Отчёта по лабораторной работе 10

Понятие подпрограммы. Отладчик GDB.

Эллина Майзингер НММбд-02-22

Содержание

# 1 Цель работы

Целью работы является приобретение навыков написания программ с использованием подпрограмм. Знакомство с методами отладки при помощи GDB и его основными возможностями.

# 2 Задание

1. Изучите примеры реализации подпрограмм
2. Изучите работу с отладчиком GDB
3. Выполните самостоятеьное задание
4. Загрузите файлы на GitHub.

# 3 Выполнение лабораторной работы

1. Создадим каталог для выполнения лабораторной работы № 10, перейдем в него и создадим файл lab10-1.asm:
2. В качестве примера рассмотрим программу вычисления арифметического выражения f(x) = 2x+7 с помощью подпрограммы calcul. В данном примере x вводится с клавиатуры, а само выражение вычисляется в подпрограмме. (рис. 1, 2)

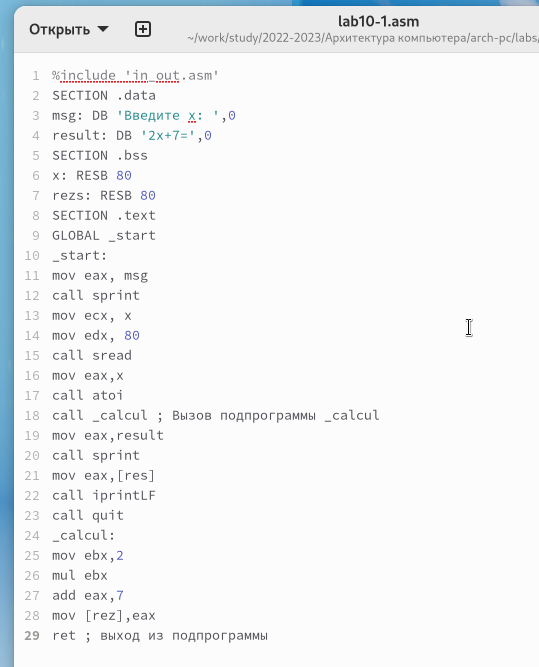


Рис. 1: Файл lab10-1.asm

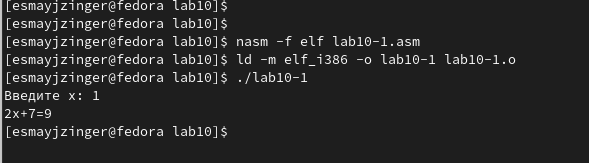


Рис. 2: Работа программы lab10-1.asm

1. Изменим текст программы, добавив подпрограмму subcalcul в подпрограмму calcul, для вычисления выражения f(g(x)), где x вводится с клавиатуры, f(x) = 2x + 7, g(x) = 3x − 1(рис. 3, 4)

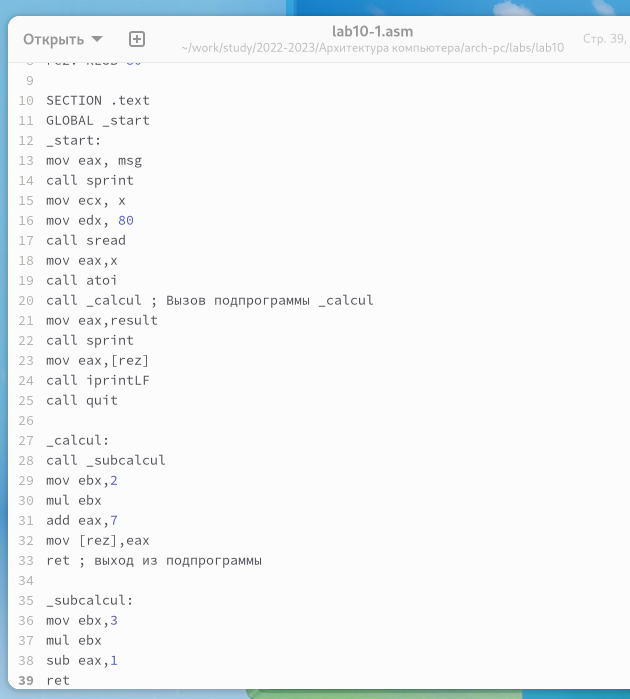


Рис. 3: Файл lab10-1.asm

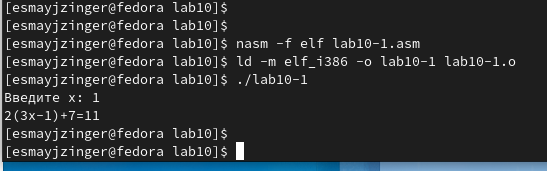


Рис. 4: Работа программы lab10-1.asm

1. Создадим файл lab10-2.asm с текстом программы из Листинга 10.2. (Программа печати сообщения Hello world!): (рис. 5)

