

Отчёт по лабораторной работе №7

Дисциплина: архитектура компьютеров и операционных систем

Шибаета Алесандра Алексеевна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
4.1	Реализация переходов в NASM	8
4.2	Изучение структуры файлы листинга	12
4.3	Задания для самостоятельной работы	14
5	Выводы	20
6	Список литературы	21

Список иллюстраций

4.1	Создание файлов для лабораторной работы	8
4.2	Ввод текста программы из листинга 7.1	9
4.3	Запуск программного кода	9
4.4	Изменение текста программы	10
4.5	Создание исполняемого файла	10
4.6	Изменение текста программы	11
4.7	Вывод программы	11
4.8	Создание файла	11
4.9	Ввод текста программы из листинга 7.3	12
4.10	Проверка работы файла	12
4.11	Создание файла листинга	12
4.12	Изучение файла листинга	13
4.13	Выбранные строки файла	13
4.14	Удаление выделенного операнда из кода	14
4.15	Получение файла листинга	14
4.16	Написание программы	15
4.17	Запуск файла и проверка его работы	15
4.18	Написание программы	17
4.19	Запуск файла и проверка его работы	18

Список таблиц

1 Цель работы

Изучение команд условного и безусловного переходов. Приобретение навыков написания программ с использованием переходов. Знакомство с назначением и структурой файла листинга.

2 Задание

1. Реализация переходов в NASM.
2. Изучение структуры файлы листинга.
3. Задания для самостоятельной работы.

3 Теоретическое введение

Для реализации ветвлений в ассемблере используются так называемые команды передачи управления или команды перехода. Можно выделить 2 типа переходов:

- условный переход – выполнение или не выполнение перехода в определенную точку программы в зависимости от проверки условия.
- безусловный переход – выполнение передачи управления в определенную точку программы без каких-либо условий.

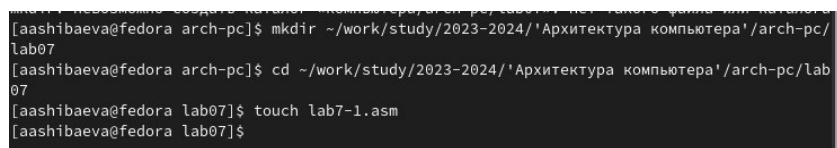
Безусловный переход выполняется инструкцией `jmp`. Инструкция `cmp` является одной из инструкций, которая позволяет сравнить операнды и выставляет флаги в зависимости от результата сравнения. Инструкция `cmp` является командой сравнения двух операндов и имеет такой же формат, как и команда вычитания.

Листинг (в рамках понятийного аппарата NASM) — это один из выходных файлов, создаваемых транслятором. Он имеет текстовый вид и нужен при отладке программы, так как кроме строк самой программы он содержит дополнительную информацию.

4 Выполнение лабораторной работы

4.1 Реализация переходов в NASM

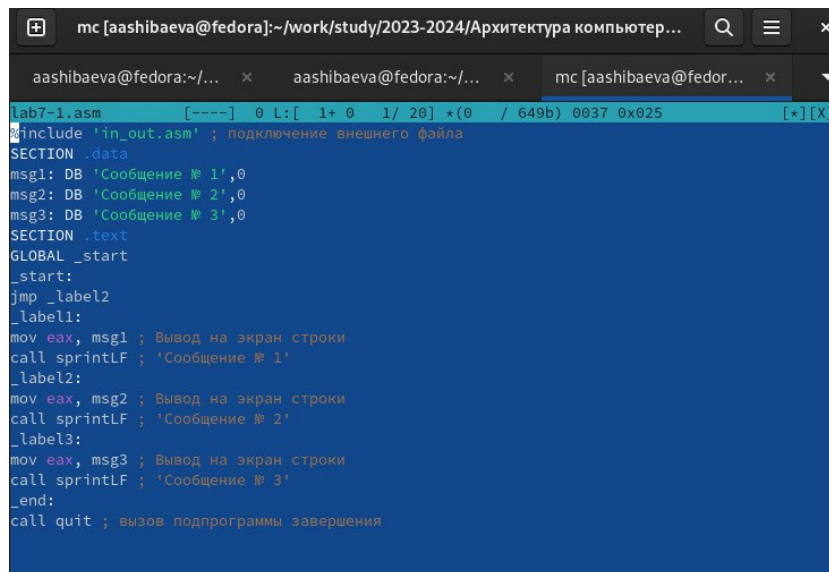
Создаю каталог для программ лабораторной работы № 7, перехожу в него и создаю файл lab7-1.asm. (рис. 4.1).



```
[aashibaeva@fedora arch-pc]$ mkdir ~/work/study/2023-2024/'Архитектура компьютера'/arch-pc/  
lab07  
[aashibaeva@fedora arch-pc]$ cd ~/work/study/2023-2024/'Архитектура компьютера'/arch-pc/lab  
07  
[aashibaeva@fedora lab07]$ touch lab7-1.asm  
[aashibaeva@fedora lab07]$
```

