Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут”

Кафедра ОТ

**ЗВІТ**

про виконання лабораторної роботи № 5

з дисципліни

“Системне програмування”

|  |  |  |
| --- | --- | --- |
| Прийняв: |  | Виконав: |
| Павлов Валерій  Георгійович |  | студент 2-го курсу  гр. ІП-53 ФІОТ  Сулима Олександр Сергійович |

Київ – 2016

**Лабораторна робота №5**

**Дослідження структури програм формату COM.**

**Мета роботи**

Вивчення прийомів написання, компіляції і відладки програм формату **COM** в середовищі **Masm32**. Здобуття навичок читання лістингу і розшифрування кодів команд.

**Порядок виконання роботи**

1. Вивчити структуру програм формату **COM** і застосування переривань **BIOS** та **MS-DOS** при роботі з консоллю [1].

2. Розробити програму на мові Асемблер, за допомогою якої на екран системної консолі по введеному паролю виводяться персональні дані студента – ПІБ, дата народження, номер залікової книжки тощо (див. лаб. роботу 1) кожне з нового рядка з попереднім очищенням вікна системної консолі. Для правильного відображення при виведенні символів кирилиці підключити відповідну кодову сторінку.

3. Вивчити опції компілятора і лінковщика і сформувати **BAT**-файл, в якому передбачити завдання назви вихідного файлу **.asm**, як параметра. Шлях до файлу має бути визначений в результаті сканування логічного диску і служити для вказівки розміщення відповідних йому об'єктного і виконуваного файлів.

4. Виконати компіляцію розробленого файлу у формат **COM**.

5. Перевірити роботу програми шляхом введення як правильного, так і невірного паролів.

6. Отриманий виконуваний файл дослідити за допомогою програми **HEX**-редактору **HIEW32** або **HIEW**. У останньому випадку для запуску програми сформувати ярлик, де виконати налаштування параметрів сумісності з використовуваною операційною системою. Демоверсія **HEX**-редактору **HIEW32**, наприклад, доступна на **Internet**-ресурсі:

**http://soft.mydiv.net/win/download-Hiew.html.**

7. Перемикаючи послідовно режими перегляду (**Text – Hex – Decode**), зняти три відповідних скріншоти програми і привести їх в звіті по лабораторній роботі.

8. Переконатися, що текст оригінала пароля, який міститься в тексті програми, може бути легко виявлений за допомогою **HEX**-редактора.

9. Замінити в тексті програми символи пароля їх **ASCII**-кодамі, знову скомпілювати **COM**-файл і переконатися, що тепер вони не виявляються явним чином в тексті виконуваного **COM**-файлу. Привести скріншоти цієї програми в режимах «**Text**» та «**Decode**» у звіті по лабораторній роботі.

10. Порівняти текст програми, який набирався в редакторові, з текстом програми в скомпільованому вигляді, який формує **HEX**-редактор **HIEW**. Виявити розбіжності і відобразити їх в звіті по лабораторній роботі.

11. На отриманому у п. 9 в режимі «**Decode**» скріншоті знайти всі команди **MOV**, виписати їх коди і розібрати по окремих полях, відповідно їх формату. Результати привести в звіті по лабораторній роботі.

12. Зробити висновки по лабораторній роботі.

Література, що рекомендується:

1. Юров В.И. Assembler. Практикум – СПб, : Питер, 2006, - 399 стр.

2. HIEW. Материал из Википедии. https://ru.wikipedia.org/wiki/Hiew.

**Лістинг командного файлу:**

.386

.model flat, stdcall

option casemap: none

include E:\masm32\include\windows.inc

include E:\masm32\macros\macros.asm

include E:\masm32\include\masm32.inc

include E:\masm32\include\user32.inc

include E:\masm32\include\kernel32.inc

include E:\masm32\include\msvcrt.inc

includelib E:\masm32\lib\masm32.lib

includelib E:\masm32\lib\msvcrt.lib

includelib E:\masm32\lib\user32.lib

includelib E:\masm32\lib\kernel32.lib

.data

nameS db "Сулима Олександр",0

numb2 db "IП-53",0

numb3 db "Series: 5318",0

before byte "Введiть пароль:",0

errors db "Введений пароль не вiрний",0

inp DWORD ?

outp DWORD ?

bufferRead byte 8 dup (0)

in\_Num DWORD ?

out\_Num DWORD ?

my\_pass byte "0404",0

messg byte 13, 10

.code

main:

invoke GetStdHandle, STD\_INPUT\_HANDLE

mov inp, eax

invoke GetStdHandle, STD\_OUTPUT\_HANDLE

mov outp, eax

invoke WriteConsoleA, outp, addr before, SIZEOF before,ADDR out\_Num,0

invoke ReadConsoleA, inp, ADDR bufferRead, 10, ADDR in\_Num, 0

invoke WriteConsoleA, outp,ADDR messg,SIZEOF messg, ADDR out\_Num,0

CLD

LEA ESI, bufferRead

LEA EDI, my\_pass

REPE CMPSB

jnz alternative

invoke ClearScreen

print chr$(10)

print addr nameS

print chr$(10)

print addr numb2

print chr$(10)

print addr numb3

print chr$(10)

inkey

invoke ExitProcess, 0

alternative:

print addr errors

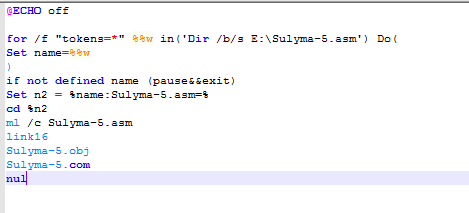
print chr$(10)

inkey

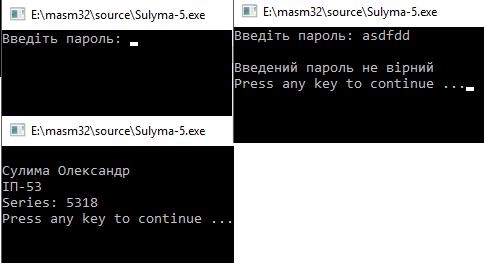
invoke ExitProcess, 0

end main

**Лістинг bat файлу:**



**Скріншоти:**



Висновки

Метою даної роботи було вивчити прийоми написання, компіляції і відладки програм формату СОМ в середовищі Masm32 і використання багато-віконного інтерфейсу для виведення інформації.