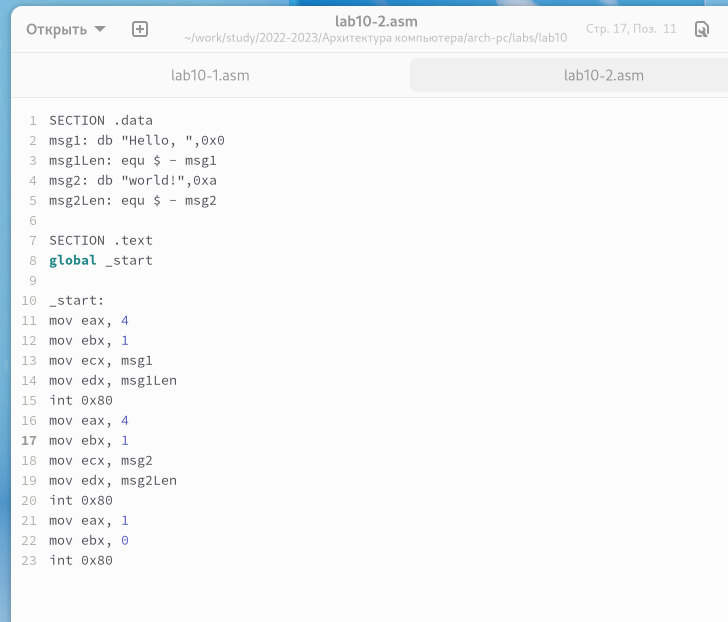


Рис. 5: Файл lab10-2.asm

Получим исполняемый файл. Для работы с GDB в исполняемый файл необходимо добавить отладочную информацию, для этого трансляцию программ необходимо проводить с ключом ‘-g’. Затем загрузим исполняемый файл в отладчик gdb: Проверим работу программы, запустив ее в оболочке GDB с помощью команды run (сокращённо r):(рис. 6)

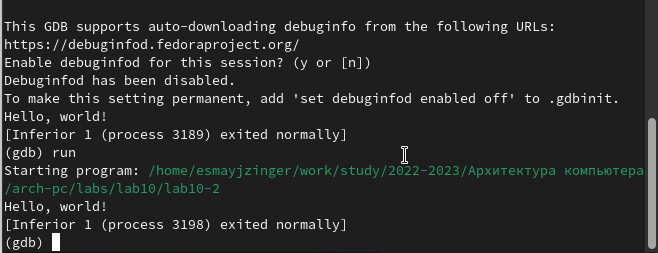


Рис. 6: Работа программы lab10-2.asm в отладчике

Для более подробного анализа программы установим брейкпоинт на метку start, с которой начинается выполнение любой ассемблерной программы, и запустим её. Посмотрим дисассимилированный код программы (рис. 7, 8)

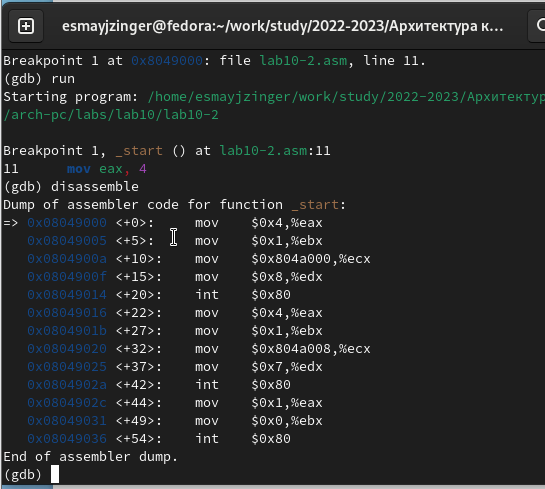


Рис. 7: дисассимилированный код

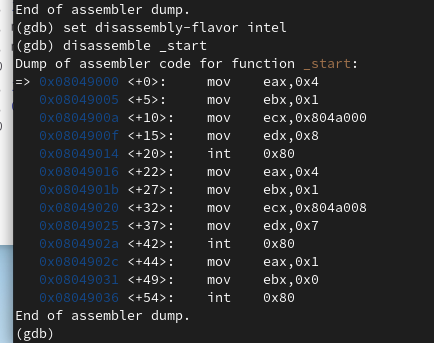


Рис. 8: дисассимилированный код в режиме интел

На предыдущих шагах была установлена точка останова по имени метки (\_start). Проверьте это с помощью команды info breakpoints (кратко i b) Установим еще одну точку останова по адресу инструкции. Адрес инструкции можно увидеть в средней части экрана в левом столбце соответствующей инструкции. Определим адрес предпоследней инструкции (mov ebx,0x0) и установим точку.(рис. 9)

