

Отчет по лабораторной работе №4

Архитектура компьютеров

Незами Ахмад Белал нкабд 05- 24

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.0.1	1	6
2.0.2	2	6
2.0.3	3	6
2.0.4	4	7
2.0.5	5	8
2.0.6	6	8
2.0.7	7	8
2.0.8	8	8
2.0.9	9	9
3	Самостоятельная работа	10
3.0.1	1	10
3.0.2	2	10
3.0.3	3	11
3.0.4	4	11
4	Ответы на вопросы	13
5	Выводы	16

Список иллюстраций

2.1	Создание каталога с помощью команд <code>mkdir -p ~/work/arch-pc/lab04</code>	6
2.2	Переход в созданный каталог с помощью команд <code>cd ~/work/arch-pc/lab04</code>	6
2.3	Создание текстового файла с помощью команд <code>touch hello.asm</code>	7
2.4	Открытие текстового редактора <code>gedit</code> с помощью команды <code>gedit hello.asm</code>	7
2.5	И ввожу в него следующий текст.	7
2.6	Ввожу команду <code>nasm -f elf hello.asm</code>	8
2.7	Расширенный синтаксис командной строки NASM.	8
2.8	Компоновщик LD.	8
2.9	Ввожу команду <code>ld -m elf_i386 obj.o -o main</code>	9
2.10	Ввожу команду <code>./hello</code>	9
3.1	Создаю копию файла <code>hello.asm</code> с именем <code>lab04.asm</code>	10
3.2	Ввожу свое имя фамилию.	10
3.3	Запускаю получившийся исполняемый файл.	11
3.4	Копирую файлы <code>hello.asm</code> и <code>lab4.asm</code> с помощью команды <code>cp hello.asm lab04.asm ~/work/study/2024-2025/“Архитектура компьютера”/arch-pc/labs/lab04/</code>	11
3.5	Проверяю.	11
3.6	Загружаю файлы на Github.	12

Список таблиц

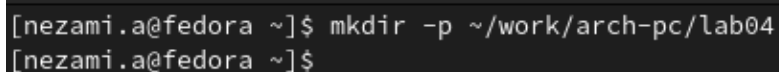
1 Цель работы

Освоение процедуры компиляции и сборки программ, написанных на ассемблере NASM.

2 Выполнение лабораторной работы

2.0.1 1

Создаю каталог для работы с программами на языке ассемблера NASM.



```
[nezami.a@fedora ~]$ mkdir -p ~/work/arch-pc/lab04  
[nezami.a@fedora ~]$
```

Рис. 2.1: Создание каталога с помощью команд `mkdir -p ~/work/arch-pc/lab04`

2.0.2 2

Перехожу в созданный каталог.



```
[nezami.a@fedora ~]$ cd ~/work/arch-pc/lab04  
[nezami.a@fedora lab04]$
```

Рис. 2.2: Переход в созданный каталог с помощью команд `cd ~/work/arch-pc/lab04`

2.0.3 3

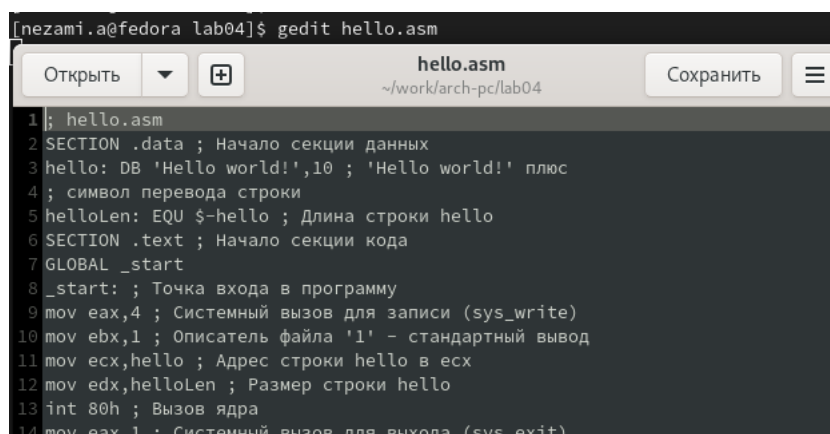
Создаю текстовый файл с именем `hello.asm`

```
[nezami.a@fedora lab04]$ touch hello.asm
[nezami.a@fedora lab04]$
```

Рис. 2.3: Создание текстового файла с помощью команд touch hello.asm

2.0.4 4

Открываю этот файл с помощью текстового редактора gedit.

