

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 9

дисциплина: *Архитектура компьютера*

Студент:

Батов Дмитрий Сергеевич

Группа:

НПМБВ-02-21

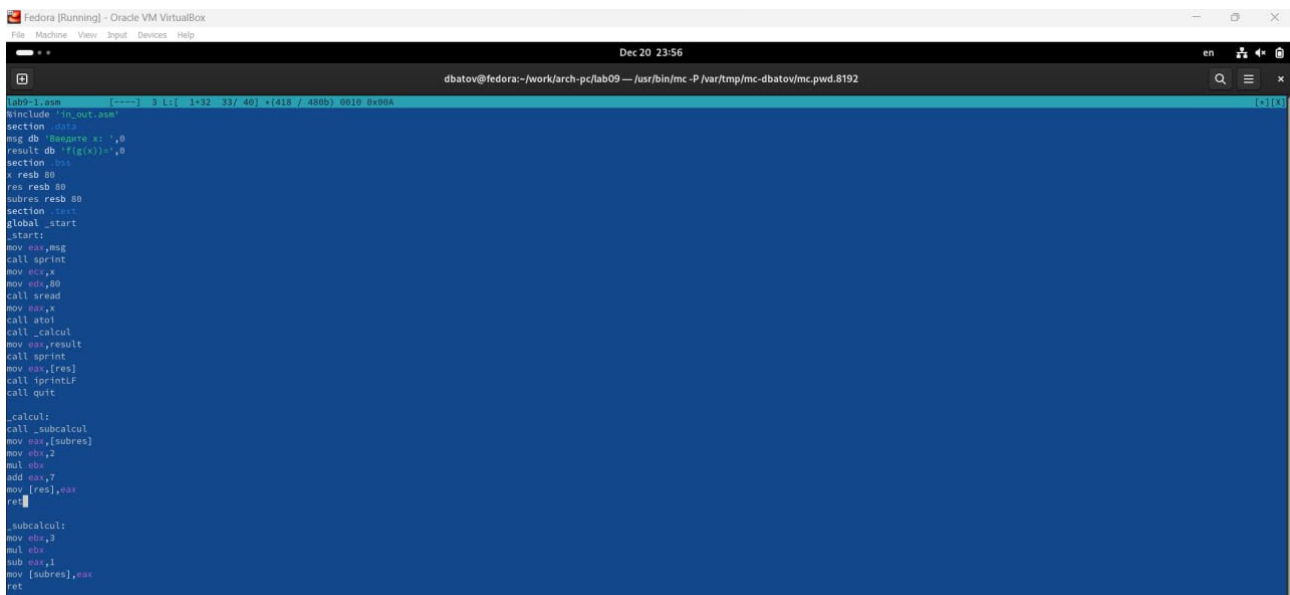
МОСКВА

2023 г.