Рис. 4.1: Создание файлов для лабораторной работы

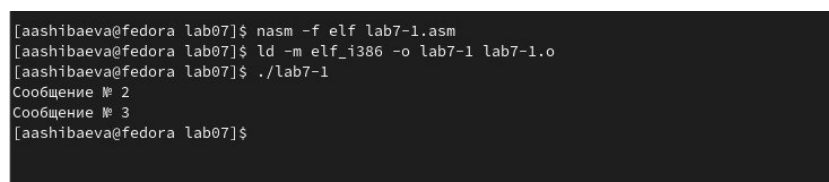
Ввожу в файл lab7-1.asm текст программы из листинга 7.1. (рис. 4.2).



```
lab7-1.asm [---] 0 L:[ 1+ 0 1/ 20] *(0 / 649b) 0037 0x025 [*][X]
#include 'in_out.asm' ; подключение внешнего файла
SECTION .data
msg1: DB 'Сообщение № 1',0
msg2: DB 'Сообщение № 2',0
msg3: DB 'Сообщение № 3',0
SECTION .text
GLOBAL _start
_start:
jmp _label2
_label1:
mov eax, msg1 ; Вывод на экран строки
call sprintf ; 'Сообщение № 1'
_label2:
mov eax, msg2 ; Вывод на экран строки
call sprintf ; 'Сообщение № 2'
_label3:
mov eax, msg3 ; Вывод на экран строки
call sprintf ; 'Сообщение № 3'
_end:
call quit ; вызов подпрограммы завершения
```

Рис. 4.2: Ввод текста программы из листинга 7.1

Создаю исполняемый файл и запускаю его. (рис. 4.3).

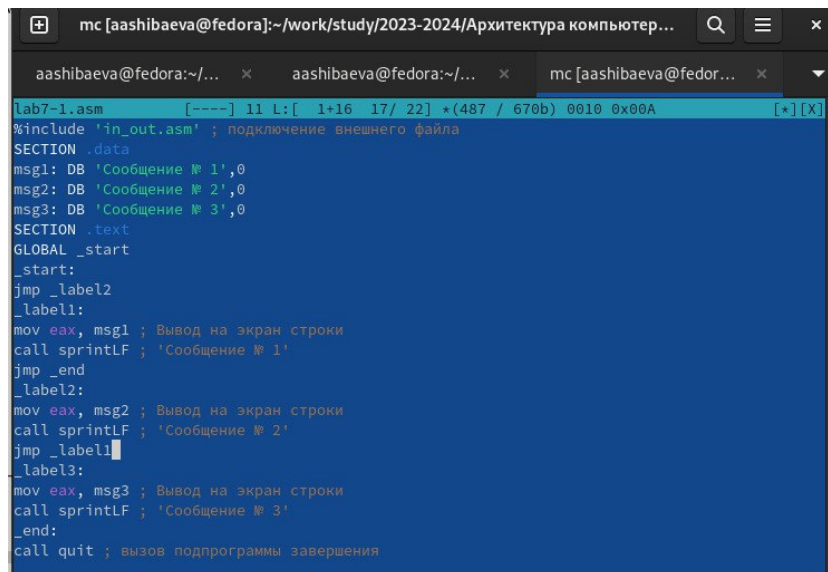


```
[aashibaeva@fedora lab07]$ nasm -f elf lab7-1.asm
[aashibaeva@fedora lab07]$ ld -m elf_i386 -o lab7-1 lab7-1.o
[aashibaeva@fedora lab07]$ ./lab7-1
Сообщение № 2
Сообщение № 3
[aashibaeva@fedora lab07]$
```

Рис. 4.3: Запуск программного кода

Таким образом, использование инструкции `jmp _label2` меняет порядок исполнения инструкций и позволяет выполнить инструкции начиная с метки `_label2`, пропустив вывод первого сообщения.