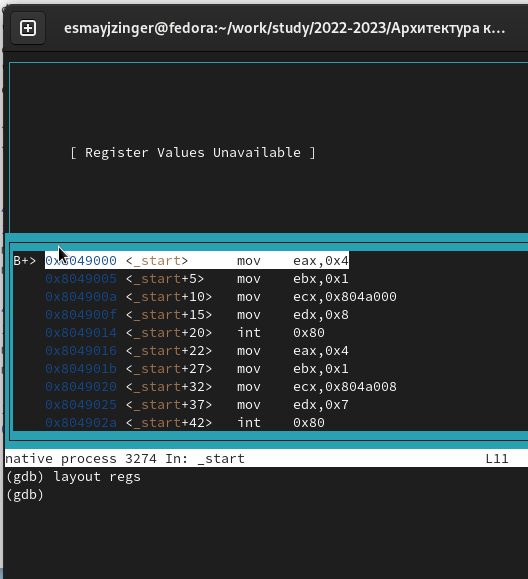


Рис. 9: точка остановки

Отладчик может показывать содержимое ячеек памяти и регистров, а при необходимости позволяет вручную изменять значения регистров и переменных. Выполним 5 инструкций с помощью команды stepi (или si) и проследим за изменением значений регистров. (рис. 11 12)