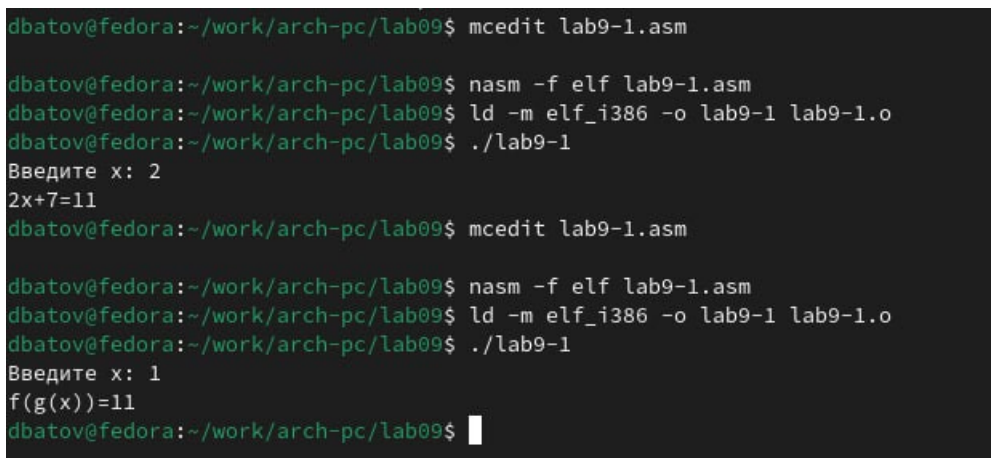
Цель работы – приобретение навыков написания программ с использованием подпрограмм, знакомство с методами отладки при помощи gdb и его основными возможностями.



```
lab9-1.asm [----] 13 L: 1+0 1/ 30 *(13 / 307b) 0111 0x00f
include "in_out.asm"
section .data
msg db "Введите x: ",0
result db "2x+7=",0
section .bss
x resb 80
res resb 80
section .text
global _start
_start:
mov eax,msg
call _write
mov ecx,x
mov eax,40
call _read
mov eax,x
call _atoi
call _calcul
mov eax,result
call _write
call _printf
call _exit
calcul:
mov ebx,2
mul ebx
add eax,7
mov [res],eax
ret
```



```
lab9-1.asm [----] 3 L: 1+32 33/ 40 *(41b / 480b) 0010 0x004
include "in_out.asm"
section .data
msg db "Введите x: ",0
result db "f(g(x))=",0
section .bss
x resb 80
res resb 80
subres resb 80
section .text
global _start
_start:
mov eax,msg
call _write
mov ecx,x
mov eax,40
call _read
mov eax,x
call _atoi
call _calcul
mov eax,result
call _write
call _printf
call _exit
calcul:
call _subcalcul
mov eax,[subres]
mov ebx,2
mul ebx
add eax,7
mov [res],eax
ret
subcalcul:
mov ebx,3
mul ebx
sub eax,1
mov [subres],eax
ret
```



```
dbatov@fedora:~/work/arch-pc/lab09$ mcedit lab9-1.asm
dbatov@fedora:~/work/arch-pc/lab09$ nasm -f elf lab9-1.asm
dbatov@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-1 lab9-1.o
dbatov@fedora:~/work/arch-pc/lab09$ ./lab9-1
Введите x: 2
2x+7=11
dbatov@fedora:~/work/arch-pc/lab09$ mcedit lab9-1.asm
dbatov@fedora:~/work/arch-pc/lab09$ nasm -f elf lab9-1.asm
dbatov@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-1 lab9-1.o
dbatov@fedora:~/work/arch-pc/lab09$ ./lab9-1
Введите x: 1
f(g(x))=11
dbatov@fedora:~/work/arch-pc/lab09$
```

В данной части лабораторной работы была написана, скомпилирована и запущена первая программа – с использованием подпрограмм (в нескольких вариантах, согласно заданию). Аналитически легко убедиться, что она выдает правильные ответы.

```

Fedora [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Dec 21 00:27
dbatov@fedora:~/work/arch-pc/lab09 — mcedit lab9-2.asm
lab9-2.asm [----] 8 L: [ 1+20 21/ 21] +(279 / 279b) <EOF>
section .data
msg1 db 'Hello, ',0xa
msgilen 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,msgilen
int 0x80
mov eax,4
mov ebx,1
mov ecx,msg2
mov edx,msg2len
int 0x80
mov eax,1
mov ebx,0
int 0x80

dbatov@fedora:~/work/arch-pc/lab09$ nasm -f elf -g -l lab9-2.lst lab9-2.asm
dbatov@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-2 lab9-2.o
dbatov@fedora:~/work/arch-pc/lab09$ gdb lab9-2

```

В данной части лабораторной работы была написана и скомпилирована программа для работы с gdb.

```

(gdb) run
Starting program: /home/dbatov/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]) n
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.
Hello, world!
[Inferior 1 (process 8791) exited normally]
(gdb) break _start
Breakpoint 1 at 0x8049000: file lab9-2.asm, line 9.
(gdb) run
Starting program: /home/dbatov/work/arch-pc/lab09/lab9-2

Breakpoint 1, _start () at lab9-2.asm:9
9      mov eax,4

