вид  Поиск  Терминал  Помощь
kyratin@vm594568:~/study_2023-2024_arch--pc/labs/lab09$ touch lab09-5.asm
kyratin@vm594568:~/study_2023-2024_arch--pc/labs/lab09$ nasm -f elf lab09-5.asm
kyratin@vm594568:~/study_2023-2024_arch--pc/labs/lab09$ ld -m elf_i386 lab09-5.o -o lab09-5
kyratin@vm594568:~/study_2023-2024_arch--pc/labs/lab09$ ./lab09-5
Результат: 25
kyratin@vm594568:~/study_2023-2024_arch--pc/labs/lab09$
```

Рис. 0.11.: Создание и проверка работы исправленного файла вычисления арифметического выражения

# Выводы

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