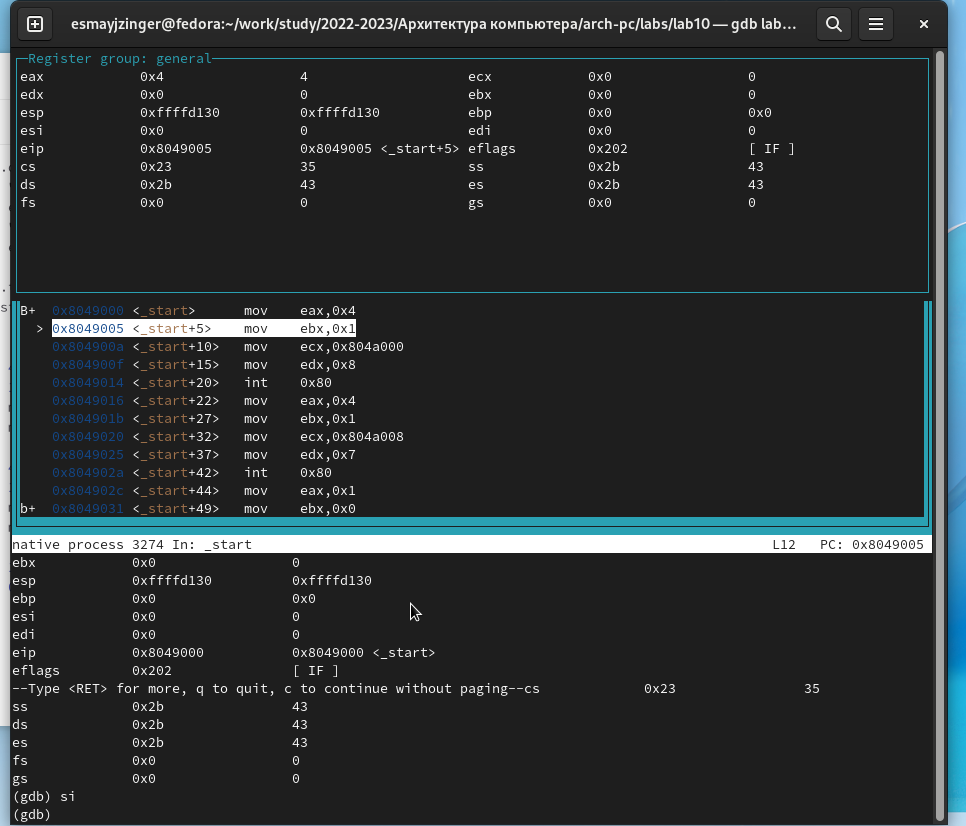


Рис. 10: изменение регистров

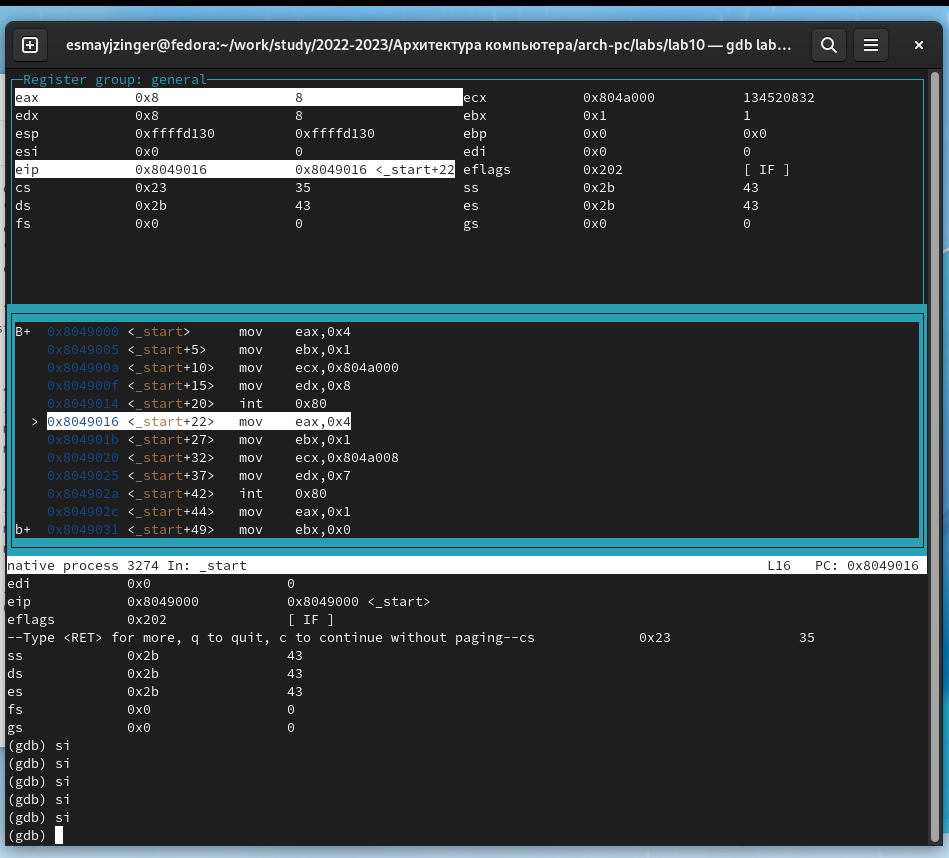


Рис. 11: изменение регистров

Посмотрим значение переменной msg1 по имени Посмотрим значение переменной msg2 по адресу Изменить значение для регистра или ячейки памяти можно с помощью команды set, задав ей в качестве аргумента имя регистра или адрес. Изменим первый символ переменной msg1 Заменим любой символ во второй переменной msg2. (рис. 12)

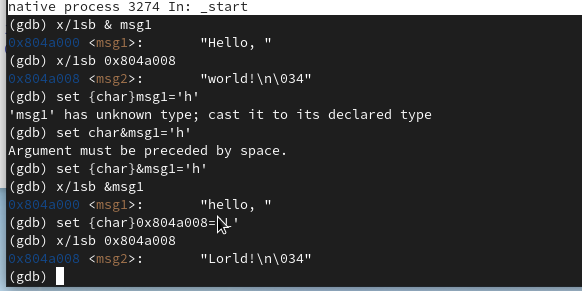


Рис. 12: изменение значения переменной

Выведем в различных форматах (в шестнадцатеричном формате, в двоичном формате и в символьном виде) значение регистра edx. С помощью команды set изменим значение регистра ebx:(рис. 13)

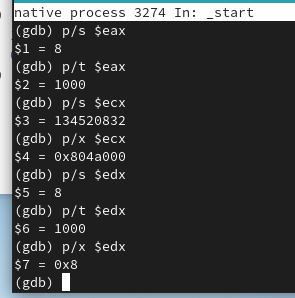


Рис. 13: вывод значения регистра

С помощью команды set изменим значение регистра ebx:(рис. 14)

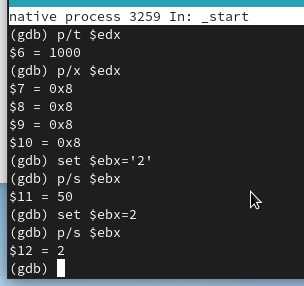


Рис. 14: вывод значения регистра

1. Скопируем файл lab9-2.asm, созданный при выполнении лабораторной работы №9, с программой выводящей на экран аргументы командной строки. Создадим исполняемый файл. Для загрузки в gdb программы с аргументами необходимо использовать ключ –args. Загрузим исполняемый файл в отладчик, указав аргументы.