```

```
End of assembler dump.
(gdb) set disassembly-flavor intel
(gdb) disassemble _start
Dump of assembler code for function _start:
```

End of assembler dump.

```
native process 8797 In: start
```

[illegible]

```
(gdb) info breakpoints
Num      Type           Disp Enb Address      What
1        breakpoint     keep y   0x08049000 lab9-2.asm:9
          breakpoint already hit 1 time
(gdb) b *0x8049031
Breakpoint 2 at 0x8049031: file lab9-2.asm, line 20.
(gdb) i b
Num      Type           Disp Enb Address      What
1        breakpoint     keep y   0x08049000 lab9-2.asm:9
          breakpoint already hit 1 time
2        breakpoint     keep y   0x08049031 lab9-2.asm:20
```

```
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
--Type <RET> for more, q to quit, c to continue without paging--c
```

```
(gdb) set $ebx='2'
(gdb) p/s $ebx
$1 = 50
(gdb) set $ebx=2
(gdb) p/s $ebx
$2 = 2
```

Разные выводы команды `p/s` связаны с тем, что в одном случае `2` – символ, в другом – число.

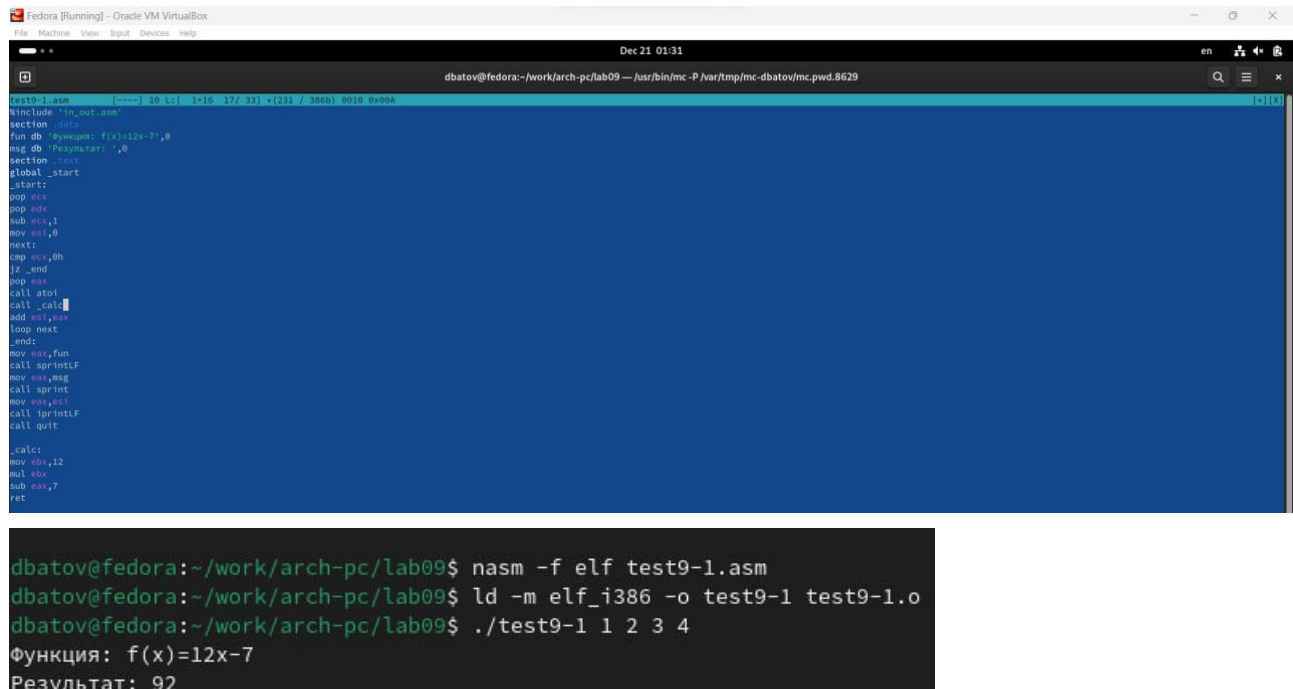
```
dbatov@fedora:~/work/arch-pc/lab09$ cp ~/work/arch-pc/lab08/lab8-2.asm ~/work/arch-pc/lab09/lab9-3.asm
dbatov@fedora:~/work/arch-pc/lab09$ nasm -f elf -g -l lab9-3.lst lab9-3.asm
dbatov@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-3 lab9-3.o
dbatov@fedora:~/work/arch-pc/lab09$ gdb --args lab9-3 аргумент1 аргумент2 'аргумент3'
GNU gdb (Fedora Linux) 14.1-1.fc39
Copyright (C) 2023 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) run
Starting program: /home/dbatov/work/arch-pc/lab09/lab9-3 аргумент1 аргумент2 аргумент3

This GDB supports auto-downloading debuginfo from the following URLs:
  <https://debuginfod.fedoraproject.org/>
Enable debuginfod for this session? (y or [n]) 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
(gdb) x/x $esp
0xffffd080: 0x00000004
(gdb) x/s *(void**) ($esp+4)
0xffffd243: "/home/dbatov/work/arch-pc/lab09/lab9-3"
(gdb) x/s *(void**) ($esp+8)
0xffffd26a: "аргумент1"
(gdb) x/s *(void**) ($esp+12)
0xffffd27c: "аргумент2"
(gdb) x/s *(void**) ($esp+16)
0xffffd28e: "аргумент3"
(gdb) x/s *(void**) ($esp+20)
0x0: <error: Cannot access memory at address 0x0>
```

