Лабораторная работа №7

Команды безусловного и условного переходов в Nasm. Программирование ветвлений.

Чекмарев Александр Дмитриевич | группа: НПИбд 02-23

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы 2.1 Реализация переходов в NASM	6 6 13
3	Самостоятельная работа	18
4	Выводы	24

Список иллюстраций

Рис 2.1.1: Создание каталога и файла .asm	6
Рис 2.1.2: Демонстрация текста программы в файле	7
Рис 2.1.3: Создание файла и его проверка	8
Рис 2.1.4: Демонстрация текста программы в файле	9
Рис 2.1.5: Создание файла и его проверка	10
Рис 2.1.6: Демонстрация измененного текста в файле	10
	11
Рис 2.1.8: Создание файла .asm	11
Рис 2.1.9: Демонстрация текста программы в файле	12
ями В	13
	14
	14
Рис 2.2.3: Вид файла .lst в текст. редакторе	15
	15
	16
Рис 2.2.6: Трансляция файла	16
Рис 2.2.7: Демонстрация ошибки в файле .lst	16
Рис 3.1.1. Создание файда	18
	19
	20
	20
	20
	21
	22
	$\frac{-2}{22}$
Рис 3.3.1: Загрузка файлов на github	23
	Рис 2.1.2: Демонстрация текста программы в файле Рис 2.1.3: Создание файла и его проверка Рис 2.1.4: Демонстрация текста программы в файле Рис 2.1.5: Создание файла и его проверка Рис 2.1.6: Демонстрация измененного текста в файле Рис 2.1.7: Проверка работы программы Рис 2.1.8: Создание файла .asm Рис 2.1.9: Демонстрация текста программы в файле Рис 2.1.10: Создание файла и проверка работы с разными значениями В Рис 2.2.1: Создание файла Рис 2.2.2: Демонстрация ввода команды Рис 2.2.3: Вид файла .lst в текст. редакторе Рис 2.2.4: Демонстрация взятых строк Рис 2.2.5: Удаление операнды Рис 2.2.6: Трансляция файла Рис 2.2.7: Демонстрация ошибки в файле .lst Рис 3.1.1: Создание файла Рис 3.1.2: Демонстрация программы Рис 3.2.1: Демонстрация 4-го вариана Рис 3.2.2: Демонстрация 4-го вариана Рис 3.2.3: (1)Программа для задачи Рис 3.2.4: (2)Программа для задачи Рис 3.2.5: Проверка программы

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 Выполнение лабораторной работы

2.1 Реализация переходов в NASM

Создадим каталог для программам лабораторной работы N^{o} 7, перейдите в него и создадим файл lab7-1.asm:

```
adchekmarev@alexanderchekmarev:~$ mkdir ~/work/arch-pc/lab07
adchekmarev@alexanderchekmarev:~$ cd ~/work/arch-pc/lab07
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ touch lab7-1.asm
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$
```

Рис. 2.1: Рис 2.1.1: Создание каталога и файла .asm

Инструкция *jmp* в NASM используется для реализации безусловных переходов. Рассмотрим пример программы с использованием инструкции *jmp*. Введем в файл *lab7-1.asm* текст программы из листинга 7.1

```
1 %include 'in_out.asm' ; подключение внешнего файла
 2
    SECTION .data
 3
 4
 5
    msq1: DB 'Сообщение № 1',0
    msg2: DB 'Сообщение № 2',0
 6
    msg3: DB 'Сообщение № 3',0
 7
 8
    SECTION .text
 9
    GLOBAL start
10
11
     start:
12
13
     jmp label2
14
     label1:
15
16
       mov eax, msg1 ; Вывод на экран строки
       call sprintLF ; 'Сообщение № 1'
17
18
     label2:
19
20
       mov eax, msg2 ; Вывод на экран строки
       call sprintLF ; 'Сообщение № 2'
21
22
     _label3:
23
24
       mov eax, msg3 ; Вывод на экран строки
25
       call sprintLF ; 'Сообщение № 3'
26
     _end:
27
      call quit ; вызов подпрограммы завершения
28
```

Рис. 2.2: Рис 2.1.2: Демонстрация текста программы в файле

Создим исполняемый файл и запустим его. Результат работы данной программы будет следующим:

```
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ nasm -f elf lab7-1.asm adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ld -m elf_i386 -o lab7-1 lab7-1.o adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./lab7-1 Сообщение № 2 Сообщение № 3 adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$
```

Рис. 2.3: Рис 2.1.3: Создание файла и его проверка

Таким образом, использование инструкции *jmp_label2* меняет порядок исполнения инструкций и позволяет выполнить инструкции начиная с метки *_label2*, пропустив вывод первого сообщения.