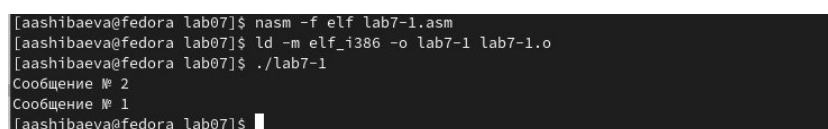
Изменяю программу таким образом, чтобы она выводила сначала 'Сообщение № 2', потом 'Сообщение № 1' и завершала работу. Для этого изменяю текст программы в соответствии с листингом 7.2. (рис. 4.4).



```
lab7-1.asm [---] 11 L: [ 1+16 17/ 22] *(487 / 670b) 0010 0x00A [X] [X]
%include 'in_out.asm' ; подключение внешнего файла
SECTION .data
msg1: DB 'Сообщение № 1',0
msg2: DB 'Сообщение № 2',0
msg3: DB 'Сообщение № 3',0
SECTION .text
GLOBAL _start
_start:
jmp _label2
_label1:
mov eax, msg1 ; Вывод на экран строки
call sprintf ; 'Сообщение № 1'
jmp _end
_label2:
mov eax, msg2 ; Вывод на экран строки
call sprintf ; 'Сообщение № 2'
jmp _label1
_label3:
mov eax, msg3 ; Вывод на экран строки
call sprintf ; 'Сообщение № 3'
_end:
call quit ; вызов подпрограммы завершения
```

Рис. 4.4: Изменение текста программы

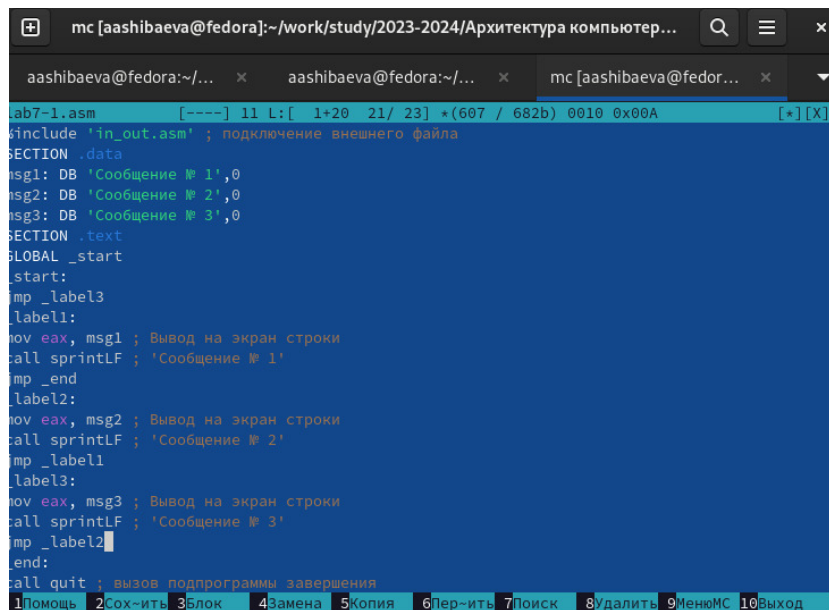
Создаю исполняемый файл и проверяю его работу. (рис. 4.5).



```
[aashibaeva@fedora lab07]$ nasm -f elf lab7-1.asm
[aashibaeva@fedora lab07]$ ld -m elf_i386 -o lab7-1 lab7-1.o
[aashibaeva@fedora lab07]$ ./lab7-1
Сообщение № 2
Сообщение № 1
[aashibaeva@fedora lab07]$
```

Рис. 4.5: Создание исполняемого файла

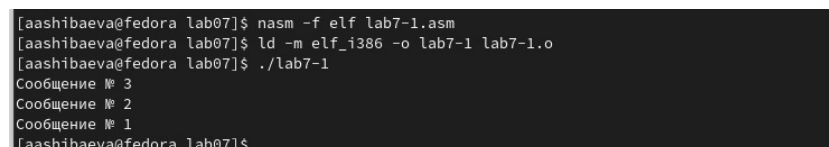
Затем изменяю текст программы, добавив в начале программы `jmp _label3`, `jmp _label2` в конце метки `jmp _label3`, `jmp _label1` добавляю в конце метки `jmp _label2`, и добавляю `jmp _end` в конце метки `jmp _label1`, (рис. 4.6).



```
lab7-1.asm [----] 11 L: [ 1+20 21/ 23] *(607 / 682b) 0010 0x00A [*][X]
#include 'in_out.asm' ; подключение внешнего файла
SECTION .data
msg1: DB 'Сообщение № 1',0
msg2: DB 'Сообщение № 2',0
msg3: DB 'Сообщение № 3',0
SECTION .text
GLOBAL _start
_start:
jmp _label3
_label1:
mov eax, msg1 ; Вывод на экран строки
call sprintf ; 'Сообщение № 1'
jmp _end
_label2:
mov eax, msg2 ; Вывод на экран строки
call sprintf ; 'Сообщение № 2'
jmp _label1
_label3:
mov eax, msg3 ; Вывод на экран строки
call sprintf ; 'Сообщение № 3'
jmp _label2
_end:
call quit ; вызов подпрограммы завершения
1Помощь 2Скопировать 3Блок 4Замена 5Копия 6Перейти 7Поиск 8Удалить 9МенюМС 10Выход
```