Для начала установим точку останова перед первой инструкцией в программе и запустим ее.

Адрес вершины стека хранится в регистре esp и по этому адресу располагается число равное количеству аргументов командной строки (включая имя программы): Как видно, число аргументов равно 5 – это имя программы lab10-3 и непосредственно аргументы: аргумент1, аргумент, 2 и ‘аргумент 3’.

Посмотрим остальные позиции стека – по адесу [esp+4] располагается адрес в памяти где находится имя программы, по адесу [esp+8] хранится адрес первого аргумента, по аресу [esp+12] – второго и т.д. (рис. 15)

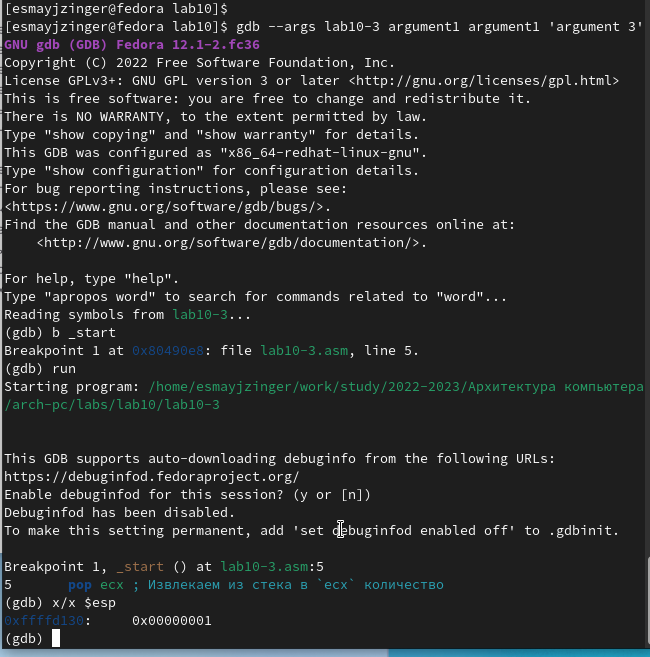


Рис. 15: вывод значения регистра

Шаг изменения адреса равен 4, потому что шаг равен размеру переменной - 4 байтам.

1. Преобразуем программу из лабораторной работы №9 (Задание №1 для самостоятельной работы), реализовав вычисление значения функции f(x) как подпрограмму. (рис. 16 17)

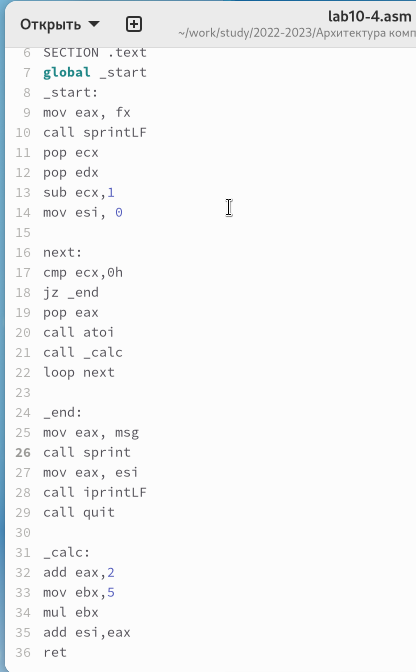


Рис. 16: Файл lab10-4.asm

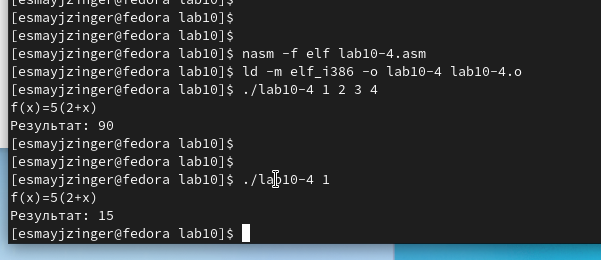


Рис. 17: Работа программы lab10-4.asm

1. В листинге приведена программа вычисления выражения (3+2)\*4+5. При запуске данная программа дает неверный результат. Проверим это. С помощью отладчика GDB, анализируя изменения значений регистров, определим ошибку и исправим ее.(рис. 18 19 20 21)