Инструкция jmp позволяет осуществлять переходы не только вперед но и назад. Изменим программу таким образом, чтобы она выводила сначала 'Сообщение N° 2', потом 'Сообщение N° 1' и завершала работу. Для этого в текст программы после вывода сообщения N° 2 добавим инструкцию jmp с меткой *_label1* (т.е. переход к инструкциям вывода сообщения N° 1) и после вывода сообщения N° 1 добавим инструкцию jmp с меткой *_end* (т.е. переход к инструкции $call\ quit$). Измените текст программы в соответствии с листингом 7.2

```
1 %include 'in out.asm' ; подключение внешнего файла
2
3
    SECTION .data
4
5
   msg1: DB 'Сообщение № 1',0
   msg2: DB 'Сообщение № 2',0
б
7
   msg3: DB 'Сообщение № 3',0
8
   SECTION .text
9
  GLOBAL _start
.0
1
     start:
12
13
    jmp label2
4
     label1:
.5
.6
       mov eax, msg1 ; Вывод на экран строки
       call sprintLF ; 'Сообщение № 1'
.7
18
       jmp end
9
     _label2:
20
21
       mov eax, msg2 ; Вывод на экран строки
       call sprintLF ; 'Сообщение № 2'
22
       jmp _label1
23
24
2.5
     _label3:
26
       mov eax, msg3 ; Вывод на экран строки
27
       call sprintLF ; 'Сообщение № 3'
28
     _end:
29
30
      call quit ; вызов подпрограммы завершения
```

Рис. 2.4: Рис 2.1.4: Демонстрация текста программы в файле

Создадим исполняемый файл и проверим его работу.

```
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ nasm -f elf lab7-1.asm
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ld -m elf_i386 -o lab7-1 lab7-1.o
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./lab7-1
Сообщение № 2
Сообщение № 1
```

Рис. 2.5: Рис 2.1.5: Создание файла и его проверка

Изменим текст программы добавив или изменив инструкции *jmp*.

```
%include 'in out.asm' ; подключение внешнего файла
  SECTION .data
  msq1: DB 'Сообщение № 1',0
  msq2: 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 sprintLF ; 'Сообщение № 1'
     jmp end
   label2:
     mov eax, msg2 ; Вывод на экран строки
     call sprintLF ; 'Сообщение № 2'
     jmp _label1
   label3:
     mov eax, msg3 ; Вывод на экран строки
     call sprintLF ; 'Сообщение № 3'
     jmp _label2
  _end:
     call quit ; вызов подпрограммы завершения
```

Рис. 2.6: Рис 2.1.6: Демонстрация измененного текста в файле

Проверим работу

```
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ nasm -f elf lab7-1.asm
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ld -m elf_i386 -o lab7-1 lab7-1.o
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./lab7-1
Сообщение № 3
Сообщение № 2
Сообщение № 1
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$
```

Рис. 2.7: Рис 2.1.7: Проверка работы программы

Использование инструкции *jmp* приводит к переходу в любом случае. Однако, часто при написании программ необходимо использовать условные переходы, т.е. переход должен происходить если выполнено какое-либо условие. В качестве примера 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 вводиться с клавиатуры

Создадим файл *lab7-2.asm* в каталоге ~/work/arch-pc/lab07.

```
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ touch lab7-2.asm
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$
```