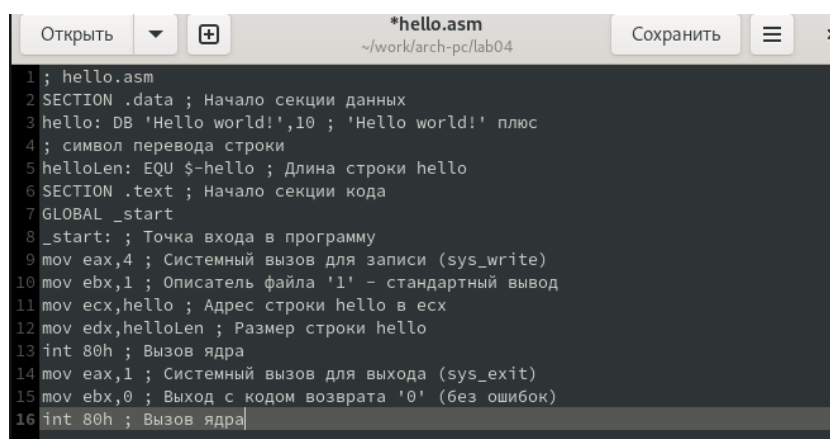


```
[nezami.a@fedora lab04]$ gedit hello.asm
```

hello.asm
~/work/arch-pc/lab04

```
1; hello.asm
2SECTION .data ; Начало секции данных
3hello: DB 'Hello world!',10 ; 'Hello world!' плюс
4; символ перевода строки
5helloLen: EQU $-hello ; Длина строки hello
6SECTION .text ; Начало секции кода
7GLOBAL _start
8_start: ; Точка входа в программу
9mov eax,4 ; Системный вызов для записи (sys_write)
10mov ebx,1 ; Описатель файла '1' - стандартный вывод
11mov ecx,hello ; Адрес строки hello в ecx
12mov edx,helloLen ; Размер строки hello
13int 80h ; Вызов ядра
14mov eax,1 ; Системный вызов для выхода (sys_exit)
```

Рис. 2.4: Открытие текстового редактора gedit с помощью команды gedit hello.asm



*hello.asm
~/work/arch-pc/lab04

```
1; hello.asm
2SECTION .data ; Начало секции данных
3hello: DB 'Hello world!',10 ; 'Hello world!' плюс
4; символ перевода строки
5helloLen: EQU $-hello ; Длина строки hello
6SECTION .text ; Начало секции кода
7GLOBAL _start
8_start: ; Точка входа в программу
9mov eax,4 ; Системный вызов для записи (sys_write)
10mov ebx,1 ; Описатель файла '1' - стандартный вывод
11mov ecx,hello ; Адрес строки hello в ecx
12mov edx,helloLen ; Размер строки hello
13int 80h ; Вызов ядра
14mov eax,1 ; Системный вызов для выхода (sys_exit)
15mov ebx,0 ; Выход с кодом возврата '0' (без ошибок)
16int 80h ; Вызов ядра
```

Рис. 2.5: И ввожу в него следующий текст.

2.0.5 5

NASM превращает текст программы в объектный код.

```
[nezami.a@fedora lab04]$ nasm -f elf hello.asm  
[nezami.a@fedora lab04]$
```

Рис. 2.6: Ввожу команду `nasm -f elf hello.asm`

2.0.6 6

Полный вариант командной строки `nasm` выглядит следующим образом:

```
[nezami.a@fedora lab04]$ nasm -o obj.o -f elf -g -l list.lst hello.asm  
[nezami.a@fedora lab04]$
```

Рис. 2.7: Расширенный синтаксис командной строки NASM.

2.0.7 7

Чтобы получить исполняемую программу, объектный файл необходимо передать на обработку компоновщику:

```
[nezami.a@fedora lab04]$ ld -m elf_i386 hello.o -o hello  
[nezami.a@fedora lab04]$
```

Рис. 2.8: Компоновщик LD.