Рис. 4.6: Изменение текста программы

Вывод программы был следующим: (рис. 4.7).



```
[aashibaeva@fedora lab07]$ nasm -f elf lab7-1.asm
[aashibaeva@fedora lab07]$ ld -m elf_i386 -o lab7-1 lab7-1.o
[aashibaeva@fedora lab07]$ ./lab7-1
Сообщение № 3
Сообщение № 2
Сообщение № 1
[aashibaeva@fedora lab07]$
```

Рис. 4.7: Вывод программы

Рассмотрим программу, которая определяет и выводит на экран наибольшую из 3 целочисленных переменных: А,В и С. Значения для А и С задаются в программе, значение В вводится с клавиатуры.

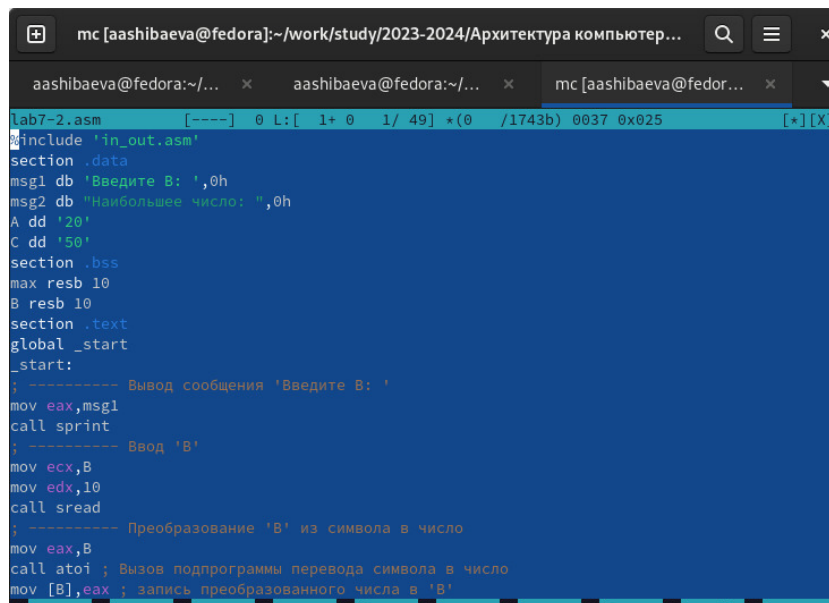
Создаю файл lab7-2.asm в каталоге ~/work/arch-pc/lab07. (рис. 4.8).



```
[aashibaeva@fedora lab07]$ touch lab7-2.asm
```

Рис. 4.8: Создание файла

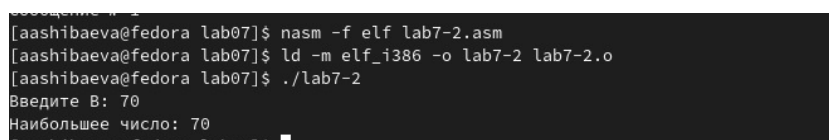
Текст программы из листинга 7.3 ввожу в lab7-2.asm. (рис. 4.9).



```
lab7-2.asm [---] 0 L:[ 1+ 0 1/ 49] *(0 /1743b) 0037 0x025 [*][X]
#include 'in_out.asm'
section .data
msg1 db 'Введите B: ',0h
msg2 db "Наибольшее число: ",0h
A dd '20'
C dd '50'
section .bss
max resb 10
B resb 10
section .text
global _start
_start:
; ----- Вывод сообщения 'Введите B: '
mov eax,msg1
call sprint
; ----- Ввод 'B'
mov ecx,B
mov edx,10
call sread
; ----- Преобразование 'B' из символа в число
mov eax,B
call atoi ; Вызов подпрограммы перевода символа в число
mov [B],eax ; запись преобразованного числа в 'B'
```

Рис. 4.9: Ввод текста программы из листинга 7.3

Создаю исполняемый файл и проверьте его работу. (рис. 4.10).



```
[aashibaeva@fedora lab07]$ nasm -f elf lab7-2.asm
[aashibaeva@fedora lab07]$ ld -m elf_i386 -o lab7-2 lab7-2.o
[aashibaeva@fedora lab07]$ ./lab7-2
Введите B: 70
Наибольшее число: 70
```

Рис. 4.10: Проверка работы файла

Файл работает корректно.