Рис. 2.8: Рис 2.1.8: Создание файла .asm

Внимательно изучим текст программы из листинга 7.3 и введем в *lab7-2.asm*.

```
%include 'in out.asm'
section .data
   msq1 db 'Введите В: ',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 В: '
   mov eax,msg1
  call sprint
 ----- Ввод 'В'
  mov ecx,B
  mov edx,10
  call sread
 ----- Преобразование 'В' из символа в число
  mov eax,B
  call atoi ; Вызов подпрограммы перевода символа в число
  mov [B],eax ; запись преобразованного числа в 'В'
 ----- Записываем 'А' в переменную 'тах'
  mov ecx,[A]; 'ecx = A'
  mov [max], ecx ; 'max = A'
 ----- Сравниваем 'А' и 'С' (как символы)
  стр есх,[С]; Сравниваем 'А' и 'С'
  jg check_B; если 'A>C', то переход на метку 'check_B',
   mov ecx,[C]; иначе 'ecx = C'
   mov [max],ecx; 'max = C'
; ------ Преобразование 'max(A,C)' из символа в число
check B:
   mov eax, max
   call atoi ; Вызов подпрограммы перевода символа в число
   mov [max],eax ; запись преобразованного числа в `max`
 ----- Cравниваем 'max(A,C)' и 'B' (как числа)
 mov ecx,[max]
   cmp ecx,[B] ; Сравниваем 'max(A,C)' и 'B'
   jg fin ; если 'max(A,C)>B', то переход на 'fin',
   mov ecx,[B]; иначе 'ecx = B'
   mov [max],ecx
 ----- Вывод результата
fin:
   mov eax, msg2
   call sprint ; Вывод сообщения 'Наибольшее число: '
   mov eax,[max]
   call iprintLF ; Вывод 'max(A,B,C)'
   call quit ; Выход
```

Рис. 2.9: Рис 2.1.9: Демонстрация текста программы в файле

Создадим исполняемый файл и проверим его работу для разных значений В.

```
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ touch lab7-2.asm
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ nasm -f elf lab7-2.asm
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ld -m elf_i386 -o lab7-2 lab7-2.o
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./lab7-2
Введите В: 42
Наибольшее число: 50
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./lab7-2
Введите В: 199
Наибольшее число: 199
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./lab7-2
Введите В: 14
Наибольшее число: 50
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./lab7-2
Введите В: -34
Наибольшее число: 50
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./lab7-2
Введите В: -51
Наибольшее число: 50
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$
```

Рис. 2.10: Рис 2.1.10: Создание файла и проверка работы с разными значениями В

Обратим внимание, в данном примере переменные А и С сравниваются как символы, а переменная В и максимум из А и С как числа (для этого используется функция *atoi* преобразования символа в число). Это сделано для демонстрации того, как сравниваются данные. Данную программу можно упростить и сравнивать все 3 переменные как символы (т.е. не использовать функцию *atoi*). Однако если переменные преобразовать из символов числа, над ними можно корректно проводить арифметические операции.

2.2 Изучение структуры файлы листинга

Обычно nasm создаёт в результате ассемблирования только объектный файл. Получить файл листинга можно, указав ключ -l и задав имя файла листинга в командной строке. Создадим файл листинга для программы из файла lab7-2.asm

Рис. 2.11: Рис 2.2.1: Создание файла

Откроем файл листинга lab7-2.lst с помощью любого текстового редактора, например mcedit:

adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07\$ mcedit lab7-2.lst

Рис. 2.12: Рис 2.2.2: Демонстрация ввода команды

```
/home/adchekmarev/work/arch-pc/lab07/lab7-2.lst
                                                   [----] 0 L:[ 1+ 0 1/225] *(0 /14560b) 0032
                                        %include 'in out.asm
                                   <1> ; Функция вычисления длины сообщения
                                   <1> slen:.
    5 00000000 53
    6 00000001 89C3
    9 00000003 803800
                                                   byte [eax], 0.
   10 00000006 7403
                                                    finished.....
   11 00000008 40
   12 00000009 EBF8
                                                   nextchar
                                   <1> finished:
   15 0000000B 29D8
   16 0000000D 5B
   17 0000000E C3
                                   <1>; Функция печати сообщения <1>; входные данные: mov eax,<message>
   23
   24 0000000F 52
   25 00000010 51
   26 00000011 53
                                           push
                                                    ebx
   27 00000012 50
                                           push
                                                    eax
   28 00000013 E8E8FFFFF
                                                    slen
   30 00000018 89C2
   31 0000001A 58
   33 0000001B 89C1
   34 0000001D BB01000000
   35 00000022 B804000000
   36 00000027 CD80
                                                    80h
   38 00000029 5B
                                           pop
   39 0000002A 59
                                            рор
   40 0000002B 5A
                                            DOD
   41 0000002C C3
   44
                                                           sprintLF
                                    <1> ; Функция печати сообщения с переводом строки
                                    <1> ; входные данные: mov eax,<message>
```

Рис. 2.13: Рис 2.2.3: Вид файла .lst в текст. редакторе

Внимательно ознакомимся с его форматом и содержимым. Подробно объяснить содержимое трёх строк файла листинга по выбору.

