Лабораторная работа №14. Основы программирования на языках Си и ассемблера в UNIX-like ОС

Макаров П. А.

1 Краткая теория

1. GNU Compiler Collection — Википедия.
2. GCC, the GNU Compiler Collection.
3. GNU Assembler — Википедия.
4. GNU linker — Википедия.
5. ld — GNU linker.
6. How Initialization Functions Are Handled.

2 Задания для самостоятельного решения

1. Напишите в текстовом редакторе `vim` файл `hello.c` с исходным текстом программы на языке Си, приведённым в Листинге 1:

Листинг 1: Содержимое файла `hello.c`

```
#include <stdio.h>

int main() {
    printf("Hello, world!\n");
    return 0;
}
```

2. Исследуйте результат работы транслятора `gcc` с помощью следующих команд:

```
$ gcc hello.c -o hello1
$ ./hello1
$ time ./hello1
$ file hello.c
$ file hello1
$ hexdump -C hello.c
$ hexdump -C hello1 | less
$ objdump -D hello1 | less
```

При выполнении последних двух команд, кроме всего прочего, обратите внимание на содержимое файла `hello1` в диапазонах адресов от `0x1149` до `0x1166` и от `0x2000` до `0x200F`.

3. Исследуйте результат работы компилятора `gcc` с помощью следующих команд:

```
$ gcc -S hello.c -o hello.s
$ ls -l
$ file hello.s
$ cat hello.s
```

Прочитайте справочную литературу о синтаксисе ассемблера AT&T. Попытайтесь понять содержимое файла `hello.s`. Подумайте и ответьте на следующие вопросы. Что такое компилятор и транслятор? Какие функции они выполняют? Какой термин более универсальный, а какой более специальный?

4. С помощью следующих команд изучите работу стандартного ассемблера `as`, используемого транслятором `gcc`:

```
$ gcc -c hello.c -o hello.o
$ ls -l
$ file hello.o
$ hexdump -C hello.o | less
$ objdump -d hello.o | less
```

5. Разберитесь, является ли ассемблирование окончательным этапом в процессе трансляции? Для этого выполните следующие команды:

```
$ gcc hello.o -o hello2
$ ls -l
$ cmp hello1 hello2
```

```
$ as hello.s -o hello.3
$ ls -l
$ file hello.3
$ cmp hello.3 hello.o
$ gcc -### hello.3 -o hello3
$ find /usr/ -name crt*
$ ld -o hello3 -dynamic-linker /lib64/ld-linux-x86-64.
  so.2 /usr/lib/x86_64-linux-gnu/Scrt1.o /usr/lib/
  x86_64-linux-gnu/crti.o /usr/lib/gcc/x86_64-linux-
  gnu/11/crtbeginS.o hello.3 -lc /usr/lib/gcc/x86_64-
  linux-gnu/11/crtendS.o /usr/lib/x86_64-linux-gnu/
  crtn.o
$ ls -l
$ ./hello3
$ file hello1
$ file hello3
$ cmp hello1 hello3
$ ldd hello1
$ ldd hello3
```

Подумайте и ответьте на следующие вопросы. Что именно делает ассемблер? Какова функция компоновщика (линкера)? Насколько удобно пользоваться инструментами `as` и `ld` по отдельности? Являются ли файлы `hello1` и `hello3` абсолютно идентичными и почему?