**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО**

**ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»  
(БГТУ им. В.Г.Шухова)**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Лабораторная работа №1

Дисциплина: Архитектура вычислительных систем

по теме Разработка программ на ассемблере.

Работа с отладчиком OllyDbg и пакетом masm32

Выполнил: ст. группы ВТ-32  
 Воскобойников И. С.

Проверил: Осипов.О.В

**Белгород 2020**

**Цель работы:** получить навыки создания и отладки простейших программ на

ассемблере с использованием пакета masm32 и отладчика OllyDbg.

Задания для выполнения к работе

1. Ознакомиться со средой OllyDbg и компилятором masm32.
2. Создать и скомпилировать программу в соответствии с вариантом задания.
3. Отладить программу.
4. С помощью OllyDbg определить местонахождение переменных в сегменте

данных, а также их размер.

1. Выполнить пошаговую трассировку программы. Определить какие регистры
2. изменяют свои значения в процессе выполнения команд.

Вариант 3

**Выполнения работы**

1. Создать файл lab1.asm со следующим содержимым:

.386 ; Тип процессора

.model flat, stdcall ; Модель памяти и стиль вызова подпрограмм

option casemap: none ; Чувствительность к регистру

; --- Подключение файлов с кодом, макросами, константами, прототипами функций и т.д.

include c:\masm32\include\windows.inc

include c:\masm32\include\kernel32.inc

include c:\masm32\include\user32.inc

; --- Подключаемые библиотеки ---

includelib c:\masm32\lib\user32.lib

includelib c:\masm32\lib\kernel32.lib

; --- Сегмент данных ---

.data

m DB 20 DUP (4)

n DB 20 DUP (8)

a DW 500

b DD ?

cc DQ 15.5

d DD 7.5

; --- Сегмент кода ---

.code

start:

MOV EAX, 77 ; Поместить в регистр EAX число 77

MOV EBX, 34

ADD EAX, EBX ; Сложение чисел 77 + 34

MOV EDX, 4

MUL EDX ; Умножение EDX = (77 + 34)\*4

push NULL

call ExitProcess ; Выход из программы

end start

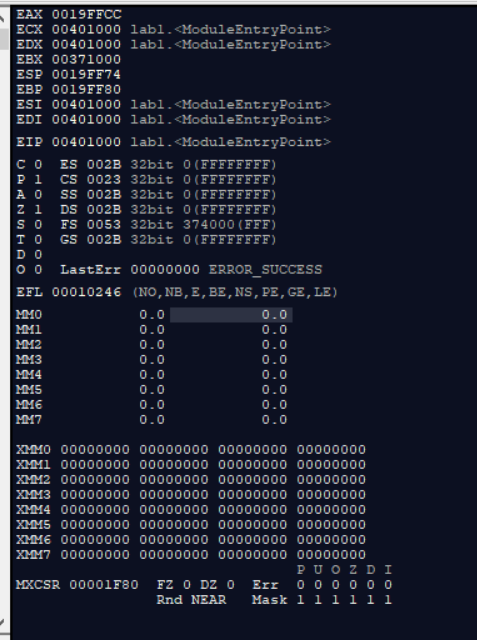
1. Скомпилировать программу и получить исполняемый файл lab1.exe.
2. Открыть файл lab1.exe в OllyDbg.
3. Сегмент данных содержит два массива и четыре переменные:



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Название переменной | Начальный адрес | Конечный адрес | Размер данных, байт | Тип |
| **m** | 00403000 | 00403013 | 20 | Массив из 20 однобайтовых целых чисел |
| **n** | 00403028 | 00403029 | 20 | Массив из 20 однобайтовых целых чисел |
| **a** | 0040302A | 0040302D | 2 | 2-байтовое целое |
| **b** | 0040302E | 00403035 | 4 | 4- байтовый символ |
| **сс** | 00403033 | 0040303B | 8 | 8-байтовое вещественное |
| **d** | 00403036 | 00403039 | 4 | 4-байтовое вещественное |
| Общий размер сегмента данных: | | | **58** |  |

1. Пошаговое выполнение программы

Исходное состояние регистров:

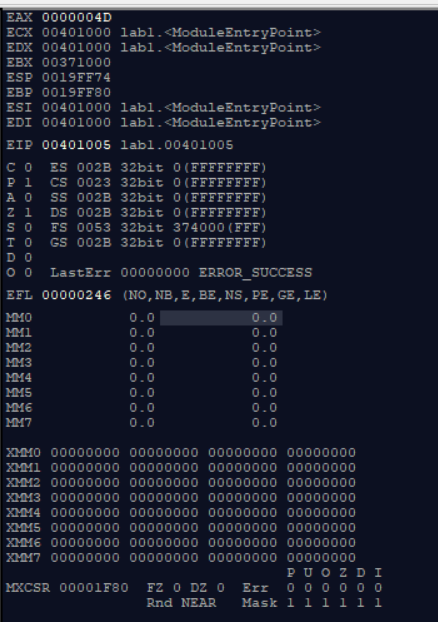


5.1

MOV EAX,4D

Код команды – **B8 4D000000**. Команда пересылает в регистр **EAX** 4 байта из ячейки памяти с адресом 0040203C -00402040

(переменная **d**). Увеличивает **EIP** на 5 (размер кода команды).

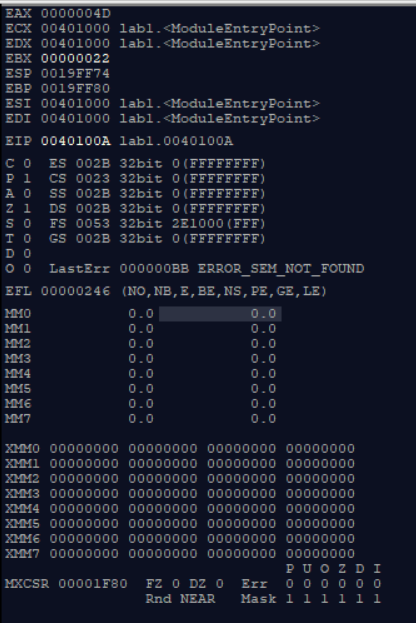


5.2

MOV EBX,22

Код команды – **BB22000000**. Команда пересылает в регистр **EBX** константу 22 . Увеличивает **EIP** на 5 (размер кода команды).

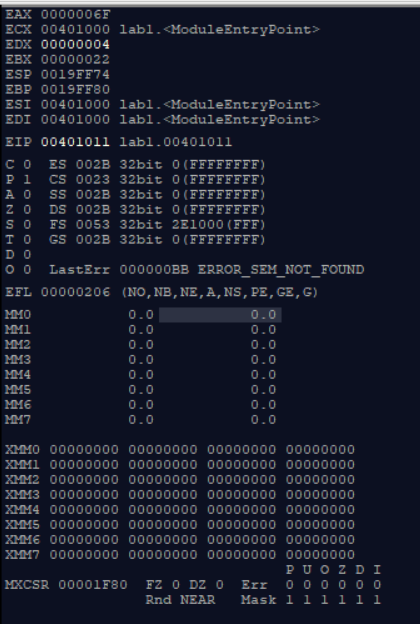
Вывод: В ходе лабараторной работы мы научились разрабатывать программу на ассемблере работать с отладчиком OllyDbg и пакетом masm32. Познакомились с регистрами процессора,способом вызова функций и как расположены данные в сегменте данных.



5.3 ADD EAX,EBX

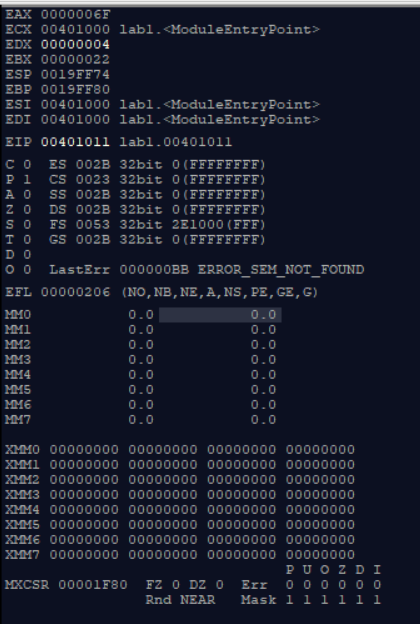
Сложение регистра аккумулятора размер – 32 бита и базового регистра размер – 32 бита.

Код команды 03С3



5.4 MOV EDX,4

Код команды – BA 04000000. Команда пересылает в регистр EAX 4 байта



5.5 MUL EDX

Код команды – **F7E2**. Команда умножает к регистру **EAX** на EDX.

Декомпиляция програаммы