Возьмем первые 3 строки файла листинга, начиная с 3-ьей*

Рис. 2.14: Рис 2.2.4: Демонстрация взятых строк

- 3 номер строки кода, "; Функция вычисления длинны сообщения" оно не имеет отношения к работе кода, это пояснение.
- 4 номер строки кода, "slen:....." название функции, не имеет адреса и машинного кода.
- 5 номер строки кода, "00000000" адрес строки, "53" машинный код, "push ebx" исходный текст программы, инструкция "push" помещает операнд "ebx" в стек.

Откроем файл с программой *lab7-2.asm* и в любой инструкции с двумя операндами удалим один операнд. Выполним трансляцию с получением файла листинга:

```
mov [max],ecx; 'max = A'
7; ------ Сравниваем 'A' и 'C' (как символы)

cmp ecx,[C]; Сравниваем 'A' и 'C'

g jg check_B; если 'A>C', то переход на метку 'check_B',

mov ecx,[C]; иначе 'ecx = C'

mov [max],ecx; 'max = C'

; ------ Преобразование 'max(A,C)' из символа в число
```

Рис. 2.15: Рис 2.2.5: Удаление операнды

Какие выходные файлы создаются в этом случае? Что добавляется в листинге?

Выполним трансляцию с измененной программой

```
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ nasm -f elf -l lab7-2.lst lab7-2.asm
lab7-2.asm:28: error: invalid combination of opcode and operands
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$
```

Рис. 2.16: Рис 2.2.6: Трансляция файла

Рис. 2.17: Рис 2.2.7: Демонстрация ошибки в файле .lst

На выходе мы не получаем файла из-за ошибки. **mov** не может работать, имея только один операнд, из-за чего нарушается работа кода

3 Самостоятельная работа

Задание№ 1 Напишите программу нахождения наименьшей из 3 целочисленных переменных а,b и с. Значения переменных выбрать из табл. 7.5 в соответствии с вариантом, полученным при выполнении лабораторной работы № 7. Создайте исполняемый файл и проверьте его работу.

Создадим новый файл *task1.asm* и напишем программу нахождения наименьшей из 3 целочисленных переменных a,b и с для варианта 4 (8,88,68).

adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07\$ touch task1.asm

Рис. 3.1: Рис 3.1.1: Создание файла

Возьмем за основу код из lab7-2.asm и переделаем его

```
1 %include 'in out.asm'
 2 section .data
     msg db "Наименьшее число: ",0h
     A dd '8'
4
     B dd '88'
     C dd '68'
 6
 7 section .bss
    min resb 0
9 section .text
     global _start
10
11 _start:
12 mov ecx,[A]; 'ecx = A'
13  mov [min],ecx; 'min = A'
14
15
     стр есх,[С]; Сравниваем 'А' и 'С'
16
     jl check B
17
     mov ecx,[C]; иначе 'ecx = C'
18
     mov [min],ecx; 'min = C'
19
20 check B:
21 mov eax,min
22
    call atoi ; Вызов подпрограммы перевода символа в число
23 mov [min],eax ; запись преобразованного числа в `min`
24
25
   mov ecx,[min]
26 cmp ecx,[B] ; Сравниваем 'min(A,C)' и 'В'
27
    jl fin ; если 'min(A,C)<B', то переход на 'fin',
     mov ecx,[B]; иначе 'ecx = B'
28
29
     mov [min],ecx
30
31 fin:
32
     mov eax, msg
     call sprint ; Вывод сообщения 'Наименьшее число: '
     mov eax,[min]
     call iprintLF ; Вывод 'min(A,B,C)'
36 call quit ; Выход
```

Рис. 3.2: Рис 3.1.2: Демонстрация программы для задания

Проверим программу

```
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ nasm -f elf task1.asm adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ld -m elf_i386 -o task1 task1.o adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./task1 Наименьшее число: 8
```

Рис. 3.3: Рис 3.1.3: Проверка программы

Программа работает как нужно для задания.