4.2 Изучение структуры файлы листинга

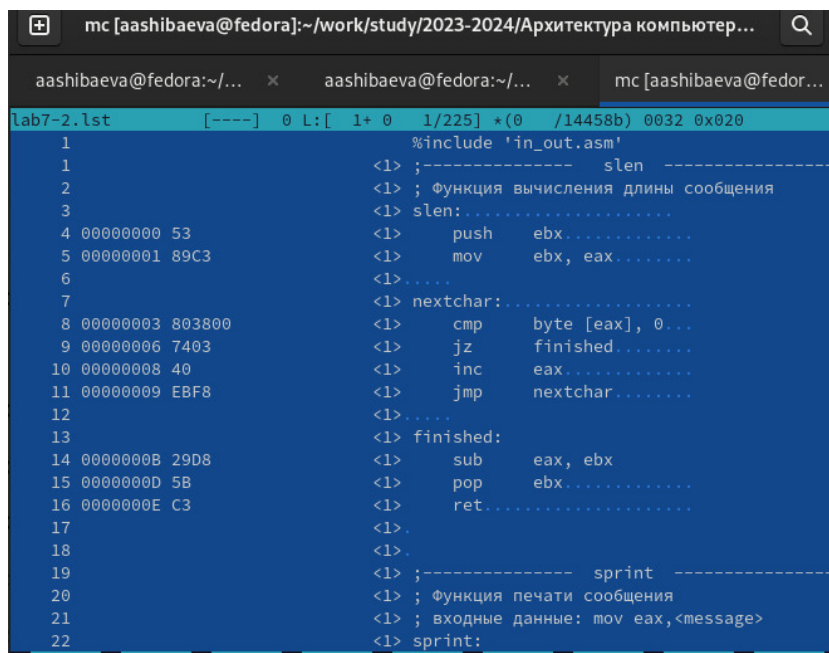
Создаю файл листинга для программы из файла lab7-2.asm. (рис. 4.11).



```
[aashibaeva@fedora lab07]$ nasm -f elf -l lab7-2.lst lab7-2.asm
```

Рис. 4.11: Создание файла листинга

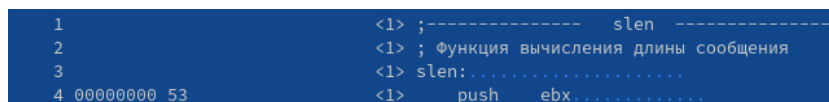
Открываю файл листинга lab7-2.lst с помощью текстового редактора и внимательно изучаю его формат и содержимое. (рис. 4.12).



```
lab7-2.lst  [----]  0 L: [ 1+ 0 1/225] *(0 /14458b) 0032 0x020
1          %include 'in_out.asm'
1          <1> ;----- slen -----
2          <1> ; Функция вычисления длины сообщения
3          <1> slen:.....
4 00000000 53          <1> push    ebx.....
5 00000001 89C3        <1> mov     ebx, eax.....
6
7          <1> .....
8 00000003 803800      <1> cmp     byte [eax], 0...
9 00000006 7403        <1> jz      finished.....
10 00000008 40         <1> inc     eax.....
11 00000009 EBF8       <1> jmp     nextchar.....
12          <1> .....
13          <1> finished:
14 0000000B 29D8       <1> sub     eax, ebx
15 0000000D 5B         <1> pop     ebx.....
16 0000000E C3         <1> ret.....
17          <1> .
18          <1> .
19          <1> ;----- sprint -----
20          <1> ; Функция печати сообщения
21          <1> ; входные данные: mov eax,<message>
22          <1> sprint:
```

Рис. 4.12: Изучение файла листинга

В представленных трех строчках содержатся следующие данные: (рис. 4.13).



```
1          <1> ;----- slen -----
2          <1> ; Функция вычисления длины сообщения
3          <1> slen:.....
4 00000000 53          <1> push    ebx.....
```

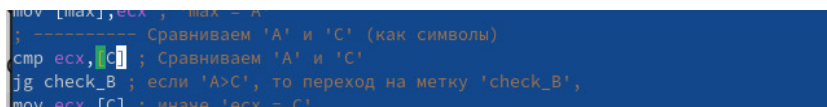
Рис. 4.13: Выбранные строки файла

“2” - номер строки кода, “; Функция вычисления длинны сообщения” - комментарий к коду, не имеет адреса и машинного кода.