2.0.8 8

Ключ `-o` с последующим значением задаёт в данном случае имя создаваемого исполняемого файла.


```
[nezami.a@fedora lab04]$ ld -m elf_i386 obj.o -o main  
[nezami.a@fedora lab04]$
```

Рис. 2.9: Ввожу команду `ld -m elf_i386 obj.o -o main`

2.0.9 9

Запуск исполняемого файла.

```
[nezami.a@fedora lab04]$ ./hello  
Hello world!  
[nezami.a@fedora lab04]$
```

Рис. 2.10: Ввожу команду `./hello`

3 Самостоятельная работа

3.0.1 1

В каталоге ~/work/arch-pc/lab04 с помощью команды cp

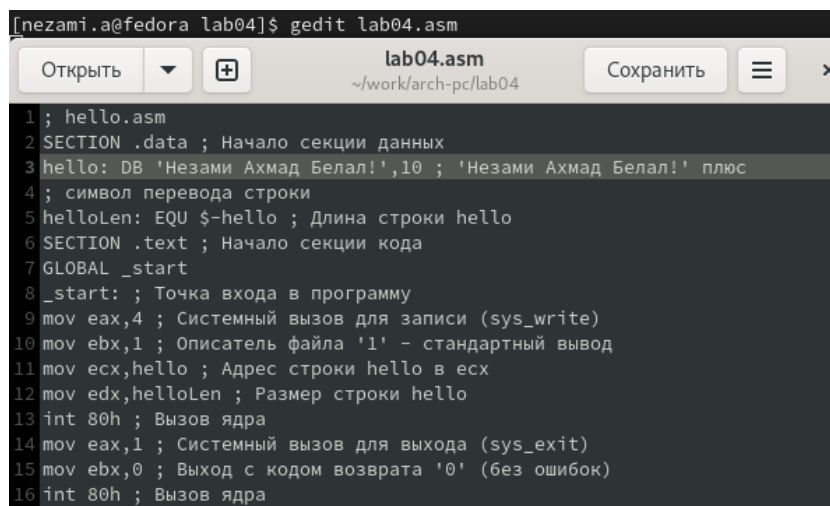
```
[nezami.a@fedora lab04]$ cp hello.asm lab04.asm
```

Рис. 3.1: Создаю копию файла hello.asm с именем lab04.asm

3.0.2 2

С помощью текстового редактора gedit ввожу изменения в тексте программы в файле lab04.asm вместо Hello world! ввожу Незами Ахмад Белал.

```
[nezami.a@fedora lab04]$ gedit lab04.asm
```



```
1 ; hello.asm
2 SECTION .data ; Начало секции данных
3 hello: DB 'Незами Ахмад Белал!',10 ; 'Незами Ахмад Белал!' плюс
4 ; символ перевода строки
5 helloLen: EQU $-hello ; Длина строки hello
6 SECTION .text ; Начало секции кода
7 GLOBAL _start
8 _start: ; Точка входа в программу
9 mov eax,4 ; Системный вызов для записи (sys_write)
10 mov ebx,1 ; Описатель файла '1' - стандартный вывод
11 mov ecx,hello ; Адрес строки hello в ecx
12 mov edx,helloLen ; Размер строки hello
13 int 80h ; Вызов ядра
14 mov eax,1 ; Системный вызов для выхода (sys_exit)
15 mov ebx,0 ; Выход с кодом возврата '0' (без ошибок)
16 int 80h ; Вызов ядра
```

Рис. 3.2: Ввожу свое имя фамилию.

3.0.3 3

Оттранслирую полученный текст программы lab04.asm в объектный файл. Выполняю компоновку объектного файла.

```
[nezami.a@fedora lab04]$ nasm -f elf lab04.asm
[nezami.a@fedora lab04]$ nasm -o obj.o -f elf -g -l list.lst lab04.asm
[nezami.a@fedora lab04]$ ld -m elf_i386 lab04.o -o lab04
[nezami.a@fedora lab04]$ ld -m elf_i386 obj.o -o main
[nezami.a@fedora lab04]$ ./lab04
Незами Ахмад Белал!
[nezami.a@fedora lab04]$
```

Рис. 3.3: Запускаю получившийся исполняемый файл.