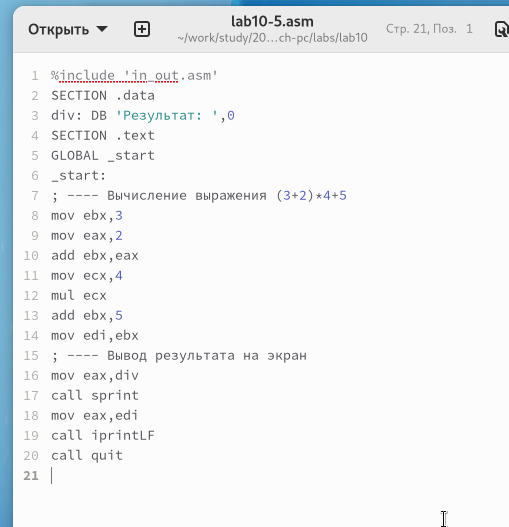


Рис. 18: код с ошибкой

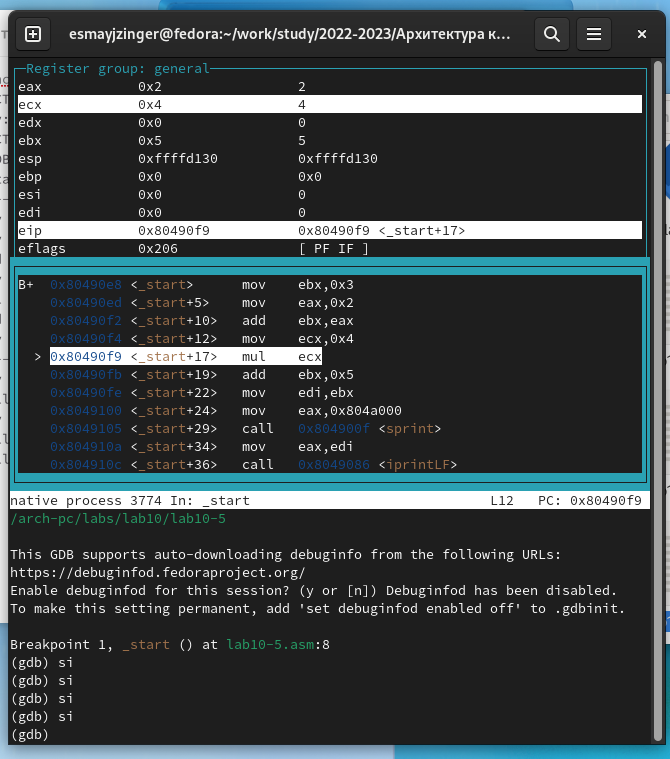


Рис. 19: отладка

Отметим, что перепутан порядок аргументов у инструкции add и что по окончании работы в edi отправляется ebx вместо eax

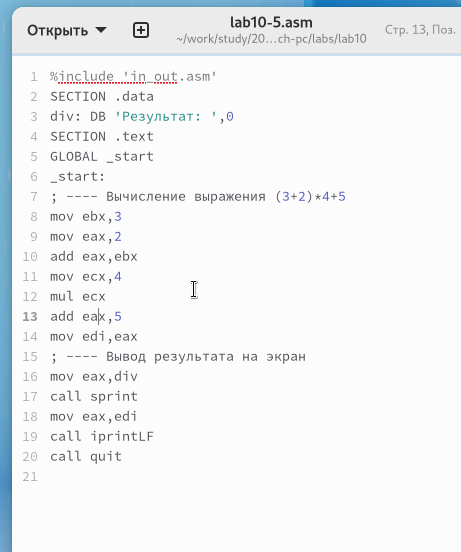


Рис. 20: код исправлен

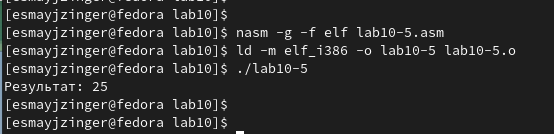


Рис. 21: проверка работы

# 4 Выводы

Во время выполнения лабораторной работы была освоена работа с подпрограммами и отладчиком.