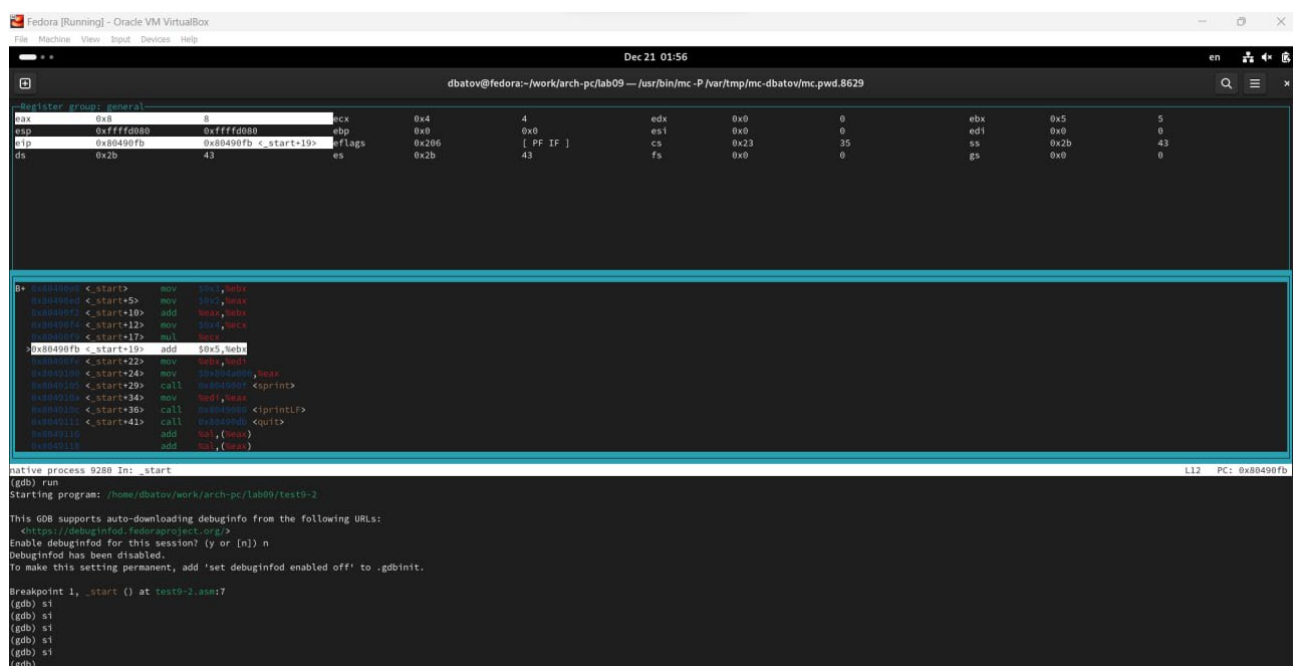
В данной части работы было продолжено изучение брейкпойнтов, также были изучены команды, связанные с регистрами и со вводом аргументов с консоли. Шаг изменения адреса равен 4, поскольку каждый раз идет смещение на 4 байта. Самостоятельная работа:



```
Fedora [Running] - Oracle VM VirtualBox
dbatov@fedora:~/work/arch-pc/lab09 — /usr/bin/mc -P /var/tmp/mc-dbatov/mc.pwd.8629
[1] 16 17 35 * (21 / 366) 0016 0x004
section .data
fun db 'symque: f(x)=12x-7',0
msg db 'Pezymat: '0
section .text
global _start
_start:
pop ecx
pop edx
sub ecx,1
mov esi,0
next:
pop ecx,0h
if_end
pop ecx
call atoi
call _calc
add esi,msg
loop next
_end:
mov ecx,fun
call sprintf
mov ecx,msg
call sprintf
mov ecx,esi
call sprintf
call quit
_calc:
mov ebx,12
mul ebx
sub ecx,7
ret

dbatov@fedora:~/work/arch-pc/lab09$ nasm -f elf test9-1.asm
dbatov@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o test9-1 test9-1.o
dbatov@fedora:~/work/arch-pc/lab09$ ./test9-1 1 2 3 4
Функция: f(x)=12x-7
Результат: 92
```