3.0.4 4

Копирую файлы hello.asm и lab04.asm в локальный репозиторий в каталог ~/work/study/2024-2025/“Архитектура компьютера”/arch-pc/labs/lab04/.

```
[nezami.a@fedora lab04]$ cp hello.asm lab04.asm ~/work/study/2024-2025/"Архитектура
компьютера"/arch-pc/labs/lab04/
[nezami.a@fedora lab04]$
```

Рис. 3.4: Копирую файлы hello.asm и lab4.asm с помощью команды cp hello.asm lab04.asm ~/work/study/2024-2025/“Архитектура компьютера”/arch-pc/labs/lab04/

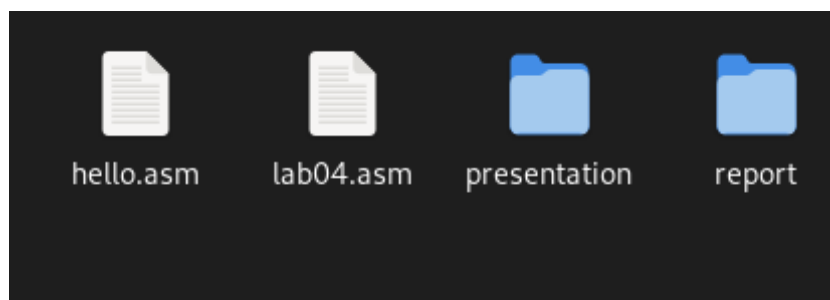


Рис. 3.5: Проверяю.

```

[nezami.a@fedora arch-pc]$ git add .
[nezami.a@fedora arch-pc]$ git commit -am 'feat(main): add files lab-4'
[main e5d8439] feat(main): add files lab-4
61 files changed, 4666 insertions(+), 1 deletion(-)
create mode 100644 labs/lab02/report/image (2).rar
create mode 100644 labs/lab02/report/image (2)/image/1.png
create mode 100644 labs/lab02/report/image (2)/image/10.png
create mode 100644 labs/lab02/report/image (2)/image/11.png
create mode 100644 labs/lab02/report/image (2)/image/12.png
create mode 100644 labs/lab02/report/image (2)/image/13.png
create mode 100644 labs/lab02/report/image (2)/image/14.png
create mode 100644 labs/lab02/report/image (2)/image/15.png
create mode 100644 labs/lab02/report/image (2)/image/16.png
create mode 100644 labs/lab02/report/image (2)/image/2.png
create mode 100644 labs/lab02/report/image (2)/image/3.png
create mode 100644 labs/lab02/report/image (2)/image/4.png
create mode 100644 labs/lab02/report/image (2)/image/5.png
create mode 100644 labs/lab02/report/image (2)/image/6.png
create mode 100644 labs/lab02/report/image (2)/image/7.png
create mode 100644 labs/lab02/report/image (2)/image/8.png
create mode 100644 labs/lab02/report/image (2)/image/9.png
delete mode 100644 "labs/lab02/report/\320\23302_\320\220\321\205\320\274\320\26
320\264.docx"
create mode 100644 "labs/lab02/report/\320\233\321\20002 \320\220\321\205\320\27
320\260\320\264.docx"
create mode 100644 "labs/lab02/report/\320\233\321\20002 \320\220\321\205\320\27
320\260\320\264.pdf"
create mode 100644 labs/lab04/presentation/Makefile
create mode 100644 labs/lab04/presentation/image/kulyabov.jpg
create mode 100644 labs/lab04/presentation/presentation.md
create mode 100644 labs/lab04/report/Makefile

```

Рис. 3.6: Загружаю файлы на Github.