“3” - номер строки кода, “slen” - название функции, не имеет адреса и машинного кода.

“4” - номер строки кода, “00000000” - адрес строки, “53” - машинный код, “push ebx” - исходный текст программы, инструкция “push” помещает операнд “ebx” в стек.

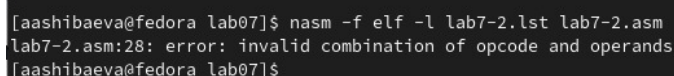
Открываю файл с программой lab7-2.asm и в выбранной мной инструкции с двумя операндами удаляю выделенный операнд. (рис. 4.14).



```
mov [max],ecx ; max = A
; ----- Сравниваем 'A' и 'C' (как символы)
cmp ecx,[C] ; Сравниваем 'A' и 'C'
jg check_B ; если 'A>C', то переход на метку 'check_B',
mov ecx,[C] ; иначе 'ecx = C'
```

Рис. 4.14: Удаление выделенного операнда из кода

Выполняю трансляцию с получением файла листинга. (рис. 4.15).



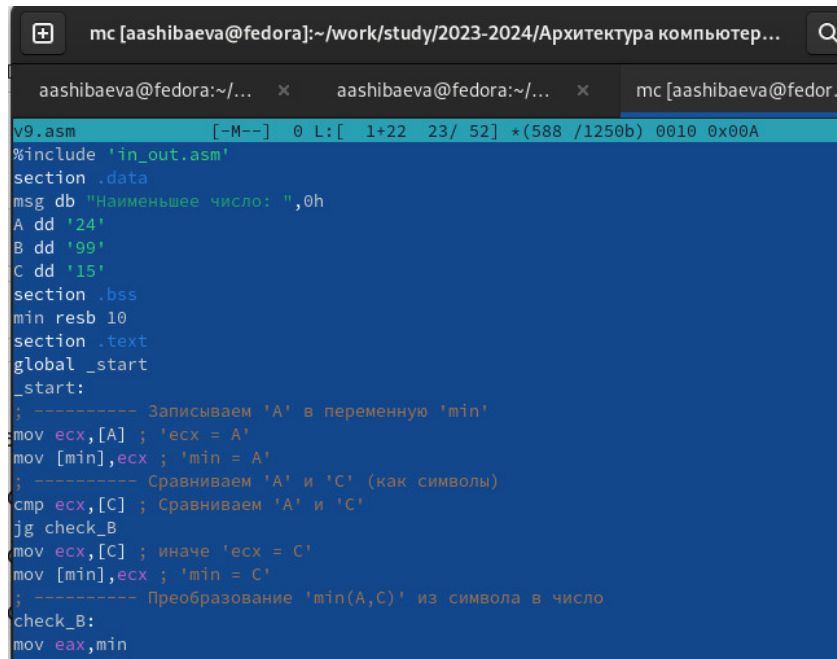
```
[aashibaeva@fedora lab07]$ nasm -f elf -l lab7-2.lst lab7-2.asm
lab7-2.asm:28: error: invalid combination of opcode and operands
[aashibaeva@fedora lab07]$
```

Рис. 4.15: Получение файла листинга

На выходе я не получаю ни одного файла из-за ошибки:инструкция mov (единственная в коде содержит два операнда) не может работать, имея только один операнд, из-за чего нарушается работа кода.

4.3 Задания для самостоятельной работы

1. Пишу программу нахождения наименьшей из 3 целочисленных переменных a, b и c. Значения переменных выбираю из табл. 7.5 в соответствии с вариантом, полученным при выполнении лабораторной работы № 7. Мой вариант под номером 9, поэтому мои значения - 24, 99 и 15. (рис. 4.16).



```
v9.asm [-M--] 0 L: [ 1+22 23/ 52] *(588 /1250b) 0010 0x00A
#include 'in_out.asm'
section .data
msg db "Наименьшее число: ",0h
A dd '24'
B dd '99'
C dd '15'
section .bss
min resb 10
section .text
global _start
_start:
; ----- Записываем 'A' в переменную 'min'
mov ecx,[A] ; 'ecx = A'
mov [min],ecx ; 'min = A'
; ----- Сравниваем 'A' и 'C' (как символы)
cmp ecx,[C] ; Сравниваем 'A' и 'C'
jg check_B
mov ecx,[C] ; иначе 'ecx = C'
mov [min],ecx ; 'min = C'
; ----- Преобразование 'min(A,C)' из символа в число
check_B:
mov eax,min
```