Задание \mathbb{N}^2 2 Напишите программу, которая для введенных с клавиатуры значений x и а вычисляет значение заданной функции f(x) и выводит результат вычислений. Вид функции f(x) выбрать из таблицы 7.6 вариантов заданий в соответствии с вариантом, полученным при выполнении лабораторной работы \mathbb{N}^2 7. Создайте исполняемый файл и проверьте его работу для значений x и а из 7.6

Создадим файл task2.asm для 2-го задания

adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07\$ touch task2.asm

Рис. 3.4: Рис 3.2.1: Демонстрация 4-го вариана

Напишем код к решению 4-го варианта

4
$$\begin{cases} 2x + a, & a \neq 0 \\ 2x + 1, & a = 0 \end{cases}$$
 (3;0)

Рис. 3.5: Рис 3.2.2: Демонстрация 4-го вариана

```
1 %include 'in_out.asm'
 2 section .data
4 msg1 DB 'Введите х: ',0h
 5 msg2 DB "Введите a: ",0h
 6 otv: DB 'F(x)=',0h
8 section .bss
9 x: RESB 10
10 a: RESB 10
11 res: RESB 10
12
13 section .text
14 global _start
15 _start:
16
17 mov eax, msg1
18 call sprint
19 mov ecx, x
20 mov edx,10
21 call sread
22 mov eax,x
23 call atoi
24 mov [x],eax
25
26 mov eax, msg2
27 call sprint
28 mov ecx,a
29 mov edx,10
30 call sread
31 mov eax,a
32 call atoi
33 mov [a],eax
34
35 mov ecx, [a]
36 cmp ecx, 0
37 je x is 0
38 mov eax, [x]
39 mov ebx,2
40 mul ebx
41 add eax, ecx
42 jmp calc_res
43 x_is_0:
44 mov ebx,2
45 mov eax, [x]
46 mul ebx
47 inc eax
48 calc_res:
49 mov [res],eax
50 fin:
51 mov eax, otv
52 call sprint
```

Рис. 3.6: Рис 3.2.3: (1)Программа для задачи

```
53 mov eax,[res]
54 call iprintLF
55 call quit
```

Рис. 3.7: Рис 3.2.4: (2)Программа для задачи

Проверим работу программы

```
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ nasm -f elf task2.asm
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ld -m elf_i386 -o task2 task2.o
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./task2
Введите х: 3
Введите а: 0
F(x)=7
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$ ./task2
Введите х: 3
Введите х: 3
Введите а: 2
F(x)=8
adchekmarev@alexanderchekmarev:~/work/arch-pc/lab07$
```

Рис. 3.8: Рис 3.2.5: Проверка программы

Как видно по (рис 3.2.5) программа работает корректно и я выполнил задание Загрузим все файлы на github по окончании лаб. работы

```
Adchekmarev@alexanderchekmarev: /work/study/2023-2024/Apxmertypa κομπωστερα/arch-pc/labsS git add .

adchekmarev@alexanderchekmarev: /work/study/2023-2024/Apxmertypa κομπωστερα/arch-pc/labsS git commit -am 'feat(main): add files lab-7'

22 files changed, 208 insertions(+), 119 deletions(-)

22 files changed, 208 insertions(+), 119 deletions(-)

23 files changed, 208 insertions(+), 119 deletions(-)

24 files changed, 208 insertions(+), 119 deletions(-)

25 files changed, 208 insertions(+), 119 deletions(-)

26 files changed, 208 insertions(+), 119 deletions(-)

27 files changed, 208 insertions(+), 119 deletions(-)

28 files changed, 208 insertions(+), 119 deletions(-)

29 files changed, 208 insertions(+), 119 deletions(-)

20 files changed, 208 insertions(+), 119 deletions(-)

21 files changed, 208 insertions(+), 119 deletions(-)

22 files changed, 208 insertions(+), 119 deletions(-)

23 files changed, 208 insertions(+), 119 deletions(-)

24 files changed, 208 insertions(+), 119 deletions(-)

25 files changed, 208 insertions(+), 119 deletions(-)

26 files changed, 208 insertions(+), 119 deletions(-)

27 files changed, 208 insertions(+), 119 deletions(-)

28 files changed, 208 insertions(+), 119 deletions(-)

29 files changed, 208 insertions(+), 119 deletions(-)

20 files changed, 208 insertions(+), 119 deletions(-)

20 files changed, 208 insertions(+), 119 deletions(-)

20 files changed, 208 insertions(+), 119 deletions(-), 119 deletions(-),
```

Рис. 3.9: Рис 3.3.1: Загрузка файлов на github

4 Выводы

Я изучил команды условного и безусловного переходов. Приобрел навыки написания программ с использованием переходов. Познакомился с назначением и структурой файла листинга.