4 Ответы на вопросы

1. Основное отличие ассемблера от языков высокого уровня — Байт-код или байткод (англ. byte-code), иногда также используется термин псевдокод — машинно-независимый код низкого уровня, генерируемый транслятором и исполняемый интерпретатором. Большинство инструкций байт-кода эквивалентны одной или нескольким командам ассемблера. Трансляция в байт-код занимает промежуточное положение между компиляцией в машинный код и интерпретацией.
2. Инструкция ассемблера генерирует машинный код, таким образом, способствует размеру программы. Директива ассемблера не создает какого-либо машинного кода, таким образом, не способствует размеру программы. IT приказывает ассемблеру выполнять определенные действия на этапе сборки.
3. Правила написания программ на языке assembler Исходный текст программы на языке ассемблера имеет определенный формат. Каждая команда и директива представляет собой строку: Метка, операция, операнд(ы), комментарии.
4. Создание исполняемого файла издавна производилось в три этапа: (1) обработка исходного кода препроцессором, (2) компиляция в объектный код и (3) компоновка объектных модулей, включая модули из объектных библиотек, в исполняемый файл. Это классическая схема для компилируемых языков.

5. На этапе трансляции осуществляется перевод команд ассемблера в соответствующие машинные команды. В результате трансляции формируются файл объектного модуля и файл листинга.
6. Если в процессе ассемблирования не было выявлено ошибок в ассемблерном листинге, то программа-ассемблер создаст объектный файл (с расширением OBJ).

Затем необходимо воспользоваться компоновщиком (линковщиком), который входит в комплект программы-ассемблера. Данная процедура выполняется гораздо быстрее ассемблирования.

Именно компоновщик создает готовый к запуску файл (программу) с расширением COM или EXE из объектного файла (OBJ). Оба типа имеют отличия в структуре ассемблерной программы. Первый тип (COM) не может превышать 64 Кбайт и используется только в MS-DOS (и для совместимости поддерживается в Windows), однако он очень компактный и удобный для написания небольших программ и резидентов. В большинстве случаев, если программа написана на чистом ассемблере под MS-DOS, нет необходимости создавать EXE-файлы. В этой книге в части I рассматриваются именно программы типа COM.

В отличие от создания программ типа COM, при создании стандартных EXE-программ под MS-DOS нет необходимости указывать какие-либо параметры линковщику при компоновке. Дело в том, что компоновщик не может автоматически определить, какой тип подвергается компоновке.

Линковщик также проверяет, нет ли каких-либо ошибок в объектном файле, но не грамматических, а логических. Например, отсутствие необходимой объектной библиотеки, указанной в самом файле либо в командной строке (программа-ассемблер этого не делает).

Если ошибки не были обнаружены, компоновщик создает машинный код (программу типа COM или EXE), которую можно запускать на выполнение.

7. Для того чтобы выполнить пробный прогон ассемблерной программы, ее

необходимо сначала оттранслировать и скомпоновать. Пусть текст исходной программы хранится в файле с именем SIMPLE.ASM. Трансляцию можно осуществить вызовом турбо ассемблера TASM.EXE с помощью, например, следующей команды DOS:

```
tasm /l/z/zi/n simple.asm
```

8. NASM поддерживает множество форматов выходных файлов, среди них:

bin — файл произвольного формата, определяемого только исходным кодом. Пригоден как для файлов данных, так и для модулей с исполняемыми кодами — например, системных загрузчиков, образов ПЗУ, модулей операционных систем, драйверов .SYS в MS-DOS или исполняемых файлов .COM. obj — объектный модуль в формате OMF, совместимый с MASM и TASM. win32 и win64 — объектный модуль для 32- и 64-битного кода, совместимый с Win32- и Win64-компиляторами Microsoft. aout — объектный модуль в варианте формата a.out, использовавшегося в ранних Linux-системах. aoutb — версия формата a.out для BSD-совместимых операционных систем. coff — объектный модуль в формате COFF, совместимом с компоновщиком из DJGPP. elf32 и elf64 — объектный модуль в форматах ELF32 и ELF64, используемых в Linux и Unix System V, включая Solaris x86, UnixWare и SCO Unix. Формат выходного файла можно задать с помощью ключа командной строки -f. Форматы могут расширять синтаксис некоторых инструкций и добавлять собственные инструкции.

5 Выводы

В ходе выполнения этой лабораторной работы я освоил процедуру компиляции и сборки программ, написанных на ассемблере NASM.