Рис. 4.16: Написание программы

Создаю исполняемый файл и проверяю его работу, подставляя необходимые значение. (рис. 4.17).



```
[aashibaeva@fedora lab07]$ nasm -f elf v9.asm
[aashibaeva@fedora lab07]$ ld -m elf_i386 -o v9 v9.o
[aashibaeva@fedora lab07]$ ./v9
Наименьшее число: 15
[aashibaeva@fedora lab07]$
```

Рис. 4.17: Запуск файла и проверка его работы

Программа работает корректно.

Код программы:

```
%include 'in_out.asm'
section .data
msg db "Наименьшее число:",0h
A dd '24'
B dd '99'
C dd '15'
```

```

section .bss
min resb 10
section .text
global _start
_start:
; ——— Записываем 'A' в переменную 'min'
mov ecx,[A] ; 'ecx = A'
mov [min],ecx ; 'min = A'
; ——— Сравниваем 'A' и 'C' (как символы)
cmp ecx,[C] ; Сравниваем 'A' и 'C'
jg check_B
mov ecx,[C] ; иначе 'ecx = C'
mov [min],ecx ; 'min = C'
; ——— Преобразование 'min(A,C)' из символа в число
check_B:
mov eax,min
call atoi ; Вызов подпрограммы перевода символа в число
mov [min],eax ; запись преобразованного числа в min
; ——— Сравниваем 'min(A,C)' и 'B' (как числа)
mov ecx,[min]
cmp ecx,[B] ; Сравниваем 'min(A,C)' и 'B'
jl fin ; если 'min(A,C)<B', то переход на 'fin',
mov ecx,[B] ; иначе 'ecx = B'
mov [min],ecx
; ——— Вывод результата
fin:
mov eax,msg
call sprint ; Вывод сообщения 'Наименьшее число:'
mov eax,[min]

```


call iprintLF ; Вывод 'min(A,B,C)'

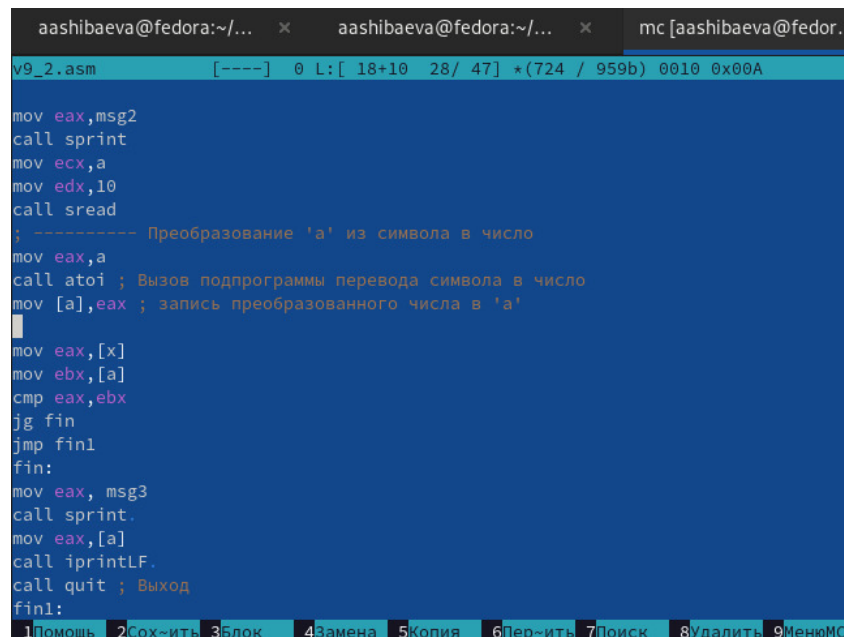
call quit ; Выход

2. Пишу программу, которая для введенных с клавиатуры значений x и a вычисляет значение и выводит результат вычислений заданной для моего варианта функции $f(x)$:

$a + x$, если $x \leq a$

a , если $x > a$

(рис. 4.18).



```
y9_2.asm      [----]  0 L: [ 18+10  28/ 47] *(724 / 959b) 0010 0x00A

mov  eax,msg2
call sprint
mov  ecx,a
mov  edx,10
call sread
; ----- Преобразование 'a' из символа в число
mov  eax,a
call atoi ; Вызов подпрограммы перевода символа в число
mov  [a],eax ; запись преобразованного числа в 'a'
mov  eax,[x]
mov  ebx,[a]
cmp  eax,ebx
jg   fin
jmp  fin1
fin:
mov  eax, msg3
call sprint.
mov  eax,[a]
call iprintLF.
call quit ; Выход
fin1:
```

Рис. 4.18: Написание программы

Создаю исполняемый файл и проверяю его работу для значений x и a соответственно: (5;7), (6;4). (рис. 4.19).

```

^C[aashibaeva@fedora lab07]$ nasm -f elf v9_2.asm
[aashibaeva@fedora lab07]$ ld -m elf_i386 -o v9_2 v9_2.o
[aashibaeva@fedora lab07]$ ./v9_2
Введите x:5
Введите a:7
Ответ:12
[aashibaeva@fedora lab07]$ ./v9_2
Введите x:6
Введите a:4
Ответ:4
[aashibaeva@fedora lab07]$

```

Рис. 4.19: Запуск файла и проверка его работы

Программа работает корректно.

Код программы:

```

%include 'in_out.asm'

section .data
msg1 db "Введите x:",0h
msg2 db "Введите a:",0h
msg3 db "Ответ:",0h

section .bss
x resb 10
a resb 10

section .text
global _start
_start:
mov eax,msg1
call sprint
mov ecx,x
mov edx,10
call sread
mov eax,x
call atoi ; Вызов подпрограммы перевода символа в число
mov [x],eax ; запись преобразованного числа в 'x'
mov eax,msg2

```

```

call sprint
mov ecx,a
mov edx,10
call sread
; ——— Преобразование 'а' из символа в число
mov eax,a
call atoi ; Вызов подпрограммы перевода символа в число
mov [a],eax ; запись преобразованного числа в 'а'
mov eax,[x]
mov ebx,[a]
cmp eax,ebx
jg fin
jmp fin1
fin:
mov eax, msg3
call sprint
mov eax,[a]
call iprintLF
call quit ; Выход
fin1:
mov eax,msg3
call sprint
mov eax,[x]
mov ecx,[a]
add eax,ecx
call iprintLF
call quit ; Выход

```

5 Выводы

По итогам данной лабораторной работы я изучила команды условного и безусловного переходов, приобрела навыки написания программ с использованием переходов и ознакомилась с назначением и структурой файла листинга, что поможет мне при выполнении последующих лабораторных работ.

6 Список литературы

1. GDB: The GNU Project Debugger. — URL: <https://www.gnu.org/software/gdb/>.
2. GNU Bash Manual. — 2016. — URL: <https://www.gnu.org/software/bash/manual/>.
3. Midnight Commander Development Center. — 2021. — URL: <https://midnight-commander.org/>.
4. NASM Assembly Language Tutorials. — 2021. — URL: <https://asmtutor.com/>.
5. Newham C. Learning the bash Shell: Unix Shell Programming. — O'Reilly Media, 2005. — 354 с. — (In a Nutshell). — ISBN 0596009658. — URL: <http://www.amazon.com/Learningbash-Shell-Programming-Nutshell/dp/0596009658>.
6. Robbins A. Bash Pocket Reference. — O'Reilly Media, 2016. — 156 с. — ISBN 978-1491941591.
7. The NASM documentation. — 2021. — URL: <https://www.nasm.us/docs.php>.
8. Zarrelli G. Mastering Bash. — Packt Publishing, 2017. — 502 с. — ISBN 9781784396879.
9. Колдаев В. Д., Лупин С. А. Архитектура ЭВМ. — М. : Форум, 2018.
10. Куляс О. Л., Никитин К. А. Курс программирования на ASSEMBLER. — М. : Солон-Пресс, 2017.
11. Новожилов О. П. Архитектура ЭВМ и систем. — М. : Юрайт, 2016.
12. Расширенный ассемблер: NASM. — 2021. — URL: <https://www.opennet.ru/docs/RUS/nasm/>.
13. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — БХВПетербург, 2010. — 656 с. — ISBN 978-5-94157-538-1.
14. Столяров А. Программирование на языке ассемблера NASM для ОС Unix. — 2-е изд. — М. : МАКС Пресс, 2011. — URL: http://www.stolyarov.info/books/asm_unix.

15. Таненбаум Э. Архитектура компьютера. — 6-е изд. — СПб. : Питер, 2013. — 874 с. — (Классика Computer Science).
16. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — 1120 с. — (Классика Computer Science).