В первой части самостоятельной работы была преобразована программа из прошлой лабораторной работы с использованием подпрограммы. На тестовом наборе чисел программа показала верный ответ.



```
Fedora [Running] - Oracle VM VirtualBox
dbatov@fedora:~/work/arch-pc/lab09 — /usr/bin/mc -P /var/tmp/mc-dbatov/mc.pwd.8629
Register window:
eax 0 ecx 0x4 4 edx 0x0 0 ebx 0x5 5
esp 0xffffd080 0xffffd080 ebp 0x0 0 esi 0x0 0 edi 0x0 0
eip 0x80490fb 0x80490fb <_start+19> eflags 0x206 [ PF IF ] cs 0x23 35 ss 0x2b 43
ds 0x2b 43 es 0x2b 43 fs 0x0 0 gs 0x0 0

B> 0x80490fb <_start+19> mov 10x,ebx
0x80490fd <_start+21> mov 10x,ecx
0x80490ff <_start+23> add 10x,ebx
0x8049101 <_start+25> mov 10x,ecx
0x8049103 <_start+27> mul 10x
0x8049105 <_start+29> add 10x,ebx
0x8049107 <_start+31> mov 10x,ecx
0x8049109 <_start+33> call 0x804900f <_start+19>
0x804910b <_start+35> call 0x804900f <_start+19>
0x804910d <_start+37> call 0x804900f <_start+19>
0x804910f <_start+39> call 0x804900f <_start+19>
0x8049111 <_start+41> add 10x,ecx
0x8049113 <_start+43> mul 10x,ecx

Native process 9288 In: start
(gdb) run
Starting program: /home/dbatov/work/arch-pc/lab09/test9-2
This GDB supports auto-downloading debuginfo from the following URLs:
<https://debuginfod.fedoraproject.org>
Enable debuginfod for this session? (y or [n]) n
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.
Breakpoint 1, _start () at test9-2.asm:7
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb)
```

На втором этапе самостоятельной работы было изучена программы с ошибкой при помощи отладчика. Ошибка заключалась в том, что команда mul умножает значение в

регистре `eax`, в то время как все остальные действия в программе производились со значением регистра `ebx`.

В результате лабораторной работы мной были приобретены навыки написания программ с использованием подпрограмм; кроме того, я ознакомился с методами отладки при помощи `gdb` и его основными возможностями.